

**DEPARTMENT OF HOMELAND SECURITY
APPROPRIATIONS FOR 2010**

HEARINGS
BEFORE A
SUBCOMMITTEE OF THE
COMMITTEE ON APPROPRIATIONS
HOUSE OF REPRESENTATIVES
ONE HUNDRED ELEVENTH CONGRESS
FIRST SESSION

SUBCOMMITTEE ON HOMELAND SECURITY

DAVID E. PRICE, North Carolina, *Chairman*

JOSÉ E. SERRANO, New York	HAROLD ROGERS, Kentucky
CIRO RODRIGUEZ, Texas	JOHN R. CARTER, Texas
C.A. "DUTCH" RUPPERSBERGER, Maryland	JOHN ABNEY CULBERSON, Texas
ALAN B. MOLLOHAN, West Virginia	MARK STEVEN KIRK, Illinois
NITA M. LOWEY, New York	KEN CALVERT, California
LUCILLE ROYBAL-ALLARD, California	
SAM FARR, California	
STEVEN R. ROTHMAN, New Jersey	

NOTE: Under Committee Rules, Mr. Obey, as Chairman of the Full Committee, and Mr. Lewis, as Ranking Minority Member of the Full Committee, are authorized to sit as Members of all Subcommittees.

STEPHANIE GUPTA, JEFF ASHFORD, SHALANDA YOUNG,
JIM HOLM, WILL PAINTER, and ADAM WILSON,
Staff Assistants

PART 2

DEPARTMENT OF HOMELAND SECURITY

	Page
Securing the Nation's Rail and Transit Systems (Part 1)	1
Securing the Nation's Rail and Transit Systems (Part 2)	95
Improving the Efficiency of the Aviation Security System	281
Biometric Identification	356
Developing and Transitioning Homeland Security Research	
Products Into Use	436
Member Requests	568
Outside Witness Testimony	598



Transit
Av.Sec.
Bio.
S&T
Mem.Req.
Out.Wit.

PART 2—DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS FOR 2010

DEPARTMENT OF HOMELAND SECURITY
APPROPRIATIONS FOR 2010

HEARINGS
BEFORE A
SUBCOMMITTEE OF THE
COMMITTEE ON APPROPRIATIONS
HOUSE OF REPRESENTATIVES
ONE HUNDRED ELEVENTH CONGRESS
FIRST SESSION

SUBCOMMITTEE ON HOMELAND SECURITY

DAVID E. PRICE, North Carolina, *Chairman*

JOSÉ E. SERRANO, New York	HAROLD ROGERS, Kentucky
CIRO RODRIGUEZ, Texas	JOHN R. CARTER, Texas
C.A. "DUTCH" RUPPERSBERGER, Maryland	JOHN ABNEY CULBERSON, Texas
ALAN B. MOLLOHAN, West Virginia	MARK STEVEN KIRK, Illinois
NITA M. LOWEY, New York	KEN CALVERT, California
LUCILLE ROYBAL-ALLARD, California	
SAM FARR, California	
STEVEN R. ROTHMAN, New Jersey	

NOTE: Under Committee Rules, Mr. Obey, as Chairman of the Full Committee, and Mr. Lewis, as Ranking Minority Member of the Full Committee, are authorized to sit as Members of all Subcommittees.

STEPHANIE GUPTA, JEFF ASHFORD, SHALANDA YOUNG,
JIM HOLM, WILL PAINTER, and ADAM WILSON,
Staff Assistants

PART 2

DEPARTMENT OF HOMELAND SECURITY

	Page
Securing the Nation's Rail and Transit Systems (Part 1)	1
Securing the Nation's Rail and Transit Systems (Part 2)	95
Improving the Efficiency of the Aviation Security System	281
Biometric Identification	356
Developing and Transitioning Homeland Security Research	
Products Into Use	436
Member Requests	568
Outside Witness Testimony	598



Printed for the use of the Committee on Appropriations

U.S. GOVERNMENT PRINTING OFFICE

COMMITTEE ON APPROPRIATIONS

DAVID R. OBEY, Wisconsin, *Chairman*

JOHN P. MURTHA, Pennsylvania	JERRY LEWIS, California
NORMAN D. DICKS, Washington	C. W. BILL YOUNG, Florida
ALAN B. MOLLOHAN, West Virginia	HAROLD ROGERS, Kentucky
MARCY KAPTUR, Ohio	FRANK R. WOLF, Virginia
PETER J. VISCLOSKEY, Indiana	JACK KINGSTON, Georgia
NITA M. LOWEY, New York	RODNEY P. FRELINGHUYSEN, New Jersey
JOSÉ E. SERRANO, New York	TODD TIAHRT, Kansas
ROSA L. DELAURO, Connecticut	ZACH WAMP, Tennessee
JAMES P. MORAN, Virginia	TOM LATHAM, Iowa
JOHN W. OLVER, Massachusetts	ROBERT B. ADERHOLT, Alabama
ED PASTOR, Arizona	JO ANN EMERSON, Missouri
DAVID E. PRICE, North Carolina	KAY GRANGER, Texas
CHET EDWARDS, Texas	MICHAEL K. SIMPSON, Idaho
PATRICK J. KENNEDY, Rhode Island	JOHN ABNEY CULBERSON, Texas
MAURICE D. HINCHEY, New York	MARK STEVEN KIRK, Illinois
LUCILLE ROYBAL-ALLARD, California	ANDER CRENSHAW, Florida
SAM FARR, California	DENNIS R. REHBERG, Montana
JESSE L. JACKSON, JR., Illinois	JOHN R. CARTER, Texas
CAROLYN C. KILPATRICK, Michigan	RODNEY ALEXANDER, Louisiana
ALLEN BOYD, Florida	KEN CALVERT, California
CHAKA FATTAH, Pennsylvania	JO BONNER, Alabama
STEVEN R. ROTHMAN, New Jersey	STEVEN C. LATOURETTE, Ohio
SANFORD D. BISHOP, JR., Georgia	TOM COLE, Oklahoma
MARION BERRY, Arkansas	
BARBARA LEE, California	
ADAM SCHIFF, California	
MICHAEL HONDA, California	
BETTY MCCOLLUM, Minnesota	
STEVE ISRAEL, New York	
TIM RYAN, Ohio	
C.A. "DUTCH" RUPPERSBERGER, Maryland	
BEN CHANDLER, Kentucky	
DEBBIE WASSERMAN SCHULTZ, Florida	
CIRO RODRIGUEZ, Texas	
LINCOLN DAVIS, Tennessee	
JOHN T. SALAZAR, Colorado	

BEVERLY PHETO, *Clerk and Staff Director*

**DEPARTMENT OF HOMELAND SECURITY
APPROPRIATIONS FOR 2010**

THURSDAY, MARCH 12, 2009.

**SECURING THE NATION'S RAIL AND TRANSIT SYSTEMS,
PART 1**

WITNESSES

**JOHN SAMMON, ASSISTANT ADMINISTRATOR FOR TRANSPORTATION
SECTOR NETWORK MANAGEMENT, TRANSPORTATION SECURITY AD-
MINISTRATION**

**W. ROSS ASHLEY, ASSISTANT ADMINISTRATOR OF GRANT PROGRAMS,
FEDERAL EMERGENCY MANAGEMENT AGENCY**

**BILL MORANGE, DEPUTY EXECUTIVE DIRECTOR AND DIRECTOR OF
SECURITY, NEW YORK METROPOLITAN TRANSPORTATION AUTHOR-
ITY**

**JACK ECKLES, DEPUTY EXECUTIVE OFFICER FOR SYSTEM SAFETY
AND SECURITY, LOS ANGELES COUNTY METROPOLITAN TRANSPOR-
TATION AUTHORITY**

OPENING STATEMENT OF CHAIRMAN PRICE

Mr. PRICE. Good morning. The subcommittee will come to order. Today's hearing will focus on how well security programs have been operating in the rail and transit arena and how effectively Federal dollars have been spent to protect the users of these systems from any incidents. These efforts are jointly run by the Transportation Security Administration, which is in charge of surface transportation security efforts, and the Federal Emergency Management Agency, FEMA, which is responsible for distributing grants annually to rail and transit systems to strengthen the security efforts.

I am including funds here contained in the recently enacted economic recovery package. To date rail and transit entities have received a total of \$1.67 billion in grants for security enhancements, including infrastructure protection, deterrence, facility hardening, and employee training.

Worldwide the most common transportation terrorist targets have been rail and transit systems. We have been lucky in the United States, but others have not been so fortunate. The attacks in Madrid, London, Mumbai all come to mind when we discuss rail and transit security.

More recently, on January 24th, the Indian Army recovered two powerful bombs near a railway station in the state of Assam. The bombs were discovered just 2 days before India's Republic Day celebration. As a result the Assam government suspended night train

operations until after the holiday out of concern for possible sabotage attempts.

In addition, in Pakistan on February 7th bus drivers began receiving letters from the Taliban threatening attacks by suicide bombers if Western devices such as audio and video equipment were not removed.

Finally, on February 18th, in our own country, in my own State of North Carolina, we had a bomb scare on Amtrak, February 18th. After dogs inspected the train for about 4 hours, the train was cleared to move ahead.

While we have thus far been spared the type of violent attacks that occurred elsewhere, we must be ever vigilant in our efforts to prevent incidents from occurring in this country.

Based on the Homeland Security Department's first Federal valuation of mass transit security, however, transit and rail security efforts are not as vigorous as they should be. The report showed that 77 percent of the Nation's largest rail and bus systems are not meeting Homeland Security guidelines. By contrast, 96 percent of the airlines are complying with security requirement. This isn't surprising given that when the Transportation Security Administration was created in 2001 it was tasked first of all with federalizing aviation security. Since that time aviation security has received the preponderance of Federal funding and attention. In comparison, other modes of transportation security such as rail and transit have remained under the purview of local communities in the private sector, receiving yearly grant funds to address their highest security risks.

During Secretary Napolitano's confirmation hearing, she announced that she would focus on surface transportation security because, as she said, we have done an awful lot in the aviation world. Secretary Napolitano followed this up with the secretarial directive asking TSA to review the current strategies, plans and programs for security of the air, surface and maritime transportation sectors, to include a side-by-side comparison of the threat environment resources and personnel devoted to each transportation sector.

The budget blueprint we received just 2 weeks ago places a renewed emphasis on transportation systems. It is my hope that today we can discuss how TSA and FEMA through its grants plan to focus on rail and transit security, including what efforts the Department and the largest rail and transit entities are undertaking to improve the poor assessments that they have received.

We have a distinguished panel before us to discuss the security threats, vulnerabilities, and needs of our Nation's rail and transit systems. The panel consists of Mr. John Sammon, TSA's Assistant Administrator of Transportation Sector Network Management; Mr. Ross Ashley, the Assistant Administrator for Grants of the Federal Emergency Management Agency; Mr. William Morange, Deputy Executive Director and Director of Security, New York Metropolitan Transportation Authority; and Mr. Jack Eckles, the Deputy Executive Officer, System Safety, Security and Law Enforcement, Los Angeles County Metropolitan Transportation Authority. We welcome all of you and look forward to your participation here today.

I will ask Mr. Sammon to begin, followed by Mr. Ashley, Mr. Morange, and finally Mr. Eckles. If each of you could summarize

your statement in 5 minutes, your full written statement will be entered into the record and after all of you have concluded we will proceed with questions. Let me turn now to our distinguished ranking member, Harold Rogers, for his opening comments.
[The information follows:]



COMMITTEE ON APPROPRIATIONS

David Price (D-NC), Chairman, Subcommittee on Homeland Security

FOR RELEASE UPON DELIVERY

Thursday, March 12, 2009

Media Contact:
Phil Feagan
202-225-1784

OPENING STATEMENT OF CHAIRMAN DAVID PRICE *Securing the Nation's Rail and Transit Systems* *March 12, 2009 / 10:00 am*

Good morning. Today's hearing will focus on how well security programs have been operating in the rail and transit arena and how effectively federal dollars have been spent to protect the users of these systems from any incidents. These efforts are jointly run by the Transportation Security Administration, which is in charge of surface transportation security efforts, and the Federal Emergency Management Agency, which is responsible for distributing grants annually to rail and transit systems to strengthen their security efforts. To date, including funds contained in the recently enacted economic recovery package, rail and transit entities have received a total of \$1.67 billion in grants for security enhancements, including infrastructure protection, deterrence, facility hardening, and employee training.

Worldwide, the most common transportation terrorist targets have been rail and transit systems. While we have been lucky in the United States, others have not been so fortunate. The attacks in Madrid, London, and Mumbai all come to mind when we discuss rail and transit security. More recently, on January 24th, the Indian Army recovered two powerful bombs near a railway station in the state of Assam. The bombs were discovered just two days before India's Republic Day celebration. As a result, the Assam government suspended night train operations until after the holiday out of concern for possible sabotage attempts. In addition, in Pakistan on February 7th, bus drivers began receiving letters from the Taliban threatening attacks by suicide bombers if western devices, such as audio and video equipment, were not removed. Finally, on

February 18th, my own state of North Carolina had a bomb scare on Amtrak, but after dogs inspected the train for about four hours, the train was cleared.

While we have thus far been spared the type of violent attacks that have occurred elsewhere, we must be ever vigilant in our efforts to prevent incidents from occurring here. However, based on the Department of Homeland Security's first federal evaluation of mass transit security, transit and rail security efforts are not as vigorous as they should be. This report showed that 77 percent of the nation's largest rail and bus systems aren't meeting Homeland Security guidelines. By contrast, 96 percent of the airlines are complying with security requirements. This is not surprising, given that when the Transportation Security Administration was created in 2001, it was tasked with federalizing aviation security. Since that time, aviation security has received the preponderance of federal funding and attention. In comparison, other modes of transportation security, such as rail and transit, have remained under the purview of the local communities and the private sector, receiving yearly grant funds to address their highest security risks.

During Secretary Napolitano's confirmation hearing, she announced that she would focus on surface transportation security because "we have done an awful lot in the aviation world." Secretary Napolitano followed this up with a Secretarial directive asking TSA to review "the current strategies, plans and programs for security of the air, surface, and maritime transportation sectors, to include a side by side comparison of the threat environment, resources and personnel devoted to each transportation sector." The budget blueprint we received just two weeks ago places a renewed emphasis on transportation systems. It is my hope that today, we can discuss how TSA, and FEMA through its grants, plan to focus on rail and transit security, including what efforts the Department and the largest rail and transit entities are undertaking to improve the poor assessments they received.

We have a distinguished panel before us to discuss the security threats, vulnerabilities, and needs of our nation's rail and transit systems. The panel consists of Mr. John Sammon, TSA Assistant Administrator of Transportation Sector Network Management; Mr. Ross Ashley, Assistant Administrator for Grants of the Federal Emergency Management Agency; Mr. William

Morange, Deputy Executive Director and Director of Security, New York Metropolitan Transportation Authority; and Mr. Jack Eckles, Deputy Executive Officer, System Safety and Security, Los Angeles County Metropolitan Transportation Authority. I welcome you all and appreciate your participation here today. I will ask Mr. Sammon to begin, followed by Mr. Ashley, Mr. Morange, and finally Mr. Eckles. If each of you could summarize your statement in five minutes, your full written statement will be entered into the record. After all of you have concluded, we will proceed with questions.

But first I would like to recognize Ranking Member Rogers for an opening statement.

###

OPENING STATEMENT OF RANKING MEMBER ROGERS

Mr. ROGERS. Thank you, Mr. Chairman, and welcome to our guests today.

Recent well-coordinated attacks on rail and mass transit systems are a sobering reminder that our homeland security priorities are vast and continually changing. The terrorist strikes on the Madrid system in 2004, London in 2005, and the recent events in Mumbai all raise the question of whether we are effectively addressing vulnerabilities within our own rail and transit systems here at home, particularly at a time when public transportation ridership has risen to its highest level in 52 years.

DHS has initiated a number of programs over the last 6 years to strengthen security measures within the various surface transportation modes. Given the complexity of ownership and variety of systems and authorities involved it is no easy task, but it is a challenge that I believe can be overcome through careful coordination, analysis, and strategic planning. DHS has many tools at its disposal, and we must utilize them effectively.

First and foremost, more than \$1.5 billion have been provided for rail and transit grants since 9/11. However, only a paltry 12.6 percent of that money has actually been spent, leaving \$1.3 billion languishing in the coffer. That is unacceptable, but unfortunately nothing new to this subcommittee. Billions upon billions in first responder and other DHS grants are left by the wayside every year. While I certainly see the value of providing this assistance to our State and local partners, I have got to question its impact if they are not put towards their intended purpose.

With only a small fraction of grant funding having been spent, I have serious concerns about whether we have made any measurable dent in the security risks of our transit systems. The taxpayers deserve to know what we are buying and for what purpose we are buying.

Second, TSA's increasing deployments of Visual Intermodal Prevention and Response Teams, VIPeR, to mass transit stations appears to be a promising sign. It is my hope that these teams of law enforcement agents and canine teams are deterring those who would target rail and mass transit stations. TSA also appears to be honing in on the threat to rail shipments of hazardous materials with the issuance of new, improved regulations, most notably to establish a chain of custody for such materials. Again these are good signs, but are these efforts being coordinated with approved security plans as well as the available grant funding. We want to know that.

Third, the resource that pulls all this together is the TSA surface transportation inspectors. Their recent assessment of the Nation's largest transit systems reveal that only 23 percent demonstrated satisfactory security mechanisms and processes. That tells me that there are big gaps to fill that we are not addressing with either the grants or the VIPeR teams.

While it is evident that securing these transportation modes is extremely challenging, there must be effective ways to provide sufficient security without unduly hindering the free flow of passengers and commerce.

To help us address this issue we have with us some very experienced professionals from two of the Nation's largest transit systems. Gentlemen, we thank you for being here. We look forward to hearing your thoughts and ideas and hopefully some suggestions that we can take seriously.

I also look forward to hearing from Mr. Sammon of TSA, Mr. Ashley of FEMA on how DHS is working with its State and local partners to better secure the transit systems that on average make more than 27 million passenger trips a day across our great Nation.

Thank you, Mr. Chairman. I look forward to today's discussions.
[The information follows:]

OPENING STATEMENT

CONGRESSMAN
Hal Rogers



FIFTH DISTRICT • KENTUCKY

Offices in
Washington, D.C.
Somerset, Prestonsburg,
Hazard

Contact: Stefani Zimmerman

202.225.4601

**Opening Statement
Subcommittee on Homeland Security Appropriations**

Rail & Transit Security

Witnesses:

**Mr. John Sammon, Assistant Administrator of Transportation Sector
Network Management, TSA**

Mr. W. Ross Ashley, Director of Grants Program Directorate, FEMA

**Mr. Jack Eckles, Deputy Executive Officer for System Safety and Security,
Los Angeles Metropolitan Transportation Authority**

**Mr. Bill Morange, Deputy Executive Director & Director of Security,
New York Metropolitan Transportation Authority**

10:00 AM | Thursday | March 12, 2009 | 2359

Thank you, Mr. Chairman, and welcome to our distinguished guests.

Recent, well-coordinated attacks on rail and mass transit systems are a sobering reminder that our homeland security priorities are vast and continually changing. The terrorist strikes on the Madrid train system in 2004, the attack on the London transit system in 2005, and the recent incidents in Mumbai all raise the question of whether we are effectively addressing vulnerabilities within our own rail and transit systems here at home -- particularly at a time when public transportation ridership has *risen to its highest level in 52 years*.

DHS has initiated a number of programs over the last six years to strengthen security measures within the various surface transportation modes. Given the complexity of ownership, and variety of systems and authorities involved, it is no easy task -- but it is a challenge that *I believe can be overcome through careful coordination, analysis and strategic planning*. DHS has many tools at its disposal, and we must utilize them effectively.

First and foremost, more than \$1.5 billion has been provided for rail and transit grants since 9/11. However, only a paltry 12.6 percent has actually been spent -- leaving some \$1.3 billion languishing in the coffer. This is unacceptable, but unfortunately, is nothing new to this Subcommittee. Billions upon billions in first responder and other DHS grants are left by the wayside every year. And while I certainly see the value of providing this assistance to our State and local partners, I have to question its impact if they're not being put towards their intended purpose. With only a small fraction of grant funding having been spent, I have serious concerns about whether we've made any measurable dent in the security risks our transit systems face. The taxpayer deserves to know what we're buying and for what purpose.

Second, TSA's increasing deployments of Visual Intermodal Prevention and Response teams -- or VIPR teams -- to mass transit stations appears to be a promising sign.

It is my hope that these teams of law enforcement agents and canine teams are deterring those who would target rail and mass transit stations. TSA also appears to be honing in on the threat to rail shipments of hazardous materials with the issuance of new, improved regulations -- most notably, to establish a chain of custody for such materials. Again, these are good signs, but how are these efforts being coordinated with approved security plans as well as the available grant funding?

Third, the resource that pulls all this together is the TSA surface transportation inspectors. Their recent assessment of the nation's largest transit systems revealed that only 23% demonstrated satisfactory security mechanisms and processes. That tells me that there are big gaps to fill that we are not addressing with either the grants or the VIPR teams.

While it's evident that securing these transportation modes is extremely challenging, there must be effective ways to provide sufficient security without unduly hindering the free flow of passengers and commerce.

To help us address this issue, we have with us some very experienced professionals from two of the Nation's largest transit systems—gentlemen, we thank you for being here and I look forward to hearing your thoughts.

I also look forward to hearing from Mr. Sammon of TSA and Mr. Ashley of FEMA on how DHS is working with its State and local partners to better secure the transit systems that, on average, make more than 27 million passenger trips a day across our great Nation.

Thank you, Mr. Chairman. I look forward to today's discussion.

###

Mr. PRICE. Thank you. Mr. Sammon, please proceed.

OPENING STATEMENT OF JOHN SAMMON

Mr. SAMMON. Thank you. Good morning, Chairman Price, Ranking Member Rogers, distinguished members of the subcommittee, and my colleagues from FEMA, New York, and Los Angeles. I am pleased to be here today to discuss progress by the Transportation Security Administration on rail and mass transit security grant programs.

The transit grant program is an important part of TSA's Intel driven, risk-based, counterterrorism transit security strategy. TSA's counterterrorism transit strategy is focused on making high risk transit systems less attractive targets and more secure, less attractive through forward leaning visible deterrents such as VI-PeRs, canines, mobile screening, security surges, trained front line employees and an aware public and behavioral detection capabilities, more secure through intrusion and anomaly detection, access control, and facility hardening.

TSA's transit strategy begins with active security partner engagement. Peer advisers, two-way communication, best practice and intelligence sharing, followed by continuous improvement and, finally, risk based allocation of grant funding.

TSA's grant strategy begins with a regional focus. We believe that effective transit security requires an overall regional level of security. Manhattan cannot be protected if potential terrorists have free access to transit systems in New Jersey. The grant process in the past had mostly to do with dividing up the pie and individual agencies selecting projects that they separately deemed appropriate. TSA has shaped the process to begin with intelligence insights, focused resources on high risk agencies, give priority to low cost, high return security measures and use regional transit security working groups to identify, discuss and determine regional priorities.

Security partner input has helped shape this process in many important ways. Two weeks after I started my job at TSA in the summer of 2006, I went to New York to meet Bill Morange and his staff for his transit security insights. Bill stressed the training, drills, canine teams and mobile bag screening were common practices on the MTA. The same month I traveled to Houston to ask Chief Tom Lambert how we might set up a transit advisory group for TSA composed of key transit law enforcement chiefs. He said, hire somebody who has walked in our shoes to lead the transit effort, and we did. We hired Paul Lennon, Jack Eckles' predecessor in Los Angeles, as the general manager of transit. Paul is right over here in the corner. We also hired Sonia Proctor, former chief with Amtrak and we also hired Fred Godeen, Vice President, Safety and Risk Management, from Washington Metro.

Subsequent conversations with Chief Lambert created a way to streamline training grants to encourage more transit agencies to release front line employees for training classes. New Jersey Transit approved champion getting behavioral assessment training on a DHS approved list for transit officers. The Los Angeles Sheriff's Department fostered a regional versus agency view of transit security priorities. Chief John O'Connor from Amtrak developed the op-

erating agreement protocols to allow increased Federal and local VIPeR coordination exercises. Executive Director Bill Morange and Chief Jim Hall from New York and Chief Dan Finkelstein of Los Angeles are among the fine group of law enforcement chiefs advising TSA on a regular basis.

In summary, TSA's transit strategy evolves through and is better from constant interaction with our security partners and advisers. It is designed to make terrorist attack planning more difficult and the targets less attractive, and it is designed to make the facilities and systems more secure. Transit grants are an important part of that strategy. The grant process is an important tool to support a transit security strategy, and all of us at DHS want it to be as successful as possible. We look forward to working with our partners at FEMA to award the additional grant funds provided in the Recovery Act as expeditiously as possible to put more Americans to work securing our transit systems and to make this grant process as streamlined and as effective for security as we can.

Thank you, and I will be happy to answer any questions you may have.

[The statement of Mr. Sammon follows:]

UNITED STATES DEPARTMENT OF HOMELAND SECURITY
TRANSPORTATION SECURITY ADMINISTRATION

Statement of

JOHN SAMMON
ASSISTANT ADMINISTRATOR

Before the

SUBCOMMITTEE ON HOMELAND SECURITY
COMMITTEE ON APPROPRIATIONS
UNITES STATES HOUSE OF REPRESENTATIVES

MARCH 12, 2009

Good morning Chairman Price, Ranking Member Rogers, and distinguished members of the Subcommittee. Thank you for the opportunity to appear today to provide an update on the Transportation Security Administration's (TSA) efforts to improve surface transportation security through the public transportation (Transit) and freight railroad (Rail) grant program jointly administered and implemented with the Federal Emergency Management Agency (FEMA). I am pleased to be here today with my colleague, W. Ross Ashley, III, the Assistant Administrator for FEMA's Grant Programs Directorate; and representatives from two of our industry partners, Jack Eckles, Deputy Executive Officer, System Safety and Security, Los Angeles County Metropolitan Transportation Authority; and Bill Morange, Deputy Executive Director and Director of Security, New York Metropolitan Transportation Authority (NYMTA).

I would like to begin by thanking the members of the Subcommittee for your support of the initiatives of TSA and our stakeholders to improve Transit and Rail security. I especially want to thank the Subcommittee for the supplemental funding provided in the American Recovery and Reinvestment Act of 2009, P.L. 111-5 (Recovery Act), and the level of funding in the Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009, P.L. 110-329 (FY09 Consolidated Act) for grant awards for FEMA. These two Acts provide critical funding to our industry partners and enhance TSA's ability to coordinate strategic security efforts to address ongoing and emerging threats. TSA will be working expeditiously with FEMA and the eligible entities to award the additional funding in the Recovery Act to improve security while generating an economic benefit in the local area. We also look forward to working with our partners at the Department of Transportation to expedite the award of Recovery Act grant funding for Amtrak.

Transit Security Strategy

TSA's security strategy for Transit and all modes of transportation involves a risk-based approach that is flexible and capable of responding to evolving threats. We analyze intelligence

on a daily basis to ensure our strategy is focused on the most serious threats and to assist our stakeholders in implementing appropriate security measures in a cost-effective manner. We recognize that we cannot protect every person or all property against every possible threat to a system. Given the nature of the threats to Transit, we must manage risk consistent with what we understand of the threats, vulnerabilities, and consequences. We prioritize our resources to protect against the high-threat, high-consequence events.

The Transit grant program is an important part of TSA's security strategy. The grant program enhances our ability to focus on making high-risk Transit systems less attractive as targets and more secure for the traveling public. The grant program directly funds a host of critical security measures such as the forward-leaning deployment of visible deterrence--Visible Intermodal Protection and Response (VIPR) teams, explosives detection canine (Canine) teams, and trained individuals and equipment to conduct mobile screening of passengers and security surges. The grant program funds security training for front-line employees and law enforcement and public awareness campaigns to engage the public as force multipliers, important measures required by the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53 (9/11 Act). With other offices within the Department of Homeland Security (DHS), we collectively worked to tailor a behavior awareness, recognition, and detection training program for law enforcement officers protecting Transit systems. On a more permanent basis, the grant program makes Transit systems more secure by expanding the deployment of surveillance, monitoring, and detection technologies to improve intrusion and anomaly detection; strengthen access control measures; and otherwise add layers to harden facility security.

The success of our Transit security strategy begins with active stakeholder engagement. Because Transit systems operate in a much more open environment than commercial aviation, our success relies even more on the efforts and commitment of our stakeholders. We engage and communicate with Transit stakeholders on a regular basis through the Transit Policing and Security Peer Advisory Group, the Transit Government Coordinating Council, and the Transit Sector Coordinating Council. On a more informal basis, we actively encourage two-way communication between TSA and stakeholders. Through the Baseline Assessment and Security Enhancement (BASE) program, TSA compiled 55 Smart Security Practices to be shared throughout the Transit sector. The Smart Security Practices contain contact information for an official in the source agency that professional colleagues may consult for more information. Perhaps our most important exchanges with stakeholders involve ongoing classified threat and analysis briefings and the timely distribution of security information products and recommendations through the Mass Transit Security Information Network. Combined with the daily assessment work by TSA's Surface Transportation Security Inspectors, these efforts are continuously improving Transit security and the risk-based allocation of grant funding.

Regional Focus

Today the Transit grant program focuses on strengthening security on a regional basis. TSA believes that effective Transit security requires overall deterrence on a regional level. For example, Manhattan cannot be protected if potential terrorists have free access to a connecting Transit system in New Jersey. In the past, the grant process has awarded portions of the available funding to individual agencies, often in interconnected Transit systems, with the

agencies spending the funding as they separately deemed appropriate and not always with a full analysis of how the spending may or may not have improved security for the larger, interconnected Transit system.

The Transit grant program is now structured to reflect this regional approach by designating Transit regions in two separate groups based on risk. The highest risk Transit regions, comprised of the eight largest Transit systems of Atlanta, Boston, Chicago, Los Angeles, the National Capital Region, New York, Philadelphia, and the San Francisco Bay area, are designated as Tier I regions. In each Tier I region, DHS meets with a Regional Transit Security Working Group (RTSWG) to establish a Cooperative Agreement that identifies projects with the greatest security impact based on regional priorities. Tier II regions consist of other large urban areas and for these, DHS awards grants on a competitive basis considering the security impact of risk reduction projects.

TSA has shaped the grant process to begin with analysis of applicable intelligence. On a global scale, terrorists have successfully targeted trains, stations, and buses. There have been numerous credible threats to Transit systems in the United States. We focus resources on high-risk Transit agencies—those systems having dense passenger loads in confined areas, often involving underground locations, and where there is a history of a credible threat.

TSA gives priority to those projects with security measures that are low-cost yet highly effective, such as security training for front-line employees, security drills and exercises, deployment of Canine teams, mobile screening operations, security surge operations, intrusion detection technology, and access control measures. We collaborate with each RTSWG to identify, consider, and determine the grant submissions in their respective region.

Stakeholder Input

Our engagement with stakeholders is more than a process. Stakeholder input is truly valued and has shaped this process in many important ways. For example, two weeks after I accepted my position at TSA in the summer of 2006, I went to New York to meet with Bill Morange and his staff to ask for his Transit security insights. Chief Morange stressed that training, drills, Canine teams, and mobile bag screening were common practices of NYMTA and the New York Police Department. That same month, I traveled to Houston to ask Chief Tom Lambert how we might set up a Transit advisory group for TSA composed of key Transit security chiefs. Chief Lambert encouraged the TSA to hire someone who has “walked in [Transit agency] shoes” to lead the TSA Transit organization—and we did. We held subsequent discussions with Chief Lambert on how to streamline and structure the training grants to encourage more Transit agencies to release front-line employees for training classes. There are many more examples. Chief Joe Bober of New Jersey Transit advocated the approval of behavioral assessment training by DHS for Transit officers, and Chief John O’Connor from Amtrak worked with us in developing the operations protocols to allow increased Federal and local VIPR coordination and exercises.

Rail Security Strategy

Although Rail grants are a more recent addition to the grant program and are not awarded at the same funding level as Transit grants, the Rail grants are an important component of TSA's Rail security strategy. The principle element of TSA's Rail security strategy is to reduce the risk of Toxic Inhalation Hazard (TIH) chemicals in high threat urban areas. TSA works in close cooperation with the Rail industry to measure risk as a function of unattended standing TIH rail car time in high-threat urban areas. We track every TIH rail car using the Rail industry's Automatic Car Identification readers. These readers are accurate for mainline movements, but are less accurate in complex urban areas. The Rail grant program prioritizes awards to compensate TIH tank car owners and lessors for installing Global Positioning Satellite (GPS) devices on their tank cars. The GPS devices will ensure awareness of the location of the highest risk shipments and enable appropriate security response as such shipments move into or through high consequence urban areas. Security grants will also fund the delivery of security awareness and emergency response training for front-line employees, conduct vulnerability assessments, and develop security plans.

9/11 Act Implementation

I would also like to thank the Subcommittee for your support in providing additional funding to TSA for fiscal years (FY) 2008 and 2009 for the implementation of new regulations and activities authorized by the 9/11 Act. As set forth in the FY2009 TSA Spend Plan for 9/11 Act implementation, which TSA recently submitted to the Subcommittee, the funding will enable TSA to increase our security efforts in many critical areas. We are conducting additional vulnerability assessments for high-risk Transit, Rail, and over-the-road bus operators, expanding the Intermodal Security Training and Exercise Program, developing a transportation security Information Sharing & Analysis Center, hiring an additional 50 Surface Transportation Security Inspectors (STSI), and implementing other important activities.

The 9/11 Act, as this Subcommittee is well aware, directed TSA to implement over 100 programs, rulemaking actions, and activities relating to Transit and Rail security. We continue to make significant progress and we are pleased to report that many of the requirements from the 9/11 Act have been completed. Among those completed actions, I would like to highlight a few to illustrate our progress:

- expanded the existing security grant program for Transit to include Rail and other eligible entities;
- published an interim final rule covering the process for handling false statements made relating to security background check requirements for Transit and Rail workers;
- issued guidance to Transit and Rail operators for conducting voluntary security background checks;
- established and adopted security improvement priorities for Transit; and
- completed updates to Transit security assessments with assessments conducted by STSIs.

TSA is proceeding with implementing the remaining requirements of the 9/11 Act to further enhance surface transportation security. Although some of our ongoing rulemaking efforts have not been completed by the dates established in the 9/11 Act, we are taking action to accomplish some of the same goals through other efforts. For example, TSA developed and implemented a focused security training initiative under the grant program to encourage and expand the availability of the training to front-line workers. DHS revised the eligible costs under the grant program to allow coverage of overtime expenses and streamlined the application process to expedite awards for training. As a result, we have greatly expanded the availability of security training to Transit and Rail workers while we proceed with the formal rulemaking process. Through our ongoing efforts, including efficient use of our resources within our base funding, and your support, we are confident we will continue to enhance security for Transit and Rail, as well as the other modes of transportation.

Conclusion

TSA's Transit and Rail security strategy evolves through, and is improved by, constant interaction with our stakeholders. Our strategy is designed to make terrorist attack planning more difficult and less attractive by making the facilities and systems more secure. The grant program is an important tool in implementing our security strategy. We strive to conduct the process in a transparent manner by making the grant guidance, security project priorities, the process for allocating the money available, and other related information publicly available on the TSA website. We look forward to working with our partners at FEMA to make this grant process as streamlined, effective, and successful as possible. Mr. Chairman, thank you again for this opportunity and I will be happy to respond to your questions.

John P. Sammon

Assistant Administrator for Transportation Sector Network Management

As the assistant administrator for Transportation Sector Network Management, John P. Sammon leads a unified effort to protect and secure, through public-private networks, our nation's intermodal transportation systems, including aviation, rail, transit, maritime, cargo, highway and energy pipelines.

Sammon brings more than 25 years of transportation experience to his position, including management of customer networks for railroads, motor carriers, ocean carriers, petrochemical manufacturers, and ports and other public agencies.

Most recently, Sammon was the principal partner in a software venture, e-Carload. Before that, he spent many years in the railroad industry, working for both Conrail and CSX. As senior vice president at CSX he was responsible for a \$3.5 billion industrial products business unit with a staff of 500. Sammon has extensive experience with business development, operations and managing change.

Sammon has a Bachelor of Science in economics from Bucknell University and a Masters of Science in economics from Texas A&M University.

Mr. PRICE. Thank you, Mr. Sammon.
Mr. Ashley.

OPENING STATEMENT OF W. ROSS ASHLEY

Mr. ASHLEY. Good morning Chairman Price, Ranking Member Rogers, and members of the Subcommittee. I am Ross Ashley. I serve as the Assistant Administrator of the FEMA Grant Programs Directorate. Thank you all for the opportunity to appear before you today to discuss our efforts to secure our Nation's transit systems.

As you know, FEMA is the Department of Homeland Security's lead agency assisting State, local and tribal jurisdictions and regional authorities to prepare, respond to, and recover from natural disasters, terrorist acts, and other catastrophic events.

As part of that mission the Grant Programs Directorate in partnership with TSA administers a number of programs designed to enhance the security of surface transportation systems throughout the country. One such program is the Transit Security Grant Program, or TSGP. TSGP has evolved since its inception in 2005, and I would like to highlight a couple of the process improvements that have taken place. Let's talk for a moment about the risk-based process.

Practically 90 percent of the funds that have been mentioned earlier today have been applied towards the top eight Tier 1 transit systems in the country. This indicates the Department's commitment to provide necessary funding to those urban areas with the greatest risk.

In order to truly identify those high risk transit systems over the past few years, the Department has continued to make improvements to the risk methodology that we use. Four years ago the Department, for the first time, distributed transit security funds using multiple risk factors. Each subsequent year the Department has applied a more mature and consistent threat and risk analysis in determining allocations for those later year funds. Also, we have considerably improved our processes in terms of outreach which is another successful component of the Transit Security Grant Program. As you all have noticed in her recent action directives, one such directive is related to engagement with our State, local and private sector partners. The Secretary is fully committed to conducting regular outreach with these partners. The owners and operators of infrastructure are partners in this process and are vital to the well-being in the States and the urban areas which they serve. Thus, it is imperative for transit systems to be incorporated into a regional preparedness planning effort and to have regional strategies.

The Department believes that a regional approach is critical to overall preparedness. These strategies are intended to integrate individual agencies' needs into a regional perspective in order to identify transportation security vulnerabilities, and to focus Federal, State, and local funding.

This year in fiscal year 2009, the Transit Security Grant Program continues to build on the progress made in the past to institutionalize the risk-based regional approach used for the allocation of transit security funding.

One last successful component of this program is the Department's collaborative efforts which Mr. Sammon also mentioned earlier. From the development of program guidance to the application process, FEMA works and coordinates with numerous governmental and nongovernmental entities to ensure an appropriate level of subject matter expertise, and to solicit feedback from Federal, State, local and industry partners.

FEMA works with a number of DHS components, including TSA, the Office of Infrastructure Protection, the United States Coast Guard and the Science and Technology Directorate, as well as the Department of Transportation's Federal Transportation Administration and Federal Railroad Administration.

We have also worked closely with State and local transportation officials from across the country, as well as industry groups, including the Association of American Railroads and the American Public Transportation Association.

Before I conclude my statement, I would like to take a moment to illustrate how the successful evolution of this program through the use of risk-based allocations, outreach and collaboration has impacted real transit agencies and effectively mitigated existing and future threats.

Transit agencies in Philadelphia in fiscal year 2007 used funds on a regional project to create a transit specific intelligence analysis center. The center allows officials from Philadelphia and New Jersey to share information and analyze potential threats, allowing officials to take appropriate mitigation and prevention activities.

In fiscal year 2006, Portland's Tri-Met system created and began to administer an extensive front line employee training program. Through this effort, Portland's transit employees are trained on a recurring basis on security and IED awareness and principles of behavior assessment screening.

Most recently and very importantly, on November 23, 2008, TSA informed FEMA that a potential threat was identified against New York City's subway system. New York requested financial assistance for the rapid buildup of its police presence in the subway system, including deployment of specialized teams. In less than two hours the day before Thanksgiving, FEMA released over \$23 million in previously awarded fiscal year 2008 Transit Security Grant Program funds for New York in support of this operational need.

Mr. Chairman and Members of the Subcommittee, this concludes my testimony. Thank you and your staff for your support of FEMA's Grant Programs Directorate and the Department of Homeland Security. I am happy to answer any questions you might have.

[The statement of Mr. Ashley follows:]

The Honorable W. Ross Ashley, III

**Assistant Administrator
Grant Programs Directorate
Federal Emergency Management Agency
U. S. Department of Homeland Security**

Before

the

Subcommittee on Homeland Security

Committee on Appropriations

U. S. House of Representatives

March 12, 2009

Washington, D.C.

Chairman Price, Ranking Member Rogers and Members of the Committee, my name is Ross Ashley and I serve as Assistant Administrator of the Grant Programs Directorate within the Department of Homeland Security's Federal Emergency Management Agency. I am pleased to appear before you today to discuss our efforts to secure our Nation's transit systems.

FEMA is the Department's lead agency for preparing the Nation against terrorism, natural and other hazards by assisting States, local and tribal jurisdictions, and regional authorities to prepare, prevent, respond to, and recover from natural disasters, terrorist acts and other catastrophic incidents. As part of this mission, FEMA provides support to our Nation's emergency prevention and preparedness community through a number of different grant programs, training and exercise support, and technical assistance. Specifically, FEMA's Grant Programs Directorate, in partnership with the Department of Homeland Security's Transportation Security Administration (TSA) administers a number of programs designed to enhance the security of surface transportation systems throughout the country.

Transit Security Grant Program

Since the creation of DHS in February 2003, and subsequent authorization under the Implementing Recommendations of the 911 Commission Act of 2007, the Department of Homeland Security has awarded more than \$892 million specifically for the Transit

Security Grant Program since FY 2005 of which over \$789 million has been directed to the nation's transit systems in the eight Tier I urban areas.

In Fiscal Year (FY) 2003, under the Urban Areas Security Initiative (UASI), funding allocation decisions for transit systems were based solely on ridership, which at the time was the only reliable risk variable available. In FY 2004, the Department provided additional funds to 25 major transit systems through the UASI Program for additional security enhancements. For these funds, the Department added the additional criteria of track mileage to make final funding allocations.

Under the FY 2005 program, the Department for the first time distributed transit security funds using multiple risk factors. The formula for rail transit funding was based on: ridership, track mileage, the number of stations and credible threat data. Each subsequent year, the Department has applied a more mature and consistent threat and risk analysis in determining allocations for these later year funds. In its most simple terms, the weighted analysis combines a 20% threat component and an 80% vulnerability and consequence component. The latter component includes track mileage, underwater structures and ridership figures provided to us by the American Public Transportation Association. It also considers the presence of critical infrastructure.

Throughout the program development and application process, FEMA works and coordinates closely with numerous governmental and non-governmental entities to ensure an appropriate level of subject matter expertise and to solicit feedback from our Federal,

State, local, and industry partners. We work collaboratively with a number of DHS components, including officials from the Transportation Security Administration, the Office of Infrastructure Protection, the United States Coast Guard, and the Science and Technology Directorate, as well as the Department of Transportation's Federal Transit Administration and Federal Railroad Administration. We have also worked closely with State and local transportation officials from across the country, and with industry groups, including the Association of American Railroads and the American Public Transportation Association.

Since FY 2005, a major focus of the Transit Security Grant Program has been to establish and sustain a risk-based regional planning process to ensure that transit security priorities are considered in a systematic, risk-based manner. Regional Transit Security Working Groups are strongly encouraged to develop a Regional Transit Security Strategy. As the owners or operators of infrastructure vital to the well-being of the States and urban areas they serve, it is imperative transit systems are incorporated into regional preparedness planning efforts and have regional strategies. The Strategies are intended to integrate individual agency needs into a regional perspective in order to identify transportation security vulnerabilities and focus Federal, State and local funding. In addition, transit systems selected for funding under the FY 2005 TSGP were required to conduct a risk assessment and use this data to create Security and Emergency Preparedness Plans (SEPP) specifically to identify how the transit system intends to address shortfalls in the risk assessment. The Department continues to recommend and encourage transit entities

to revise, update and implement a Regional Transit Security Strategy as part of the FY 2009 Transit Security Grant Program.

A regional approach is critical to overall preparedness. That is why the Department strongly encourages all Working Groups to include representation from the applicable State(s) and urban area(s) served by the transit systems receiving funds, and strongly recommends that other transit agencies whose systems intersect with those of the grant recipients also participate in the Working Group process. In addition, for those transit operations that intersect with those of Amtrak in the Northeast Corridor and in Chicago, a representative of the National Railroad Passenger Corporation (Amtrak) should be included in the Working Group. Close coordination with Amtrak on the expenditure of funds for security enhancements at shared facilities is also encouraged.

The Regional Transit Security Strategy should serve as the integration point between the individual, risk-based Security and Emergency Preparedness Plan, and the overall security goals and objectives of a region. Therefore, the Strategy should demonstrate a clear linkage to the applicable State and Urban Area homeland security strategies developed. Security and Emergency Preparedness Plans and the Strategy provide a roadmap that serves as the basis on which funding is allocated to address regional transit security priorities, and the vehicle through which transit agencies justify and access other funding and resources available on a region-wide basis through other DHS-supported grant programs.

The FY 2009 Transit Security Grant Program builds on the progress made in the past to institutionalize a risk-based, regional approach to the allocation of transit security funding. Congress appropriated \$400 million for this program in FY 2009. In addition to the enhancements made since the program's inception, the FY 2009 program further refines the risk formula for the allocation of Transit Security Grant Program funds; encourage integration of the Working Groups and each region's Strategy with the existing Urban Area Working Groups and Strategies.

Since 2003, the Department's Transit programs were structured to help state and local responders maximize this federal funding.

Real World Impacts

On the afternoon of November 23, 2008, FEMA was informed by TSA that a potential threat was identified against New York City's subway system. New York requested financial assistance for a rapid build up of its police presence in the subway system, including deployment of specialized teams. On that Wednesday afternoon before the Thanksgiving Holiday, FEMA was, in under two hours, able to arrange for the immediate release of over \$23 million in previously awarded FY 2008 TSGP funds from the Treasury to New York in support of its operational needs.

Transit agencies in the greater Philadelphia area used FY 2007 TSGP funds to undertake a regional project creating a transit-specific intelligence analysis center. This center

allows officials from Philadelphia and New Jersey to share information and analyze potential threats, allowing officials to take appropriate mitigation and prevention action.

In FY 2006, Portland, Oregon's Tri-Met System created and began to administer an extensive, front line employee training program. Through this effort, Portland's transit employees are trained on a recurring basis. Training includes security awareness, IED awareness and principles of behavioral assessment screening.

I'd like to take a few minutes to walk you through the grant process, and how we develop and implement the TSGP.

Transit Security Grant Program Applications

Transit agencies eligible for FY 2009 TSGP funding are identified using a comprehensive, empirically-grounded risk analysis model. The risk methodology for the TSGP is linked to the risk methodology used to determine eligibility for the core DHS State and local grant programs. TSGP basic eligibility is derived from the UASI eligibility list and the Department of Transportation's list of the top 100 transit agencies, determined by ridership. Grantees are assigned to two, separate risk tiers, for which funding is allocated.

In the past, the Department has made TSGP awards to Governor-designated State Administrative Agencies who in turn award sub-granted funds to DHS-designated transit agencies. Pursuant to the Consolidated Security, Disaster Assistance and Continuing

Appropriations Act of 2009, FEMA will make direct awards to eligible transit entities for the first time in FY 2009.

Previous Executive branch policies required the use of a specific, web-based application process, government wide. This system, known as Grants.gov, presents challenges, particularly for first-time users, as it requires a multi-step application that can take several days. Specifically, first time applicants are required to apply for a Grants.gov password that is returned to the applicant upon determination of the applicant's eligibility for a particular grant. This often requires a waiting period as long as several days. Eligible entities attempting to submit applications near or at the application submission deadline have been locked out of this system. FEMA has addressed this issue through stakeholder outreach, education, technical assistance and, when necessary, allowing applicants to access FEMA's own Grants Management System for the purpose of application submission. We have also identified computer server capacity issues at the Grants.gov website that are being addressed. No eligible Transit Security Grant Program entity will be denied grant funding because of technical difficulties related to the grant application process.

Transit Security Grant Program Project Review and Approval

Project proposals under the TSGP are subject to a number of review processes. These processes include substantive, programmatic review to determine the eligibility of proposed expenditures and consistency with Department program priorities as outlined in the TSGP Application Kit and Program Guidance. Depending on the nature of a TSGP proposal, it may be subject to Environmental and Historic Preservation review as prescribed by law. This involves determining whether and to what extent a project proposal may adversely impact the environment or a structure or area that is protected under preservation laws and regulations imposed by State, local or the federal government.

As noted above, TSGP eligible entities are grouped into two, separate tiers. The review requirements for each Tier group are different in one respect requiring additional time for Tier 1 programmatic approval. Specifically, applications submitted by transit entities in the high risk Tier I are subject to project review and approval by the Transportation Security Administration. Approval is based upon TSA policies that place high emphasis on projects that address high risk scenarios and hazards. This ensures that the highest risk entities address the most critical, risk-based needs in their proposals. Lower risk, Tier II applications are subject to a competitive review undertaken by a multi-agency review panel. Proposals are reviewed and funded either in whole or in part, based upon consistency with the requirements and priorities contained within the TSGP Application Kit and Program Guidance. Tier II applications recommended for approval by the Review Panel are subject to further approval by an Executive Review Panel at FEMA and

TSA and final review by the Secretary. As there is not an opportunity for Tier II applicants to negotiate their proposals once submitted, the process through which Tier II grantees are allowed access to grant funds is typically faster than high risk Tier I grantees, whose awards are made through cooperative agreements negotiated with TSA.

FEMA and our TSA partners are addressing these issues through a simplified application process reducing information required in Investment Justifications, outreach to eligible entities to help provide process transparency and After Action Conferences to provide all stakeholders with a formalized forum in which to provide constructive feedback.

Environmental and Historic Preservation project review, when applicable, is an important step, designed to protect our national resources. FEMA is addressing delays this review may cause by conducting outreach to stakeholders explaining EHP requirements, allowing TSGP applicants to anticipate and address EHP-related issues pre-award. We have also strengthened our own internal protocols to track project review and status, and we are adding additional staff and are training existing staff to expedite the EHP review process. A recent change allows FEMA's Grant Programs Directorate program analysts to approve, on their own authority, categorical exclusions as allowed under the National Environmental Policy Act (NEPA), for such program activities as planning, organizational costs, training, exercises and equipment not requiring fixed installation. This single step has markedly increased our ability to make funds available to grantees for purposes that are not subject to NEPA requirements. Finally, GPD is also working with FEMA's Office of Environmental and Historic Preservation to develop a

programmatic, environmental assessment (PEA) tailored to our specific grant programs and grant funded projects to further simplify the NEPA review process. Finally, we have streamlined financial budget review by empowering grants management specialists to communicate directly with grantees to resolve any questions or concerns that may arise from the review. This simple step has contributed to increased efficiency in the release of funds to grantees.

While it is also true that state and local requirements, including both procurement regulations and local political leadership approval of TSGP grantee priorities, may contribute to a delay in the execution of program implementation, FEMA has and will continue to reach out to and work with stakeholders to assist them in identifying appropriate, local expertise as early as possible in the process. We will also continue our work in ensuring process transparency and facilitating the most rapid and effective program implementation possible. We look forward to future collaboration with our State, local and federal partners in making the Department's Transit Security Grant Program among the most efficient and effective programs aimed at increasing the public safety.

Mr. Chairman and Members of the Committee, this concludes my testimony. Thank you for your continued support for FEMA's Grant Programs Directorate and the Department of Homeland Security. I am happy to answer any questions the Committee may have.

W. Ross Ashley III

Assistant Administrator, Grant Programs



W. Ross Ashley was confirmed by the United States Senate in December 2007 and currently serves as the Assistant Administrator of the Grant Programs Directorate (GPD). Before assuming his position at GPD, Mr. Ashley served as the Chief Executive Officer of the National Children's Center (NCC), prior to which he was on the Board of Directors. During his time with the NCC, Mr. Ashley led all aspects of the agency including quality of care and financial management.

Prior to his tenure at the NCC, Mr. Ashley joined ChoicePoint in 2004, and served as the Vice President of Federal Government Affairs.

In February 2000, Mr. Ashley founded the Templar Corporation. Working with the National Institute of Justice (NIJ), The Templar Corporation began the development of sophisticated data integration solutions with a single purpose in mind: to improve public safety and security agency's capabilities to share information. Under Mr. Ashley's leadership, Templar products grew to support over 100 federal, state and local government agencies.

Prior to founding Templar, as the Director of Law Enforcement Technologies at ISX Corporation, Mr. Ashley was responsible for several information sharing initiatives for federal, state and local law enforcement agencies. He provided senior level consultation services to the National Institute of Justice on various information technology programs for the DOD/DOJ Joint Program Steering Group and external agencies such as DARPA.

Prior to joining ISX, Mr. Ashley served in a variety of private sector positions to include supporting the National Intelligence Community and providing high level operational support planning to the Secretary of Defense, Chairman of the Joint Chiefs and Secretary of the Air Force in intelligence collection planning and analysis, and operational combat assessments. Mr. Ashley is a retired Air Force Information Operations Officer serving both in the Virginia Air National Guard and the United States Air Force Reserves.

Mr. Ashley is a distinguished graduate of the Academy of Military Science, holds a BA from George Mason University and a MS from the Joint Military Intelligence College. He and his wife Lauren, and their four children reside in Arlington, Virginia.

Mr. PRICE. Thank you. Now we turn to the leaders from our major systems, beginning with Mr. Morange.

OPENING STATEMENT OF WILLIAM MORANGE

Mr. MORANGE. Good morning, Chairman Price, Vice Chairman Serrano and Members of the Subcommittee. My name is Bill Morange. I am the Deputy Executive Director, Director of Security for the MTA.

I joined the MTA in 2003 after having served 39 years-plus in the New York City Police Department where I retired as the Chief of the Organized Crime Control Bureau. Before that I was the Chief of Patrol and served as the Incident Commander down at Ground Zero on 9/11.

My role in the MTA is to ensure that the actions we are taking in light of September 11th, Madrid, London and Mumbai and other threats, prepared our organization to respond to terrorist and other emergency incidents and to provide as secure an environment for our customers as is humanly possible. I will talk about that and our relationship with the Department of Homeland Security and the Federal Government and what other security needs we look for as we go forward.

As you well know, the MTA is the largest transportation provider in the Western Hemisphere. We provide over 8 and a half million subway, rail and bus rides each day in the New York Metro area, roughly one-third of all transit rides nationally. Approximately 900,000 vehicles cross our seven bridges and two tunnels each day, carrying over 1.4 million passengers.

Certainly 9/11 was a traumatic event that happened in the New York Metropolitan region and our system was directly affected. But some of the things that we have learned from that day and as we move forward we should continue to do. Since then we have done many things internally and also externally in hardening and operational within the system.

Some of things that I do like to talk about that have been positives are working along with TSA and all the emergency drills that we have undertaken. I am a firm believer that the emergency drills are probably the most important thing that we can do. Six weeks prior to 9/11, we did a drill, and the OEM, Office of Emergency Management, for New York City at that time was in 7 World Trade. And the biggest thing about the drills was not everybody knowing what everybody else does, but everybody gets to know who is who. And when you respond up on the scene, Bill knows Mr. Price, Mr. Price knows Bill, and it is a lot easier to perform your function. And on that day we lost a lot of senior leadership, but we were able to move and do everything that we had to do to further protect the city. It was probably the first time I was really acquainted with the MTA, because when you come from a police department of 40,000 people you would never realize that we would need a lot of help to evacuate the city. That was the first time we called for buses and we used New Jersey Transit and we used other police departments from around the area.

The other programs I would like to talk about is see something, say something, keeping all our customers and people aware of what is happening out there and to make sure that they have a way to

contact us immediately and we have a way of responding back to let them know what the outcome was. I think the more informed public that you have, the better off you are. And I always say that the riding public is your best eyes and ears that are out there, because every day if you get in a train they sit in the same seat, take the same train, they know what belongs and what doesn't belong.

Another thing that we were able to accomplish through TSA and DHS was the training of our front line employees in which we feel is very important that they are also aware. Because they, like our customers know what belongs and what doesn't belong in those systems.

I would like to talk about before we go further, proposed recommendations that we feel will improve the process. Going forward, the MTA would like to emphasize a number of points that we believe will improve the Federal process. One, we believe the regional transit security program should broaden emphasis areas and have identified several areas where we think Federal funds are necessary. Consequence management, projects to enhance egress, lighting and signage, interoperable communication for our police and regional partners, backup power redundancy, and chemical, biological and radiological detection devices, which we have some deployed already in our system.

We look for consistency in the grant guidelines from year to year which will allow us to do more effective long-range project planning and better address our transit agency's 5-year capital security plans.

We need flexibility to use Federal funds for design project management and construction management tasks conducted by in-house forces. Presently these tasks are reimbursable only if they are done by third-party contractors. We feel that our in-house forces know the system better than others, and also we could do it at a lot less of a price and use the rest of those Federal funds for other areas that are well needed.

We need flexibility to fund all in-house flagging and track excess work on straight time. As of now it is in lieu of overtime because we are not allowed to use that with Federal funds, we are not allowed to put in for that. We support the creation of a one-stop shopping mechanism for better coordination between FEMA and TSA. The current process requires one agency to approve the funds and the other to approve the scope of the project. This causes delay in approving the grant package every year. In fact, we are still awaiting approval for funding under the fiscal year 2008 funding measure.

We recommend that our annual grant guidance be issued before the Federal fiscal year. This would enable grantees to address their security-related needs prior to the publication. Grantees would be able to submit applications at the beginning of the Federal fiscal year once appropriations are known. This would accelerate the review and approval process by TSA and FEMA and enable the transit agencies to advance their projects in a more timely manner.

Seven, we would like to emphasize the critical role that the State has in the grant process and encourage a more active role for the State administrative agency.

In developing the regional security strategy, we would like to propose the State SAA be formally part of the Transit Security Grant Program and chair regional transit security meetings, which we do now up in the New York area between New Jersey Transit, the MTA, NYPD, the Connecticut DOT, Westchester County.

And finally, the funding sources under the TSGP process are designed to support the security needs of the transit agency and their primary law enforcement provider. Allocations that are directed to local municipal law enforcement agencies have the potential for a negative impact on the core objectives of the grant program.

Thank you, and I would be happy to answer any questions that you may have.

[The statement of Mr. Morange follows:]

**Remarks of William A. Morange
Deputy Executive Director and Director of Security
NYS Metropolitan Transportation Authority
House Appropriations Subcommittee on Homeland Security
Washington, DC
March 12, 2009**

Good afternoon Chairman Price, members of the Subcommittee. My name is William Morange, Deputy Executive Director and Director of Security for the NYS Metropolitan Transportation Authority (MTA). I joined the MTA in 2002 after having served for 39 years with the New York City Police Department. I retired as the Chief of the Organized Crime Bureau and was Chief of Patrol – a roll i served in on September 11.

My role at the MTA is to ensure that the actions we are taking in light of 9/11, Madrid, London, Mumbai, and other threats, prepare our organization to respond to terrorist and other emergency incidents, and to provide as secure an environment for our customers as is humanly possible. I will talk about that, our relationship with Department of Homeland Security (DHS) and the federal government, and what our security needs are going forward.

As you may know, the MTA is the largest transit provider in the Western Hemisphere and is comprised of several operating entities:

- MTA New York City Transit (NYCT)
- MTA Long Island Rail Road (LIRR)
- MTA Metro-North Railroad (MNR)
- MTA Bridges and Tunnels (B&T)
- MTA Capital Construction (MTA CC)
- MTA Bus Company (MTABus)

We provide over eight and a half million subway, rail and bus rides each day in the NY metro area – roughly one third of all transit rides nationally. Approximately 900,000 vehicles cross our 7 bridges and 2 tunnels each day, carrying over 1.4 million passengers.

9/11 and the MTA

Certainly 9/11 was traumatic for the NY metropolitan region and our system. We were front and center at Ground Zero, with 3 subway stations directly serving the Trade Center site and hundreds of express and local buses serving its perimeter. It's likely that more than 80% of the Trade Center's 50,000 workers took one or more MTA services to get to work each day.

Despite one completely destroyed station and 4 others that were put out of service for as much as a year, not a single MTA customer or employee was killed or seriously injured in or on our system. On 9/11 our subways whisked tens of thousands of riders from the center of the World Trade Center site to safe locations north and south. Our buses and subways evacuated millions more from Manhattan Island. Our railroads took shocked commuters safely to their homes and returned with rescue workers who had no other way to get into the City to help.

Since then we have done much work, both internally and with our partners in New York City and New York State, the federal government and the broader transit industry, to assess the

risks of future acts of terror on our system and to try to minimize them. We are doing so through a series of capital and operating investments in the system and additional employee training for our 65,000 employees. Let me first talk about the capital and operating investments.

In 2002, with the assistance of the Federal Transit Administration, we conducted the first of a number of system-wide risk assessments, identifying \$2-\$3 billion in needs. We immediately launched a two-phase capital investment program to address those needs and harden our system. Phase I, comprised of \$720 million in investments is largely completed. While I cannot go into detail in public about many of the projects we have undertaken, one of the most visible initiatives included installing over 1,000 surveillance cameras and 3,000 intrusion detection devices in our subways and commuter rail facilities as part of a \$260 million Integrated Electronic Security System. We have also begun work on elements of our \$495 million Phase II, which takes, in turn, the next most critical projects.

We've grown our police department by nearly 40% to nearly 750 individuals at an additional cost of more than \$70 million (plus an additional \$37 million in overtime) since 2002 and in the same time period have added 261 bridge and tunnel officers at a cost of \$101 million. The bridge and tunnel officers inspect vehicles entering our bridge and tunnel facilities. We've spent over \$10 million to create and equip 50 bomb-sniffing canine teams and have added two MTA PD emergency service units at an additional \$6 million. Additional equipment, training and communication efforts have also proven to be very costly, but necessary.

Emergency Drills and Training

We continue to undertake real-life emergency drills on all parts of the MTA system. Much of the reason for our success in evacuating Manhattan on 9/11 was that our organization is and has been committed to preparing for emergencies. Our agencies have always done more than simply write volumes of emergency and response plans that sit on shelves. *We drill* those plans several times a year. The experience, lessons learned, and perhaps most importantly, the *relationships* forged in those exercises are tremendously valuable.

Each of our operating agencies prepare for emergencies regularly in terms of both physical drills -- with hundreds of participants -- and table-top drills. NYCT, the largest member of the MTA family, operates 8,000 subway and rail cars and 46,000 bus trips a day within New York City. Transit conducts four emergency drills annually in conjunction with the MTA PD, the LIRR, MTA Bus and MNR as well as the NYPD, the FDNY, the EMS and the Office of Emergency Management (OEM).

In addition, all key NYCT operating employees are provided ongoing formal "eyes & ears" training; fire protection & evacuation training; and DuPont Safety training. Over 45,000 employees have taken these courses and we are about to conduct a top to bottom update and review of those training courses in concert with our represented employees.

While Federal Railroad Administration regulations already require one full-scale drill annually, the LIRR conducts a minimum of 4 major full-scale emergency drills annually, including one in NY's Penn Station, the busiest railroad station in the country. Likewise, MNR conducts a number of drills during the year, including one in Grand Central Terminal. The carefully crafted emergency scenarios require emergency responders to demonstrate skills in

communications, fire fighting, rescue, extrication, hazardous material and first aid. Participants include county, village and town Police, Fire and EMS services throughout Nassau and Suffolk, Westchester, Orange, Rockland, Dutchess and Putnam counties in New York and Fairfield and New Haven counties in Connecticut.

Railroad emergency preparedness training is conducted at a number of locations, from Penn Station and Grand Central Terminal to major hubs such as Flatbush/Atlantic Ave Terminal, Jamaica Station, Grand Central Terminal, 125th Street, New Haven, as well as shop/yard facilities in New York and Connecticut.

MTA Bridges and Tunnels, which operates 7 bridges and 2 tunnels within NYC, the most notable of which includes the nation's longest suspension bridge, the Verrazano Bridge, has conducted over twenty multi-agency (MTA PD, NYPD, FDNY, MTA, OEM) exercises that have tested preparedness; response; inter-agency cooperation; perimeter security; IED mitigation; Hazardous Materials Spills; decontamination, and even power reduction scenarios.

Since 9/11 we've had other real-life opportunities to test what we do on a regional scale. When the electrical grids in the Northeast went out on August 14th, 2003, we – along with our partners in emergency preparedness throughout the region – were able to safely evacuate of over 400,000 riders from both underground and elevated parts of our system. We're proud that there were no customer or employee injuries in those instances – a truly amazing feat.

Engaging our Customers in Emergency Preparedness

While we're committed to aggressively training and drilling our employees for potential emergencies, we've also focused on making sure that our customers are aware of how they should respond in certain situations.

Through the creation of the internationally acclaimed "**If You See Something, Say Something**" campaign, we've informed our customers in print and on radio about being vigilant and in the process have enlisted their help by giving them an outlet to report suspicious activities: 1-888-NYC-SAFE. Public response has been extremely positive and we have shared our materials with dozens of transit systems and municipalities around the country and the globe.

In direct response to the lessons learned from the Madrid bombings – we both customized our ads to focus on packages left in transit vehicles and we've produced Customer Train Evacuation Brochures and internet-based evacuation videos that show how to properly evacuate subway and commuter railroad cars in an emergency. Printed copies of this information were distributed on our subway and rail cars. We've made both the printed material and videos available on our website, www.mta.info. In addition, we've made these videos widely available to local police departments, community groups and the public.

We also continue to supplement the more formalized training of our operating personnel with Employee Safety Guides for all our employees that tells them what to look for and how to react in emergencies.

Funding

While our needs are great and funding for many of these projects have not been identified, I would like to personally thank Congress and this Committee in particular for the financial support they have provided for the MTA and the transit industry in general.

Since 2003, MTA New York has received \$178.8 million in security funding that has helped us provide a safer environment for our 8.5 million daily transit customers – and the numerous vehicles that use our bridges and tunnels.

Through 2008, the MTA has been able to accomplish a number of projects that will provide safety to the riding public. Some of those include:

- Completion of NIMS Training for all of our operating agencies,
- Executing multi-agency table top exercise and emergency drills,
- Installing and upgrading Chemical Detection capabilities at Critical facilities,
- Installing CCTV systems and electronic access control,
- Installing Perimeter Security barriers,
- Procuring critical Emergency Response Equipment including two mobile command buses for the MTA PD,
- Expanding K-9 explosive detection teams,
- Increasing police patrol visibility through the MTA PD's Directed Patrol Program,
- Providing counter-terrorism Behavioral Assessment Training to MTA PD officers.
- Partnering with DHS in the Bio-watch Program.

The MTA has worked successfully with our regional transit partners through the transit security working group. Our partners include New Jersey Transit, the Port Authority of New York and New Jersey, Connecticut DOT, Westchester County and AMTRAK.

Through the TSGP funding program we have funded the following regionally based security projects:

- Interoperable communications,
- Interoperable communication protocols and,
- Development of regionally based response planning.

Commencing a pilot program with 2008 TSGP funding to develop a regional based terrorism suspicious activity reporting system database to monitor, track and respond to pre-attack activities. By sharing this information, the agencies can determine patterns and trends across agency boundaries.

Finally, we have taken training of our first responders to a new level concerning NIMS. The New York, New Jersey, Connecticut region are taking advantage of TEEX, a regionally based computer generated simulated attack program that assists first responders in planning and responding under the NIMS model. TEEX is a US DHS approved three and one half day training curriculum out of Texas A&M.

Your action to eliminate the local match requirement for the Transit Security Grant Program last year was much appreciated and we hope you can continue this element of the federal program as most transit agencies are already spending considerable local dollars on operating expenses such as:

- police salaries and overtime,
- canine units and anti-terrorist units, and
- improved security infrastructure in new and rehabilitated facilities.

For 2009, the MTA expects to receive additional funding for:

- Procuring equipment to support anti-terrorism teams,
- Purchasing explosive trace detective devices,
- Increasing our access control program to other critical facilities
- Expand infrastructure hardening measures at critical stations and bridges,
- Continuing the MTA PD "Directed Patrol" program.

These initiatives will enable the MTA to advance our overall security plan and reduce the vulnerability of our riding public.

Nonetheless, the need for additional federal dollars is still great and as you can imagine, we hope future funding will help us address the overwhelming needs we continue to have.

We have worked hard with Congress to increase federal transit funding from the \$65 million provided in 2003 and \$50 million in 2004 to the \$175 million provided in 2006 and beyond for transit, passenger and freight rail security, but clearly, with an identified national need of \$6 billion, more needs to be done going forward.

Proposed Recommendations to Improve Federal Process

Going forward, the MTA would like to emphasize a number of points that we believe would improve the federal process.

1. We believe the Regional Transit Security Program should broaden its emphasis areas and have identified several areas where we think federal funds are necessary:
 - Consequence Management projects to enhance; egress, lighting and signage
 - Interoperable Communications for our police and regional partners
 - Back-up power redundancy
 - Chemical/biological and radiological detection devices
2. We look for consistency in the Grant Guidelines from year to year, which will allow us to do more effective long range project planning and better address our transit agency's five-year capital security plans.
3. We need flexibility to use federal funds for design, project management and construction management tasks conducted by in-house forces. Currently, these tasks are fully reimbursable only if they are done by a third party contractor. Many transit agencies have in-house departments to do design work and project and construction management. Efficiencies are gained by utilizing these departments, whose personnel possess expertise in the individual transit system that most contractors do not have. The federally-mandated annual A133 Single Audit ensures that transit agencies have appropriate controls are in place to charge time correctly to grant-funded projects.

4. We need flexibility to fund all in-house flagging and track access work, which is currently fully reimbursable only when conducted by a third party. Individual agencies are best suited to determine needs for flagging, track access, etc., and in some cases, costs are driven by the Federal Railway Administration – Roadway Worker Protection Act, CFR Section #214.
5. We support the creation of a “One-Stop Shopping” mechanism for better coordination between FEMA and TSA. The current process requires one agency to approve the funds and the other to approve the scopes for the projects. This causes delays in approving the grant package every year. In fact, we are still awaiting approval for funding under the FY 2008 TSGP funding measure.
6. We recommend that the annual grant guidance be issued before the Federal Fiscal Year. This would enable grantees to address their security related needs prior to its publication. In addition, grantees would be able to submit applications at the beginning of the Federal Fiscal Year, once appropriations are known. This would accelerate the review and approval process by TSA/FEMA and enable the transit agencies to advance their projects in a more timely manner.
7. We would like to emphasize the critical role that the state has in the grant process and encourage a more active role for the State SAA in developing a regional security strategy. We would like to propose the State SAA be formally part of the TSGP and chair Regional Transit Security meetings. They should be involved in the process and to receive TSGP funding.
8. The funding sources under the TSGP process are designed to support the security needs of the Transit Agency and their primary law enforcement provider. Allocations that are directed to local municipal law enforcement agencies have the potential for a negative impact on the core objectives of the grant program.

There are more issues that we hope to address with your staff as we go forward, but let me conclude by thanking you once again for your personal support, concern and interest in helping us address these critically important needs. Please be assured that we at the local level are doing a tremendous amount in this effort and we need the federal government to continue to be a full partner going forward. I would be happy to answer any questions you may have.

#

William A. Morange
Metropolitan Transportation Authority
Deputy Executive Director/Director of Security

The Metropolitan Transportation Authority appointed William A. Morange, a 39-year veteran of the New York City Police Department, as MTA Deputy Executive Director and Director of Security in June 2003.

As Director of Security, Mr. Morange supervises security for the MTA's vast transportation network consisting of New York City Transit, Metro North Railroad, Long Island Rail Road, Long Island Bus and MTA Bridges and Tunnels. His responsibilities include coordinating MTA Police security efforts with the NYPD, the FBI, State Police, National Guard and the Department of Homeland Security. Director Morange also oversees the MTA's \$600+ million capital program dedicated to security enhancement.

Director Morange began his law enforcement career as a police officer in 1964 and was promoted through every uniformed rank to Chief. Before his appointment as MTA Director of Security, he worked as the NYPD's Bureau Chief for Organized Crime Control where he worked in close conjunction with Federal law enforcement agencies. Prior to that position, Mr. Morange was Chief of Patrol of the NYPD responsible for all uniformed patrol functions in the City. Both as Chief of Patrol and before that as Chief of Special Operations, Morange had extensive experience with the NYPD's infrastructure protection, and terror preparedness and response function.

Director Morange holds a B.A. in Professional Studies from the State University of New York. Mr. Morange and his wife Dianna live in Rockland County, have three grown children and five grandchildren.

###

Mr. PRICE. Thank you, sir.

Mr. Eckles.

Mr. ECKLES. Good morning, Mr. Chairman and members of the subcommittee. Thank you for this opportunity to speak before you on matters that are very important regarding the Transit Security Grant Program.

The L.A. MTA is the third largest transit agency in the United States, and we serve multiple roles as a regional transportation planner, the coordinator, the designer, the builder, the operator of the country's most populous county in the United States, more than 13 million people. One-third of California's population live and work within our 1,433 square mile service area.

Allow me to say that Secretary Napolitano stated much of what we would like to have happen with this DHS and TSA in her first action directive, as quoted by the chairman, under the State, local and tribal integration, immediately plan for an accelerated process for soliciting and collecting input from our local partners on how to improve the programs and processes of DHS.

A brief overview of our program to date is that we have received approximately \$24½ million of the over \$1 billion that has been allocated nationwide. The Transportation Security Working Group in the greater Los Angeles region had its initial growing pangs at the beginning, but this group has developed into an extremely cohesive and cooperative organization. We honestly feel these funds have helped to obtain some initial successes in addressing capital investment needs for hardening our critical infrastructure and the extensive creation and implementation of transit-specific awareness and response training and exercises.

It is important for me to point out that this grant program is considered by our group to be vital in order to better secure our systems, especially given the current economy in the Nation, in which most agencies are struggling to meet basic operating expenses.

I find that the funding for the Homeland Security grant program is critical for the protection of this Nation's vital transit infrastructure, the public transit agency, and our riders. This grant program has allowed our agency to develop security programs we would not have been able to obtain any other way. We believe we have spent the taxpayers' money in the best possible way within the restrictions and limitations given to us. However, we believe it can be and should be better.

Allow me to provide a chronology of events that have developed over time that illustrate our working group situation, but also let me say that while I do not want to engage in attribution of areas where the process has seemed to have gotten in the way of progress, I do believe that the Subcommittee must have a clear understanding of how certain procedures impact our ability to execute the intent of Congress as we strive to deliver these Homeland Security grant funded projects and programs in our local areas. There is only one purpose behind my testimony before this subcommittee, and that is to contribute to improving the program for the people we serve.

I will start out by saying that in fiscal year 2006 there was clearly undefined and confusing roles and responsibilities. Project re-

view and approval is cumbersome and difficult. This two-grant authorization notice, to want to approve your grant and then somewhere down the road after multiple reviews you get a second grant that says, oh, by the way, you can now spend down on it.

2007 was a pretty good year for us in terms of the grant process. However, the supplemental funding was fraught with problems. TSA's interference with our contracted law enforcement agency by dealing with them directly and granting them part of the supplemental funds in advance. During our investment justification approval meeting TSA made an impromptu 8-hour challenge to our transit security document, which they already possessed, already understood, but never read.

Constant reviews and rewrites by a, quote, review panel, who nobody has explained to me to this date who that is, but I only talk to one person and that is a grant analyst. I don't talk to anybody in a review panel. Requiring first simplification and then they come back and ask for more information and then they come back and ask for clarification of the information we have given them.

TSA was supposed to have held a secure briefing in 2007 after everybody had submitted their application for a security clearance, but they failed to process the application. They then turned the briefing, which people worked around their schedules because the American public transportation annual conference was scheduled that same week. It turned into a self promotion session about how ask us about how great TSA was doing with the grant program.

TSA didn't even bother to provide a sanitized version of the briefing to the agency since they couldn't get them their clearances. TSA official answering questions about grant guidance stated the grant guidance did not need to be followed and that TSA would take care of each unique situation.

TSA responded to a question about cost overruns for operational packages and the transit agency responsibility for the cost of those overruns. They replied, it would simply not be a problem. However, the FEMA member in attendance countered that in an audit the transit agency would be accountable for the overruns for the guidance and the language of the grant needed to be changed. It further stated only an information bulletin can make that change.

Inaccurate grant authorization notices for amounts not requested, in one case to \$1.6 million above and beyond what the agency asked for.

At another TSA meeting that turned into 6 hours of what training members of our region's agencies had received regarding terrorism awareness. They wanted names of courses, numbers of employees, including front line and other personnel, dates, where the future plans for training are, who is teaching and planning these courses, what is the sustainment plan for training without any prior notice that they were going to request this information.

Now mind you, I have an agency that has over 9,200 employees. I can only imagine what New York's employee status is. This was followed by questioning all of the region's projects except the operational packages, which were preapproved.

TSA was asked questions about operational package equipment was not eligible according to that grant guidance. Their response was to unilaterally decide that it would come out of the base

amount of 2007, which the agency had already divvied up and submitted their investment justifications with their budgets. We had to go back and review them, rewrite them, and reallocate to cover the equipment costs.

In 2008, TSA decided that their member was going to be a co-chair. In our region we don't have a chairman. We have a cooperative working group that spreads the dollars amount and allocations based upon project needs and demands of the regional security strategy as dictated by TSA.

On top of that they included by name the two contracted law enforcement agencies in our region to sit as members at our table and authorized them to draw down on the funds as a member, further diluting the allotment of money we get.

They also authorized them to be the approver of our agency's security plans. Our contracted law enforcement agency is now the one who has to approve our security plans. They also had to certify and review all of our projects. The operational packages submitted made the law enforcement agency a sub-grantee recipient of the transit agency, thus making us responsible for what the law enforcement agency does or fails to do.

TSA went on to state the law enforcement agencies didn't have to approve the agency's plan and that we could just simply line through "approve" and write in "concur". But to this date they have failed to give us an information bulletin to that effect.

Also, 2008 was the year that they developed a scheme to group projects, and of course their training and their operational package were at the top of that list given the highest point value. And those in infrastructure protection and prevention were put at the lowest category and given the lowest score. So if you didn't submit a project that met some numerical threshold, which we were never told or explained about, our project wouldn't be approved and our money would be allocated to another region.

2009, we went to the after action conference that TSA put on in the hopes that we could clarify and explain what our problems with the grant process were. They had scheduled it so far down into the system the grant guidance had already been written and nothing had changed in the 2009 grant guidance. Even though the entire year of 2008 we had explained the problems we had faced, nothing was changed.

This year they added a grant guidance language and included an agency requirement for the sustainment of the operational package 5 years beyond the grant. When we went on requesting clarification as to what that sustainment plan requirements were, our law enforcement agency, our contracting law enforcement agency receives the e-mail saying, the expectation is that the knowledge and capability would be sustained in some way for the transit agency and transit security in anti-terrorism although not strictly required. However, when we requested that information bulletin for that kind of clarification, none has been or was forthcoming. That is not to say we don't consider this program important. Otherwise I would not be before you today.

We do have recommendations and I believe these recommendations are important. I heard it said that there is contact with peers. Well, I also heard my commander and my contract law enforcement

name mentioned. To this date there has been no contact with me, the transit agency representative to have that kind of input, that kind of peer. I believe the recommendations should be an industry peer, not a law enforcement peer, review of the grant guidance development from year to year.

I believe they should utilize the threat and vulnerability assessment that Congress paid for in every agency. To date we have not been able to utilize that threat and vulnerability assessment to develop projects that effectively reduce our risk as determined by the audit. Detection response and recovery projects, including chem/bio, should be included.

As stated earlier, maintenance and administration costs hardly begin to touch the costs that we incur to manage these projects. 2.5 percent does not come close to anything that it costs our agency to manage this cumbersome and difficult process.

Transparency and grant allocations. They say there is a risk-based empirical formula, but I don't supposedly have the clearance to know what that is. Ladies and gentlemen, I am a lieutenant colonel in the United States Army Reserve. I have a top secret, sensitive compartmentalized information clearance. And I can't find this out? We want more transparency, ladies and gentlemen.

Grant program management, it should be either TSA or FEMA, not both. It has created a tremendous amount of confusion and a tremendous amount of delay. More predictability and flexibility in implementing priorities, that goes along primarily with the industry peer review panel, decreased emphasis on operating initiatives. We have an open system, and we need to harden it, and we can't buy enough people to secure it. So we need to implement those things that the threat vulnerability assessment says we need to expedite the approval process.

Ladies and gentlemen, we have one agency in our Transit Working Group that is still waiting on its approval for a 2006 grant because they keep getting the grant number wrong. We clarified last October going back to their after-action review, we got many of those cleared up right then and there, but we still have problems. To date, the 2008 investment justifications, some of them are going on their fourth review.

We also believe that TSA should only contact the transit agency's designated representative. The investment justification process should be more streamlined. I have over the years of this grant development one of my project managers having been in the process long enough wrote 54 pages of an investment justification hoping to avoid write, rewrites, clarifications and drawing this process out longer than it needs to be. Unfortunately, it hasn't worked.

Lastly, we all know the 9/11 Commission Report cited failure of imagination as one of the most significant shortcomings in security before the terrorist attacks. Also the Office of Homeland Security's mission statement for the transportation system sector states, "Continuously improve the risk posture of Nation's transportation system." And to further this position DHS's own sector specific plan, "Describe the security framework that will enable the sector stakeholders to make effective and appropriate risk-based security and resource allocation decisions."

Our region supports these ideals and seeks to enable them in a flexible and manageable way. We know and understand the asymmetrical threat we face; we in our own system know this best.

As an experienced battlefield commander myself having served in Iraq, I know the threat we face as do many others who work in our industry. We need to be allowed to influence our agency security destiny with the funds the American people have given us.

In summary, I would like to say that to my agency and our region would like to see a reformed Transit Security Grant Program that encourages and supports imagination and innovation at the local level in executing the intent of Congress, in securing public transit as a national critical infrastructure asset. In order to achieve this goal we need maximum flexibility and discretion at the local level to operate within a broad, but well-defined program and grant guidance from TSA.

Thank you, Mr. Chairman. I will be happy to answer any of your questions.

[The statement of Mr. Eckles follows:]

Congressional Testimony By
Jack Eckles, J.D.
Deputy Executive Officer, System Safety, Security & Law Enforcement
Los Angeles County Metropolitan Transportation Agency
for the
U.S. House Appropriations Committee
Subcommittee on Homeland Security
March 12, 2009

Good morning, Mr. Chairman and members of the subcommittee. Thank you for this opportunity to speak before you on the important matter of transit security grants.

I would like to start off with just a little bit of background on my agency and how we are engaged everyday in homeland security. With nearly 490 million annual boardings, the Los Angeles County MTA is our nation's third largest public transit agency. Metro employs more than 9,200 people in a broad range of technical specialties and services ranging from Metro Bus and Metro Rail operators and mechanics to construction engineers and safety inspectors, from transportation planning professionals to customer information agents.

We are unique among the nation's transportation organizations in that we serve multiple roles as the regional transportation planner, coordinator, designer, builder and operator for the country's largest and most populous county. More than 13 million people - one-third of California's population - live and work within our 1,433-square-mile service area.

Allow me to also say that Secretary Napolitano stated much of what we would like to have happen with DHS and TSA in her first Action Directive, January 12, 2009 where she states under State, local and tribal integration: "Immediately plan for an accelerated process for soliciting and collecting input from our...local...partners on how to improve the programs and processes of DHS."

Therefore, along that line, I would like to provide you a brief overview of our transit security grant experience to date. Since 2003, Los Angeles Metro has received approximately \$24.5 million of the \$1 billion that has been allocated nationwide. However, we have utilized those dollars to maximum effect within the restrictive guidelines as determined by the Transportation Security Administration (TSA). The Regional Transportation Security Working Group (RTSWG) for the Greater Los Angeles Region had its initial growing pains as they attempted to shake out and shape how the group would work within a shared arrangement of grant funding. Over time, this group has developed into an extremely cohesive and cooperative organization.

We honestly feel that these funds have helped in obtaining some initial success in addressing capitol investment needs for hardening our critical infrastructure and the creation and implementation of extensive transit specific awareness and response training. Unfortunately, for the last 3 grant cycles, more and more emphasis has been placed on training and awareness and less and less on hardening our facilities. Additionally, there have been more and more conditions placed upon the RTSWG in order to obtain funding, which I will address soon.

It is important for me to point out that this grant program is considered by our group to be vital in order to better secure our systems, especially given the current economy in which most agencies are struggling to meet basic operating expenses. It has become even more critical in California when you add that the recent budget that was passed in our state completely suspended the State Transit Assistance program for local agency transit operations. This situation has been compounded by the fact that the State has, for at least the past two years, raided the fund for other purposes to meet the State's budget shortfalls.

I find that the funding for the Homeland Security grant program is critical for the protection of this nation's vital transit infrastructure, public transit agency, and their riders. I, like all other recipients, believe there should be more dollars available, but the realities are quite different. However, agencies cannot afford the amount of money required to secure an entire open system from a level of threat that could not have been foreseen in this country prior to 9/11. With the current state of our nation's economy, we may not be able to afford these capital improvements with local funds for the foreseeable future.

This grant program has allowed our agency to develop security programs we would not have been able to obtain any other way. And we believe we have spent the taxpayers' money in the best possible way within the restrictions and limitations presented to us.

However, we believe that it can and should be done better. We have run into some hurdles and some downright obstacles that make the current program difficult at best to address each agency's particular needs.

Allow me to provide a chronology of events that have developed over time that illustrate our working group's situation:

Let me first say that while I do not want to engage in attribution of areas where the process has seemed to get in the way of progress, I do believe that this subcommittee must have a clear understanding of how certain procedures impact our ability to execute the intent of Congress as we strive to deliver these homeland security grant funded projects and programs in our local areas. There is only one purpose behind my testimony before this subcommittee and that is to contribute to improving the program for the people we serve.

FY 06: There were undefined/confusing roles and responsibilities (grant staff vs. agency security staff to TSA-Grants & Training-State Administrative Agency/deadlines and guidance clarification. It was extremely difficult to understand who was responsible for what (see Concerns Regarding Homeland Security Grant Guidelines for FY 06).

Project Review and Approval is cumbersome and difficult; a two Grant Authorization Notice (GAN) system was instituted by TSA grants personnel. The 1st GAN, we were told, was only to "obligate and expend" grant funds, but it did not authorize the agency to draw down the funds. The 2nd GAN then authorized the drawdown of funds, but in many cases the 2nd GAN was issued after countless reviews and revisions that when the 2nd GAN arrived it was so far into the grant performance period that the grant period had less than 6 months left with no automatic extensions provided. This was particularly true of the 2006 grant cycle. Many of the

grants did not get the 2nd GAN until October of 2008 when the grant period of performance was to end December 31st. Additionally, this was only done after the Grant After Action Conference when, as in our case, we personally had to travel to D.C. to make our complaints in person.

During this period we still had an agency within our group that has not received its GAN to spend down on a correct project amount. It authorized an incorrect amount, they were given inconsistent information, and referred back and forth between TSA personnel and FEMA personnel (see Fiscal Year 2006 Transit Security Grant Program, Standing Issues FEMA/TSA, Southern California Regional Rail Authority).

FY 07: This base year funding did not seem to be as difficult as the previous year. Unfortunately, the supplemental funding was fraught with problems. In that year's supplemental allocation, our region received an additional \$4.3 mil to the base allotment of \$7 mil. Upon notice, our agency met and developed our projects and began preparations for submission of our investment justifications (IJ's) (see also FY 07 Transit Security Grant Program (TSGP)-Chronology).

By mid-year, we met with members of TSA in what initially was to be a review of our IJ's for the base amount. It ended up being an impromptu 8 hour long briefing on the region's security strategy. There was much time spent on discussing and explaining our security needs. The frustrating fact of this meeting was that the information was already contained in the Regional Transit Security Strategy document we were required to develop and that was already submitted to TSA. These TSA members admitted they had received the document but had chosen not to read it beforehand. It was at this point that TSA was well aware of our region's needs and that they were based upon the various Threat and Vulnerability Assessments TSA had paid millions of dollars to develop.

The following month, we received news from "the review panel" that our IJ's were too technical and needed simplification so an average person would understand them. We were instructed to ignore the ½ page limitation on the IJ templates. Yet we continued to receive demands for clarification and correction before we could receive our spend-down GAN's, which is the constant source of delays. When we gave them simplicity, they asked for more technical details and then vice versa. We would receive requests for clarification such as what is meant by "ongoing surveillance" for cameras, "slave over to video" or "emergency telephone" and even "multi-agency", which in this last instance was directly followed in the sentence in question with "(Fire, Urban Search and Rescue, Law Enforcement, and SWAT)".

August of 2007 was the month our region received news that we would be getting our supplemental amount. However, we received some disturbing information that a member of TSA had met with Metro's contract law enforcement agency privately and without the region's knowledge. In that meeting, it was learned that this member had directed that agency to apply for half the supplemental amount for an "Operational Package" (O-Pack) and it would automatically be approved. Additionally, we learned that ours was not the only law enforcement agency across the country to which this direct offer was made. We had strenuous objections to that action and felt that it undermined our collective regional transit security efforts and was counterproductive.

In October, TSA had scheduled a "secure" briefing to inform agencies across the country about current intelligence regarding threats to mass transit. This required all participants to fill out documents for a security clearance in order to attend. The invitations were for the CEO's/GM's of the respective agencies. However, TSA failed to realize that the date of the briefing coincided with the annual American Public Transportation Association conference. Even upon early notification of this problem, TSA did not reschedule. At TSA's briefing, participants were notified that no clearance had been granted and TSA used the meeting to promote how well TSA was doing to address security threats nationwide. When asked directly about specific threats to our systems, the response was simply a remark of "If you knew what we knew, you would understand." TSA did not even make an effort to deliver an unclassified, sanitized version of threats to mass transit systems (note: the following year a member from DHS informed us that the information TSA was referring to related to concerns attached to the Madrid and London bombings and the tactics used, information which was readily available in open sources). Later on in the briefing, a TSA official answering concerns about the grant guidance stated that the grant guidance did not need to be followed and that TSA would take care of each unique situation.

In late October, the region met with TSA and FEMA grants personnel to go over our IJ for the supplemental funding. However, the following eight hours were again spent explaining what our security strategies and training levels were. This was used to somehow convince the region that we should support giving up over \$2 mil of the supplemental funding for O-Packs that had already been decided in secret. TSA spent several hours attempting to convince the regional members of the benefits of O-Packs. The regional members knew that this was a foregone conclusion and did not resist, but questions did persist. A question arose about the transit agency having to cover any cost overruns of the O-packs since the funding ownership was with the transit agency and not the law enforcement agency. The TSA member simply stated that would not be a problem. However, the FEMA member stepped in and stated that in an audit, the transit agency would be accountable for the overruns per the guidance and the language of the grant needed to be changed. He further stated that only an Information Bulletin (IB) could change the grant guidance.

It must be noted here that this is a recurring problem with TSA in that they have made promises or exceptions for individual agencies but have not furnished an IB to cover their statements.

During this period, issues with another agency within our working group were again plagued with inaccurate GANs for drawing down funds. In this instance, from February 08 until October 08 the problem persisted. As part of that year's supplemental funding, the agency received a GAN for their project but it was addressed to their contracted law enforcement provider. In March of 08, the California Office of Homeland Security, our State Administrative Agency (SAA), received a GAN for over \$1.6 more than this agency had requested for the project. In July, FEMA instructed our SAA to issue an award letter for that incorrect amount. Later that month, the transit agency officially refused to move forward on the incorrect amount, citing concerns about being bound to a legal document with an amount they and the Federal Government knew to be incorrect (see Fiscal Year 2007 Transit Security Grant

Program (TSGP) Supplemental Funding, Subgrantee Period of Performance, October 1, 2006 through June 30, 2010, Standing Issues FEMA/TSA, Orange County Transportation Authority).

In November, TSA had requested a meeting to go over the IJ's for the base year and supplemental grants dollars. At this meeting, TSA yet again delved into what training members of the region's agencies had received regarding terrorism awareness. The details they required, without any prior notice, were:

Name of the course(s); number of employees, including frontline and other personnel; dates; what were the future plans for training; who was teaching and planning to teach these courses; and what was the sustainment plan for this training...with or without Homeland Security Grant funding.

Once that was completed, TSA went on to indicate the need for further clarification on IJ's submitted on projects that only addressed hardening facilities and not O-Packs, training or training development. These clarifications only addressed why they were important to the agency in protecting their infrastructure.

Lastly, at this meeting it was explained to TSA that equipment for the "pre-approved" O-Packs was not eligible in the supplemental. TSA then unilaterally decided it would come from the Base FY 07 TSGP funds and wanted to reallocate funds within the previously submitted investments. The regional members wanted to discuss in a closed session how it was going to reallocate the funds, but the TSA member, as the grantor, insisted on being allowed to participate. The regional members insisted he leave and the State SAA supported our recommendation and assisted the TSA member out with them in order that the regional members discuss the project cuts in private. After the cuts were decided and the TSA and State SAA members were allowed to return, TSA unilaterally announce to the regional members that the FY 08 Grant Guidance will contain language that TSA will be a Co-Chair in the RTSWG.

FY 08: Upon receipt of the grant guidance, there was in fact a notice that not only was TSA a "Co-Chair" for the region, but that the two contracted law enforcement agencies in the region were specifically named as sitting members of the region, entitling them to direct grant funding (see TSGP Grant Guidance FY 2008, pgs. 1,2, 3 & 16). In addition, the guidance went on to include that the contracted law enforcement agency had the authority to approve the contracting agency's Security Plans and also to certify the review of their projects (see TSGP Grant Guidance FY 2008, pgs. 1, 2 & 3). Lastly, any O-Pack project submitted made the Law Enforcement Agency a Sub-Grantee/Recipient of the transit agency thus holding the agency accountable for what law enforcement does or fails to do. We officially notified our TSA grants representatives and our State SAA about the inherent conflict of interest these additions created. We also notified them that the idea of TSA being a "Co-Chair" was not acceptable in a Working Group that does not have a Chairperson to begin with, that all members sit as equals to put forth their projects within the grant funding available. They continued to insist that these agencies have a seat at the table as members. TSA went on to state that the law enforcement agencies didn't have to "approve" the agency's plans and that we could simply "line through

APPROVED and hand-write in CONCUR". We stated this was not acceptable and requested an IB to this effect, but to this day we have not received one.

This particular point coincides with a new scheme for what categories of projects were to be submitted. The new scheme established grouped categories of projects; training, public awareness, and O-Packs being in the top group (see TSGP Grant Guidance FY 2008, pgs. 7 & 8). Infrastructure hardening projects fell into lower groups, 2, 3, and 4. Then each group received a score value; group 1 getting 4 points, group 2 getting 3 points, group 3 getting 2 points, and group 4 getting only 1 point. Your project would then receive a score and if the score was too low (whatever that score was, as we have never been told) your project would be rejected and your region's project money reprogrammed to some other region. In this regard, TSA turned a dedicated Tier I Grant Funded program into a Tier II-like competitive grant type program if your agency did not choose a group 1 or 2 project. Additionally, TSA's grant guidance also states that funding is "Risk Based" by an "empirically-grounded risk analysis model" and consultation with our agency (see TSGP Grant Guidance FY 2008, pg. 6). However, we were and are not aware of any consultation about project types and when we asked TSA what our agency's risk analysis and score was, no response was ever provided nor an explanation of how it was derived except to say that it was classified.

During this grant cycle, our region decided that we would work at developing and selecting Group 1 & 2 type projects, attempting to squeeze our needs into these categories or face losing grant money. Though our projects have been given the first GAN, we continue to go through the difficult re-write process and on some projects we are on our 4th revision.

FY 09: In the middle of 2008 there was to have been an After Action Review (AAR) of the FY 08 grant cycle, whereby agencies could voice their concerns with that grant year and provide valuable input for the FY 09 Grant Guidance. The date was initially set and to be held in Florida. Unfortunately, Hurricane Ike struck and the dates were reset and given new locations. This time there were to be two AAR's; one in Seattle and one in Washington D.C. Unfortunately, the dates were set too far out (October) to have any impact on the formulation of the FY 09 Grant Guidance. Our region, though on the west coast, opted for D.C. in the hopes that "higher-ups" in TSA would be present. That did not occur. Instead, TSA staff in attendance included two people who had no authority to effect change. Our concerns were to be noted and taken to those who could effect change, yet in the FY 09 Grant Guidance, nothing had changed. To our disappointment, all issues, concerns and recommendations that were raised throughout the previous grant year were never implemented or addressed.

The FY 09 grant year was also the year that the State SAA's were removed as the Grantee. However we have determined that the relationship our working group has with the State is very cooperative and supportive. We continue to work with them in managing the grants program in an advisory capacity. Additionally, this year's grant guidance included more specific language about an agency's requirement for sustainment of an O-Pack for 5 years beyond the grant period (see TSGP Grant Guidance FY 2009, pg. 32). When requesting clarification about whether that was a requirement for just a plan or would the agency be obligated to actually maintain the project for 5 years beyond the grant, our contract law enforcement agency received an email reply stating "The expectation is that the knowledge and

capability would be sustained in some way for transit security and anti-terrorism, although not strictly required.”(see email Eckles, Jack, dated December 30, 2008 4:49 PM). However, when we requested an IB, none has been forthcoming and we have since withdrawn our IJ for an O-pack in the FY 09 grant cycle.

VIPR teams: Transit Security Inspectors (TSI’s) participate in VIPR exercises at Metro and throughout the region. They also provide an unannounced, high-visibility presence in a mass transit or passenger rail environment. These VIPR teams mostly act as patrollers who monitor suspicious activity and whose presence may deter terrorist activity. They are extremely useful in augmentation of existing personnel within a transit system. However, there are too few teams available for most of the events and activities for which they are most needed. This has also been pointed out by DHS’s own Office of Inspector General Report, dated February of this year. Throughout a particular year, due to their limited number, they are primarily scheduled for planned major events, such as the Rose Parade/Bowl, Los Angeles Marathon, or the Academy Awards. The remainder of their appearances is infrequent and not significant enough to have a major impact on deterrence within the region or our system. More teams would of course be better with an increase in coordination and notification to the agency and not just law enforcement.

Recommendations:

-Agency Ridership #'s in Tier I, qualifications for grant funding: Agencies in Tier I do not always meet the ridership qualifiers for Tier I grant funding guidance, but are not eligible for competitive Tier II funding because they are in Tier I. The requirements need to match the membership. If you are a Tier I member, you should qualify for a Tier I project.

- Industry Peer panel for grant guidance development and roundtables annually to discuss any new DHS/TSA priorities or security emphasis-allow the transit agencies to determine the project to solve the security concern. Additionally, allow the transit agency to put forth their concerns and issues and ensure that at the completion of conference, all parties understand what the next grant guidance will be.

-Utilize Threat/Vulnerability Assessments for each Agency to determine priorities and have TSA use the assessment and use the assessment as a progress and accountability matrix of performance and progress towards identifiable and quantifiable risk reduction.

-Detection, response & recovery projects (including Chem. & Bio. Detection) should be an available project in a specific category. Due to the expensive nature of the current technology of Chemical and especially Biological detection, the project should be funded for not only installation but also on-going maintenance.

-Maintenance/Administration Costs: The current 2.5% is way too low, more like 10-15% more realistic; guidance on how it is to be calculated needs to be more clear.

- Transparency in grant allocations to regions (NY 1/3 of all national \$\$ vs. CA 13%)
- Grants Program Management: TSA or FEMA, one or the other
- More predictability and flexibility in implementing priorities: allow agencies to engage in more long-term projects covering multiple grant years.
- Decrease emphasis on operating initiatives due to the fact that Law Enforcement has UASI grants that can be applied to the region as well. TSGP should not be used to supplement UASI grants.
- Expedited approval process similar to the FY 2007 "Expedited Training Requests" for all projects.
- DHS/TSA should only contact the transit agency's designated representative regarding security initiatives and not a subordinate or contracted law enforcement department or agency.
- IJ's should be allowed to reference security sensitive documents instead of actually including them.
- More streamlined IJ consistent with the general guidelines of FTA's Section 5307 will provide agencies with a broader range of eligible costs and streamline the grant process (for examples see Transit Security Grant Program Improvements, December 2007).
- For additional information please reference "After-Action Confernece (AAC), Wednesday, October 15, 2008, TSA Headquarters, 601 S. 12th Street, Arlington, VA, 22202" and "Key Issues with FEMA/TSA Being Involved with the TSGP".

We all know that the 9-11 Commission Report cited the "Failure of Imagination" as one of the most significant shortcomings in security before the terrorist attacks. Also, the Office of Homeland Security's Mission Statement for the Transportation System Sector states "Continuously improve the risk posture of the Nation's transportation system." And to further this position, DHS' own Sector-Specific Plan "...describes the security framework that will enable sector stakeholders to make effective and appropriate risk-based security and resource allocation decisions." (Emphasis added) (Transportation Systems, Critical Infrastructure and Key Resources, National Infrastructure Protection Plan, May 2007, Executive Summary, pg. 2) Our region supports these ideals and seeks to enable them in a flexible and manageable way. We know and understand the asymmetrical threat we face and we know our systems best. As an experienced battlefield commander, having served in Iraq, I know the threat we face as do many others who work in our industry. We need to be allowed to influence our agencies' security destiny with the funds the American people have given us.

In summary, I would like to say that my agency and our region would like to see a reformed Transit Security Grant Program that encourages and supports imagination and innovation at the local level in executing the intent of Congress in securing public transit as a national critical infrastructure asset. In order to achieve this goal, we need maximum flexibility and discretion at the local level to operate within a broad but well defined program and grant guidance from TSA.

Thank you, Mr. Chairman. I would be happy to answer any questions you may have.

Jack L. Eckles, J.D.**Biography**

Mr. Eckles has been in the security industry for in excess of 28 years in various positions and areas to include Governmental, Commercial, and Private Security & Investigations as well as working as an L. A. County Deputy Sheriff. He is currently the Deputy Executive Officer, System Safety, Security & Law Enforcement for the L. A. County Metropolitan Transportation Authority. He has responsibility for all operations and administration of the departments of System Safety, Security and management of contracted Law Enforcement Service, consisting of over 600 staff, contractors and support members covering an agency with over 9,200 employees. Areas of concentration are physical, operational, and system-wide safety, security and law enforcement; emergency preparedness and response operations, threat response and mitigation, project development and management.

His education includes a B.S. in Criminal Justice from CSULA, a B.S. in Law as well as a Juris Doctorate degree from Pacific West College of Law. He has completed the Professional Development courses from FEMA as an Emergency Manager, attended numerous training seminars in Law Enforcement, Security and Emergency Preparedness as well as attending the "Managing the Consequences of Terrorism" course by the National Interagency Civil-Military Institute.

Mr. Eckles has written many articles for various organizational and operational publications.

Mr. Eckles has spoken before many veterans' organizations and security professionals' groups as well as the L.A. County & Cities Emergency Preparedness Commission, Public Agency Risk Manager's Assoc., and the Reserve Officer Assoc.

Mr. Eckles is also currently a Lieutenant Colonel in the U.S. Army Reserves with training and expertise in Military Police, Military Intelligence, Army Special Forces (Green Berets), and Civil Affairs specialties. He is currently assigned as the Assistant Chief of Staff - Intelligence, 358th Civil Affairs Brigade, at Riverside, CA. Through his career he has traveled to many countries to include Thailand, Japan, and served duty in Kuwait as the Intelligence Operations Officer for the Combined Joint Task Force – Kuwait. Mr. Eckles has also conducted a one year tour in Iraq as a Commander for a Civil Affairs unit involved with reconstruction and humanitarian assistance efforts for which he received a Bronze Star and Purple Heart. Mr. Eckles has trained or trained with service members from countries such as Great Britain, Australia, Norway, Spain, Algeria, and the Ukraine.

AWARD AND FUNDING DELAYS

Mr. PRICE. Thank you. We obviously have a great deal to talk about.

Since 2002 and including the recently enacted economic recovery package, Congress has appropriated a total of \$1.67 billion for mass transit and passenger rail grants. These funds are used for security enhancements, including infrastructure protection, deterrence, facility hardening, employee training, and other purposes. There are numerous statutory requirements placed on TSA and FEMA as to how quickly this funding must be awarded and how quickly it must be provided to transit and passenger rail agencies.

However, once the award has been made, once the funds are obligated, this funding is commonly sitting around for up to 2 years before it is spent. We have heard a good deal of testimony this morning to that effect together with some of the reasons for this delay and some of the frustrations that accompany this delay. \$130 million, or 93 percent, remains unspent from 2006 rail and transit awards. Over \$268 million remains from 2007, that is 99 percent, and so forth.

[The information follows:]

Grant Program	Award Amount	Drawdown	Balance	Percentage Unspent
Fiscal Year 2003 Total Award:	\$ 4,286,989,351			
Urban Area Security Initiative Mass Transit System Security Grant Program	\$ 87,662,441	\$ 86,607,451	\$ 1,055,089	1.0%
Fiscal Year 2004 Total Award:	\$ 4,118,739,224			
Urban Area Security Initiative Grant Program	\$ 720,584,415	\$ 717,847,706	\$ 2,736,710	0.4%
Fiscal Year 2005 Total Award:	\$ 3,650,625,100			
Transit Security Grant Program	\$ 134,125,851	\$ 115,515,099	\$ 18,610,852	13.9%
Intracity Passenger Rail Security Grant Program (Includes Freight Rail)	\$ 135,948,693	\$ 8,214,400	\$ 127,734,293	94.0%
Freight Security Grant Program	\$ 7,242,855	\$ 5,611,803	\$ 1,631,052	22.5%
Fiscal Year 2006 Total Award:	\$ 2,824,286,746			
Transit Security Grant Program	\$ 100,000,000	\$ 6,387,632	\$ 93,612,368	93.6%
Intracity Passenger Rail Security Grant Program (Includes Freight Rail)	\$ 162,870,870	\$ 3,507,483	\$ 159,363,387	97.8%
Freight Security Grant Program	\$ 100,000,000	\$ 8,309,537	\$ 91,690,463	91.7%
Fiscal Year 2007 Total Award:	\$ 4,242,031,587			
Transit Security Grant Program	\$ 359,489,800	\$ 5,620,056	\$ 353,869,744	98.8%
Intracity Passenger Rail Security Grant Program (Includes Freight Rail)	\$ 491,429	\$ 886,612	\$ 6,604,817	88.2%

Note: FY 05 Grant award amounts include all fully processed grants that are in the pipeline, including those awaiting GPO signatures. These processed awards will eventually be obligated when signed by the recipient. FY 06 and FY 07 CDEAP includes funding for training, and unobligated amount also includes cancellations, deobligations, and unobligated funds returned (which is also deobligated), therefore the obligated amount will sometimes be lower than the drawdown.

The Subcommittee has heard repeatedly from transit entities, including those this morning, about not just the slowness of decisions being made but the extraordinary difficulty of coming to agreement with TSA about specific expenditures, and priorities, and criteria and so forth. We need to understand this more adequately and figure out how to get around these problems, just to put it mildly.

There is one thing that the 9/11 Act did which was designed to expedite the awarding of grants. We required in the 9/11 Act that these awards be made directly to transit and passenger rail agencies instead of being administered through the States. I am hearing Mr. Morange say this morning that perhaps that is irrelevant, and in fact there are other good reasons for involving the States more directly in this process. So maybe that statutory requirement or action was misguided.

Anyway, I want to ask all of you in turn to address this. Mr. Ashley, Mr. Sammon, can you please explain to the Subcommittee why it takes so long for transit and passenger rail agencies to spend their grant awards? How do you account for the delay? How do you explain that and what are you doing or what can you do to make sure that the dollars are distributed more expeditiously? What kind of due diligence are you trying to exercise to make sure this doesn't become just an endless morass of shifting criteria, standards, nontransparent processes and all the rest that we have heard described here today? How can we solve this problem?

The Subcommittee has heard a lot of complaints, persistent complaints from a variety of transit and rail agencies about restrictions on how grant funds can be used, and on uncertain shifting signals about how grant funds can be used. Entities have complained that they must continue to spend funds for training when their employees are already up to speed. Others have complained they are not allowed to use funds for chemical or biological sensors in their facilities, although their own assessment is that that is the primary need. Mr. Eckles has outlined some of these frustrations. And then finally let me do ask about the decision to not have the States any longer as the grantee. Has this change had any effect in allowing the dollars to be spent more expeditiously? Are there other reasons for having the State involved, as Mr. Morange I think suggested?

Let's start with our Administrator.

STATE ADMINISTRATIVE AGENT ISSUE

Mr. ASHLEY. I will start from an overall perspective, from a grant management perspective. First, let me comment on the State Administrative Agency (SAA) issue. This is actually the first year that the dollars will go directly to the transit agencies. This will be a new process. Previously, the dollars had gone through 56 State Administrative Agencies, and the transit entities would then be the subgrantees.

That inherently, in some people's view, created a delay in the process, because the funding would go to the State, the State would subgrant, and that process created delays.

Mr. PRICE. I must say though that none of the accounts we have heard this morning cite that.

Mr. ASHLEY. No, sir, but that would add to the overall delays from previous years. Although it makes a lot of sense when you are

looking at the regional collaboration. FEMA and TSA would both support the continued use of that process. For the last two years, the appropriations laws have mandated timelines that have been met, both in terms of getting the guidance out and making awards. We have consistently done that over the last two years.

In previous years, in 2006 and such, there were extensive delays in getting both the grant guidance as well as the awards out. So there have been improvements in that area as well.

DRAWDOWN OF FUNDS

As far as the overall drawdown of funds, when you look at awards being made and then funds actually being depleted out of the Federal treasury, there are a number of issues that surround that. Some are at the local level, some at the Federal level. Let me talk a little bit about the Federal bottlenecks and what we are doing on our end.

They primarily reside with two major issues. One is ensuring our role as the fiduciary agent of the dollars to ensure that the dollars are being spent according to good practices, and that we have detailed budget worksheets—all of the fiduciary responsibilities that we have in place to ensure that the taxpayers' dollars are being spent effectively. That is part of it—having those detailed budgets and all of that before projects are authorized to spend down.

HISTORIC PRESERVATION REQUIREMENTS

The second is, the environmental historic preservation requirements on some of the specific projects in all of these grant programs. If you take, for example, projects in New York where just about every facility that is going to be modified is greater than 50 years old, you are talking about an environmental and historic impact statement that must be conducted. Some of those statements are very detailed and take a long time to complete. That creates delays in the program.

At the local level, we primarily see the acquisition process. There is in every local jurisdiction a different acquisition process that takes time to get those monies out the door, and then on a reimbursable basis for those monies to actually be drawn down out of the Federal Government.

That outlines some of the processes. As far as improvements go, specifically with the environmental historic preservation, this year we have allowed our program analysts at FEMA to take level A projects, the first level of EHP projects, and categorically exclude EHP from it and allow grantees to be able to draw down on monies that do not have environmental impacts.

Regarding Level B, or the second level of environmental historic projects, we allow the program analysts to work directly with our NEPA staff at FEMA to collaboratively get these projects rapidly through and approved for a drawdown.

For the third level projects, we have to turn them over to the NEPA staff to do the environmental historic impact statements before funds are allowed to draw down.

When we talk about drawing funds down, if we look at New York just as an example here, if we look at the 2006 funds, 96 percent of the funds are available to be drawn down today of every dollar

that is there. There are a couple of “cat and dogs” projects out there. Ninety-two percent of the 2007 and 96 percent of the 2007 supplemental funds are available today to be drawn down.

In Los Angeles, or California I should say, in total: 88 percent of the funding in 2006, 60 percent of 2007, and 61 percent of the 2007 supplemental funds are available today to be drawn down. You can see they are differing across different transit agencies and there are a number of different reasons for each one. A lot of the California stuff is tied up in FEMA’s EHP process.

TSA ROLE

Mr. PRICE. As I understand it, 90 percent of complaints, have to do with TSA, not FEMA. So the extent the factors you cite loom large in your own mind wasn’t mentioned in any of the specific accounts we heard, but I do think we need to put the TSA role into perspective here. That appears to be where most of the delay is occurring.

TSA MODIFICATIONS TO GRANT LANGUAGE

Mr. SAMMON. Thank you very much for this opportunity. The language for the grants in 2008 was modified to go to the agencies and further modified in 2009 to go directly to transit agencies. In 2008, TSA wanted to establish the most transparent process we could. So, we did the grant guidance, there is a lot of verbiage behind it, but basically, this chart shows you the types of projects. Because we anticipated Congress saying “get the States out of the process” and have agencies competing directly agency-to-agency, we wanted to make clear what the security priorities were from an effectiveness basis, not only from a security effectiveness but also a cost effectiveness basis. We ranked them one through six and each category has a score. So, anybody can look at this and say here is a category and the score.

SECURITY RANKINGS

Separately we have security rankings for the top 150 agencies, and as protected SSI we provide those agencies with security rankings. Mr. Morange knows his, in Los Angeles they know theirs, and the other agencies know theirs. On a very transparent, simple basis, an agency can look at a project and make decisions where they think they will be in terms of putting up fences in bus yards versus where they might be in terms of training employees, or as Bill said, in terms of public awareness. It is very simple, very straightforward, and very transparent.

INTERACTION WITH THE TRANSIT COMMUNITY

In our interaction with the transit community we did add in the three largest jurisdictions in the country where the security agency is providing the boots on the ground, every day security—NYPD, Chicago Police Department and Los Angeles Sheriff Department. I know Mr. Eckles refers to him as a security contractor, but Sheriff Baca with the Sheriff’s Department for Los Angeles County is a little bit more than a security contractor. We included those folks at the table because we wanted to make sure, from a security stand-

point, that we were getting the best day-to-day, law enforcement view of what was happening down in the subway, on the bus lines, and whatever else, at the table for that discussion in terms of what really are the regional priorities. Some people work with it, some not. But, we feel, from a security standpoint, that the people who are the boots on the ground, front-line, every day, day in, day out, people who are securing the subway, have an opinion of what is important to do their job every day. We included those folks and made the process better. In terms of the specifics that Mr. Eckles is talking about, my staff could address those. I do not know those personally.

But, the idea was to make it as transparent as possible and to let people choose. In terms of the biological/chemical detection systems that was taken out in 2008 by other folks, it is back in this year's application and they are qualified things that people can look at and ask for. But, rather than go through some mysterious process, we use this. It is available on the TSA Web site where anybody can see it. It is simple as possible to say how should I apply for these monies and we made it as straightforward and simple as it could be.

Mr. PRICE. Thank you. I am going to ask our two transit representatives to respond very briefly. Assuming that this line of questioning will be pursued by Mr. Rogers and others, this will not be the only chance to further this exchange. Mr. Morange, if you could just respond briefly, particularly to the point about the State's place in the process.

Mr. MORANGE. We believe—we have found, you know, working along with all the other partners that we have up in the New York region, that if the State would pull us all together and be the guidance and, you know, not be the dictator of what is going to be done, but they would be the guidance to come along with a regional security strategy—because what we found out in the past is, like with the NYPD—I have spoke with the NYPD commissioner on many occasions. We have partnered up on things that we have done.

But we have found out that one agency would be putting in cameras here, we would be putting cameras in here. Learning the technology and finding out what is the right way to do this, what is the best way to put these systems in. As you well know, everybody went into an integrated electronic system that they wanted. The Port Authority had their own, the NYPD had their own, and we had our own. And we could have got more out of it if we all would have just combined our efforts and got together.

And I really believe that the State should be part of that process to bring us together and come out with a security strategy that we could go to TSA and say, this is our strategy, this is what we would like to do.

Mr. PRICE. Thank you. Mr. Eckles.

Mr. ECKLES. Our State representatives have been very supportive of our region's actions and our decisions in following our strategic plan that we were required to develop. They don't dictate to us what we should be doing. They don't hinder us, and they haven't hindered us. They have been a great advocate and a great representative in trying to deal with TSA and FEMA when we run into obstacles or problems.

In terms of a delay in funding, we haven't found that the State has created any kind of delay in funding once it has been approved at TSA.

Mr. PRICE. We will return to the explanations you gave for the delay in funding and how this all comes together as we proceed.

Mr. Rogers, let me turn to you.

FUNDING AVAILABILITY

Mr. ROGERS. Mr. Chairman, I am absolutely confused. I don't understand what has been said. I am trying to understand what the problem is.

Mr. Sammon, you say that a great percent of the monies available to these two systems is available now to be spent. Who said that?

Mr. ASHLEY. I did, sir.

Mr. ROGERS. Is that correct?

Mr. ASHLEY. Yes, sir.

Mr. ROGERS. Repeat that briefly.

Mr. ASHLEY. The percentage numbers?

Mr. ROGERS. Yes.

Mr. ASHLEY. Yes, sir. I can speak to any one of the Tier 1 large transit systems.

Mr. ROGERS. Keep it simple.

Mr. ASHLEY. If we look at fiscal year 2006 funds for New York, 96 percent of the funding is available to be drawn down today.

Mr. ROGERS. Today?

Well, Mr. Morange, why haven't you drawn that down?

Mr. MORANGE. Well, on most of the drawing down of the funding, you know, we have to put in vouchers and all. And this has been ongoing. A lot of times, we don't even find out that the grant has been awarded to us until almost a year and a half after the clock starts running.

Mr. ROGERS. He says the money is available now.

Right?

Mr. ASHLEY. Yes, sir. Of the 2006 dollars—

Mr. ROGERS. Now, what does it take for him to get that money?

Mr. ASHLEY. Submit a reimbursable, you know, that the funds have been expended and—

Mr. ROGERS. He spends the money and then bills you for what has been spent.

Mr. ASHLEY. Yes, sir.

Mr. ROGERS. What about that, Mr. Morange?

Mr. MORANGE. I don't really know, at this point. I will have to get back to you, because we have a staff that does that. But I am sure that—

Mr. ROGERS. Surely you know. Surely you know whether or not you can support with paper the expenditures that he says you must have. That is not difficult to understand.

Mr. MORANGE. But I am saying I believe that we have put in for all of these expenditures that we have used in 2006. And I believe that we have done almost everything in 2006. So I don't know—

Mr. ROGERS. Mr. Ashley, he said he has already done what you requested.

2006 FUNDING DRAWDOWN

Mr. ASHLEY. I don't have the drawdown figures in front of me on how much of the 2006 funding has actually been drawn down. Of the 2006 funding, all of it is available to be drawn down. I don't have what has been drawn down in front of me.

Mr. ROGERS. Does anybody here on your staff know?

Mr. ASHLEY. Do we have the drawdown figures?

No, but we can provide that back—by grant program, by project. Actually, your staff may have that information. We provide those reports to your staff on a, at a minimum, quarterly basis.

Mr. ROGERS. Well, Mr. Morange, have you submitted all of your expenditure papers that are required before you can get the drawdown?

Mr. MORANGE. I believe that we have submitted all of the paperwork on everything we have completed.

Mr. ROGERS. What about that, Mr. Ashley?

Mr. ASHLEY. I would have to check, sir. I don't know what has been submitted at this point.

Mr. ROGERS. Why are we having this hearing? Why are we here? If you don't know how much money has been drawn down or how much is due to be drawn down, the taxpayers are getting screwed. There is nothing new about that, but, goodness gracious.

Well, Mr. Sammon, you tell us. You have to approve this stuff, too.

Mr. SAMMON. We do. We approve it. All those projects have been approved, as Ross said. The money has been obligated, it has been approved. But the drawdown numbers—FEMA has the numbers; we don't have the specific drawdown numbers. But I believe all that.

For instance, when Bill mentioned—earlier, we mentioned the drawdown over Thanksgiving for the response to the threat. That was 2007 money or whatever else that was drawn, 2008 money that was drawn out of the account and paid for that surging activity. So there is current money in the accounts. But I don't have the—

Mr. ROGERS. Mr. Eckles, what about you? Tell us. I know you are perfectly content with all of this. Tell us your story.

Mr. ECKLES. Well, let me give you an example about 2006, since they have figures to tout 2006. We had a project that didn't get 2006 approval until July of 2008. And the—

Mr. ROGERS. What I want to know is, have you submitted drawdown justifications to them that have not been satisfied?

Mr. ECKLES. We haven't got—well, we have gotten all of our grant authorization to spend down, as of October of 2008 for 2006 funds. So, yes, we have done that.

Mr. ROGERS. You have done what?

Mr. ECKLES. We have submitted whatever reimbursements are required for the projects that finally got started in October of 2008.

Mr. ROGERS. And have they paid you?

Mr. ECKLES. Not to date.

2006 FUNDING DRAWDOWN CONT'D

Mr. ROGERS. They have not reimbursed you for the papers that you sent in that you spent?

Mr. ECKLES. Right. There is a pretty big lag time to get that back. It is, what, about 3 to 6 months?

Mr. ROGERS. Well, how long ago did you complete sending the paper work?

Mr. ECKLES. We do it incrementally. So—

Mr. ROGERS. Help me out. Make it simple, please. Tell me, when did you submit the justifications to be reimbursed for?

Mr. ECKLES. Since they only started in October, we have only had one submittal in December, for DART. So December was our first submittal of our initial reimbursement request.

Mr. ROGERS. Have they reimbursed you for the expenditures that you have made?

Mr. ECKLES. Not yet.

Mr. ROGERS. What is the problem?

Mr. ASHLEY. I would have to check on the specifics for the—

Mr. ROGERS. Oh, for God's sake. Did you bring anything with you?

Mr. ASHLEY. Not on what we have actually paid out, no, sir.

Mr. ROGERS. Holy cow.

Thank you, Mr. Chairman. I have heard all I want to hear.

Mr. PRICE. Mr. Rothman.

Mr. ROTHMAN. Thank you, Mr. Chairman, for holding this hearing.

And I join Ranking Member Rogers. I am shocked that, for example, FEMA and TSA don't know how much of the 2006 money has gone out. Don't you need to know whether the people's money, as approved by the Congress, has been spent according to the Congress's will as expressed in legislation that governs your agencies? Don't you want to know if it is being spent? Because if it is not being spent, then you are not fulfilling your obligations to keep rails safe in America. Don't you want to know if it is spent?

Mr. Ashley.

Mr. ASHLEY. Yes, sir, we do want to know how it is spent, when it is spent and all of that. We do provide—and it is my mistake for not having the reports in front of me—but we do provide both to your staffs. We also use it internally—exactly how much money is drawn down on a regular basis.

Mr. ROTHMAN. Excuse me, sir, I apologize. I don't know—could you explain your responsibility? How could you know the rail security picture in the United States if you don't know what has been spent from the 2006 budget? How can you be doing your job properly if you don't know?

And I am not saying you need to know every dollar, to the penny. How about a ballpark figure? I think that is more of a rhetorical question.

But let me just say this. There is also a great disparity, apparently, between what the chairman of the committee knows and what you say is the truth. The chairman said that 96 percent of the money was unspent nationwide in 2006—excuse me, 93 percent—and 99 percent from 2007 unspent. But you say that they are

available for drawdown, but, frankly, you don't know if they have been spent or not.

APPROVAL OF THE 2006 BUDGET

How about Mr. Eckles, Colonel Eckles, who says that it took him until October of 2008 to get approval for the 2006 budget? Mr. Ashley, how do you explain that considerable delay, sir?

Mr. ASHLEY. For fiscal year 2006, there were considerable problems with the process, as I am aware. I wasn't here during that time frame. There was a lot of back and forth, as I understand it, between the grantees and TSA and FEMA at that point. The process was completely different then. I was made aware that there were a number of unallowable things applied for, and all of that had to be married up.

Mr. ROTHMAN. Okay, those were bad practices. You weren't there.

Mr. ASHLEY. Correct.

PROCESS IMPROVEMENTS

Mr. ROTHMAN. On a scale of one to 10, Mr. Ashley, 10 being all the problems that caused this delay for the 2006 funds—10 being all those problems have been fixed, what number would you give the process now?

Mr. ASHLEY. Where one would be the best?

Mr. ROTHMAN. Yes.

Mr. ASHLEY. I would say we are probably around a four to five. We still have a long way to go in the process to improve it, to make it streamlined, to make it, as Mr. Eckles said, more transparent. We still have a ways to go in that process.

Mr. ROTHMAN. What is the problem?

Mr. ASHLEY. I think a couple different things. One is, it is the natural maturing of grant programs. If you take the Port Security Grant Program to date, which has been around for quite a long time, the process is much more of a streamlined process that goes forward. We have a different process in place for our Tier 1 transit agencies than we do in our Tier 2 transit agencies.

Mr. ROTHMAN. Okay, but these are the Tier 2 folks, right?

Mr. ASHLEY. Right.

JOINT ADMINISTRATION BY FEMA AND TSA

Mr. ROTHMAN. I know my time is limited, but do you gentlemen, Mr. Sammon or Mr. Ashley, do you have an opinion on whether the grant program that the transit—the security grant program should be administered jointly by FEMA and the TSA, or should it be administered by only one of your organizations?

TIER ONE PROCESS

Mr. SAMMON. I think the joint administration works because TSA sets the policy.

Let me, if I can, just walk through quickly, in terms of the Tier 1 agencies, how the process works. In 2006, it was a hands-off process that was strictly done all by competitive submissions. When the submissions came in, no one could talk to the applicant grantee—

we could not have a conversation, you couldn't pick up the phone to talk to the grantee to ask them questions about the grant.

Mr. ROTHMAN. Was that as a matter of law?

Mr. SAMMON. That was a matter of the process at that time. So we changed—

Mr. ROTHMAN. Was that as a law? Okay. That wasn't law as written by the Congress. It was regulations written in the Bush administration?

Mr. SAMMON. It was probably DHS grant guidance.

So we looked at that, and that was failed. So we said let's set up a different process; we call it a cooperative agreement. The way it works is that TSA and FEMA sit down with the regional working group, we discuss any guideline changes, funding priorities, ask preliminary questions, and the agencies develop their project concepts. They might say, I want to harden tunnels, I want to hire personnel or I want canine teams. The project concepts are preliminarily scored and ranked, because we—

Mr. ROTHMAN. Excuse me, Mr. Sammon. I have overdone my time.

Mr. Ashley said 40 percent to go to get this right? Am I right, 40 percent to go?

And maybe someone else can ask the two guys on the ground, Mr. Morange and Mr. Eckles, if they agree that there is 40 percent to go, and this is how many years after Congress first provided money. It is unacceptable. I think heads should roll and people should be fired.

Mr. PRICE. Mr. Kirk.

CASH FLOW REPORT

Mr. KIRK. Thank you, Mr. Chairman. Just two quick things, and then I am going to yield to Mr. Rogers.

You are an Air Force veteran, a lot of experience in information technology. My gentle suggestion to you would be to cancel all leave, crash this weekend, and get this committee a cash-flow report by Monday morning. And I would hope that you would be able to do that.

Mr. ASHLEY. Yes, sir. And I think it is my mistake that I don't have one in front of me. I think your staff may even have them behind you, but—

Mr. KIRK. Okay.

METRA REQUEST

Secondly, I deal with Metra, which is the largest transit agency in the Chicagoland area. We put in a grant application to link closed-circuit televisions to local police departments because, frankly, Metra police is pretty thin and not present. The Department turned it down saying, hey, because Metra is not the first responder of record at these train stations, you guys are hosed. And I would say that is probably overly restrictive. So if you could take a look at that, that would be a good thing.

And let me yield the rest of my time to the ranking member.

TWO AGENCIES IN CHARGE

Mr. ROGERS. I thank the gentleman very kindly for that time.

I have the drawdown information here. For 2008, we authorized \$359 million. You have drawn down \$5 million. You have \$354 million of that left, 98.6 percent still laying around. 2007, in the same security grant program we authorized \$162 million. You have drawn down \$3.5 million. You have 97.8 percent of it laying around. That is 2007. 2006, you still have 94 percent of it undrawn. And 2005, there is almost 14 percent of the 2005 money still laying around.

Somebody mentioned here a while ago, perhaps from the two units, that part of the problem is we have two agencies that you have to go through. And I have always figured that when you have two bosses, nobody is in charge. I would like to have one person to chew on, rather than two who bat the ball back between them so you can't know what is going on and who is responsible.

Do you all agree with that or not?

Mr. SAMMON. I think we view it is that FEMA has expertise in terms of handling grants. They handle about \$4 billion worth of grants. TSA has the ATSA requirement and its charter to be the transportation security agency for all modes of transportation. In terms of setting those priorities, TSA works with FEMA to do that and then get the money out.

APPLICATIONS PROCESS

In terms of applications and looking at where that goes, we have a project, for instance, right now from 2008 that we are trying to get resolution on, for \$36 million to harden a tunnel, and the justification is "construction and materials." We have been working with the agency to try to get a detailed justification from them. It is \$36 million with a one line justification. We have others—\$5 million for CCTV, with a one line justification.

We work with the agencies to try to get detailed information out. The process is to work a cooperative agreement, get the concepts, rank them, and then get detailed justifications. In 2008, in particular, when the matching fund requirement was removed, a number of the agencies changed the projects around. And we are still working through that process.

But, again, we have things in there that are one-line justifications that we can't put out the door until we have more detail.

Mr. ROGERS. Are these two systems involved in any of those?

Mr. SAMMON. Not for those two examples, no. Those two systems, in terms of what they have, I think there is one project from 2008 that we are working with MTA on that is about \$270 million. I forget exactly what it is for, but we are trying to finalize that. And there is one or two with L.A. that we are trying to complete.

FEMA FIDUCIARY RESPONSIBILITY

Mr. ROGERS. Why is FEMA involved in this?

Mr. SAMMON. FEMA is involved in this because there is a fiduciary responsibility to make sure that, once the money is awarded, that—first of all, there is the mechanism to put it out the door, the

administrative mechanism, and then also to make sure that the money is spent as it was initially proposed.

Mr. ROGERS. Why can't you do that, TSA?

Mr. SAMMON. Well, TSA currently does not have the mechanism to do that, the people nor the administration in place. I think the Department's view of it is, we have an agency, TSA, which is good at vetting and security and those kinds of things, but it is not an administrative agency for grant purposes. FEMA handles 4 billion dollars in grants across the way.

Mr. ROGERS. Well, FEMA, God love them, are notorious for being slow and bureaucratic, and they tie themselves up in knots over the slightest thing.

Pardon me, Mr. Ashley. I love you, but—

Mr. ASHLEY. That is all right, sir.

Mr. ROGERS [continuing]. I think privately you would probably admit that is true. And here we see the biggest example of, I think, that.

But we are frustrated. We don't know where to turn or what to do to make it work. I mean, we pump the money into the coffer, and it just lays there, rotting and mildewing. And the people riding these subways and mass transit by the millions daily are the people whose fate hangs in the balance.

So can we find a way to get the grants out there where the Congress intended them to go?

EXPEDITE GRANT PROCESS

Mr. SAMMON. We will work more closely with FEMA. Also, what we will do—we probably, in one respect, have been too nice, in a way, in terms of allowing the back-and-forth process to go on. For instance, this one-liner from the agency who wants \$36 million for a particular project, we should probably say, if we don't hear a response in 2 weeks or whatever else it is, we will move on.

But, we have been, I think, generous in terms of working with the agencies and working with changes, as, for instance, in 2008 when the Congress said you don't need to have matching funds anymore, a large number of projects were all reprogrammed because they wanted to change priorities. And we were very flexible and said we will work with you on that. That is a process that slows things down.

But we will work on a number of things with—

REPORT REQUIREMENT

Mr. ROGERS. Mr. Chairman, I would like to request that both agencies, TSA and FEMA, give this Subcommittee a report no later than 1 month from today about what can be done to expedite these grants and what the problem is and a timetable for getting this money out there. I would like to see us require them to give us something in a month's time.

Mr. PRICE. Let's do just that.

We will expect in a month's time a report on the best explanation you can give for the problems we have encountered and your plan for resolving this and giving us money where it needs to be. That is an important priority for the Administration coming in, and we,

on this Subcommittee, would like to push that forward. A month seems about right.

Mr. ROGERS. And it better be good.

Mr. ROTHMAN. Mr. Chairman, may I ask you a question with regards to the report that you and the Ranking Member were talking about? And maybe this was assumed by you in your request to these gentlemen, but that the report also include their timetable and pledge for disbursing the money.

Mr. ROGERS. That was one of the three things.

Mr. PRICE. Yes, we will flesh this out. But, of course, that is one thing we want to know, where we stand now and what the current timetable looks like, as far as they can project it. But much more than that; obviously, business as usual isn't what we are looking for here. We want to see a plan for getting this done.

Mr. ROGERS. And I want to know who is responsible. I want to know the names and addresses.

Mr. PRICE. In my period of questioning, I want to return explicitly to that, because I don't think we have yet sorted out the TSA-FEMA roles here. I want to go back to some of Mr. Eckles's problem and dissect that account and see exactly where the delays we are talking about occurred.

But I first want to turn to my friend, Mr. Serrano.

IMPORTANCE OF FUNDING

Mr. SERRANO. Thank you, Mr. Chairman.

Mr. Chairman, I, like all members, had a series of questions. But I am not going to ask those questions; I will submit them to the record. Because, at the expense of being redundant, I have to join the committee in the outrage of what I heard here today.

You know, with all due respect to you two gentlemen, those two guys, New York and L.A., with all due respect to all the rest of the Nation, have a pretty tough job on their hands. They have to protect two of the largest targets in this country. There was a reason why the terrorists hit New York. It wasn't because they knew I lived there. There was a reason: It was Wall Street, it was the stock market, it was our financial center. There was a reason why they hit the Pentagon: It was our military strength. There was a reason why they intended to hit the legislative building or the White House. So all these things made some sense in a horrific way.

As a result, we turned this government upside-down and created this Homeland Security Department of which you are part. And in turning this country and the government upside-down, we did a lot of things that some of us still feel bad about, in terms of people's civil liberties and civil rights and how we deal with implementing security.

But one thing we all did, whether we were happy about it or not happy about it, is we voted year after year—and I have been on this committee since the beginning—for the funding that goes for the whole Department and for your specific agencies.

And I have to say that, except maybe for the FBI, which was in charge of another part of fighting the war on terror, we haven't pulled any strings here when it came to holding back on dollars. A lot of money has been spent.

So even those of us who still have problems with the way Homeland Security is run and any of your agencies is run still feel that the money has to be spent. It makes us look bad if we have to fight every year to get more money and then the money is not spent.

Understand something. Yesterday the President signed a bill which was a monster bill. It had nine subcommittees involved in that one bill. But one of those bills was not Homeland Security, because that goes out by itself, because every Member of Congress knows the importance of what you do, or at least what you are supposed to do.

And here we hear that there is money ready to be drawn down but they can't draw it down. As far as I am concerned, the money was ready to be drawn down the minute the President signed the bill.

I remember working for the New York Board of Education and asking the State for money, and they always told me that the money was ready to be drawn down, except that 2 years later I still hadn't received the money for the Title 1 programs. And so I know what we are talking about here.

I think you should get at least a sense that this chairman, this ranking member, and this Subcommittee are not happy with the testimony that came today and that it is totally unacceptable to say that you don't have the numbers. Because, again, we appreciate the work you do, we appreciate the work you do, but those two are charged directly with the responsibility of taking care of Mrs. Rivera when she enters the subway system or takes the bus somewhere. And I am interested that she gets taken care of, along with Miss Smith and Miss Goldblatt and everybody else.

This is important. And I would hope that you take away from here the need to answer the questions and to get on the ball. You can't come back to us again and tell us you haven't spent money. You know, there are areas where we allocate money and hope it doesn't get spent. This is an area where we allocate money and we know it has to get spent and we want it to be spent.

And I will not tolerate this part of the panel telling me that that part, which is on the field, dealing with the issues daily, that they can't draw down the money or the support they need.

So take seriously the chairman's request and the ranking member's request for that report, and do something which is strange for some of us to do: Don't think of yourselves as bureaucrats. Think of yourselves as a team where those two may be in your position next week and you will be running New York and L.A., and then you know what they have to go through.

And so, if I sound one-sided, it is because I live in that city, I know that subway, and because in a couple of hours I will be on Amtrak back to the city of New York. So I know exactly what I am talking about. They need your support, and the answers you gave us today are not acceptable.

Thank you, Mr. Chairman.

Mr. PRICE. Thank you, Mr. Serrano.

Mr. Calvert.

ADVICE ON STREAMLINING THE PROCESS

Mr. CALVERT. Thank you, Mr. Chairman.

Before I get to my comments, I want to thank Jack Eckles, who is attached to the 358 Civil Affairs Brigade in my district in Riverside, California. Thanks for your service, your service in Iraq. We appreciate that.

And thank all of you for coming.

I have a list of questions also that I am going to submit to the record. I have a couple of comments, sharing my colleague's perspective on this.

I think what we need is your advice, Mr. Eckles, and your advice, Mr. Morange, on how to move forward. And if you could give us some written responses to the committee on your advice on how these agencies can better streamline this process, I would rather hear it from the folks in the field that we possibly can help that process along.

One of the things I heard was this issue on the historical environmental review. I would suspect that public safety trumps historical environmental review. That is one thing we can do here in Congress, is, possibly working with the chairman and the ranking member, get an expedited waiver process in those instances. I am sure my colleague from New York would agree that, even though those areas in New York where you have historical significance, there should be an expedited waiver process if public safety is at risk. I think the people in New York would go along with that. And so I think we could be helpful in that process, in trying to move that process along.

And if we could get, in the field, your advice on how this process could move faster, we would be very much interested in hearing that.

And, with that, I am going to submit my questions for the record and hope to hear back from you all.

Thank you very much.

Mr. PRICE. Thank you, Mr. Calvert.

We have been conferring here, gentlemen, and we think one way to bring some focus to this and some resolution to it, hopefully, would be to ask the two of you to come back. And although it has the effect of shortening the time frame a bit, we have a hearing scheduled on March the 31st with TSA. And we, of course, will have other business to conduct that day, but we would like to ask the two of you to reappear on that day, be available for questions and to have this material together by that time. We will very quickly get to you our specifications as to what we want that to include. So, if that is agreeable with you, we will count on that.

Mr. Eckles, I said I wanted to dissect your case a little further. And I am not looking so much for more detail as I am a kind of accounting of where the problem lay with the things you have already laid out before us.

When Mr. Rogers was raising the questions about FEMA's dispatch—or lack of dispatch in actually getting the money out the door—we were focusing on the period from the fall of last year until the present.

However, we, of course, also have a time period of 2 years, from 2006 forward to the fall of last year. And my understanding of most of what you told us is that that period was occupied with a constant back-and-forth with TSA, not with FEMA. Many of the com-

plaints that you have had to do with the shifting criteria, the lack of transparency, and the various frustrations which you outlined very well.

So I want to just get you to clarify that a bit. We are dealing with two agencies here. Their roles perhaps intersect in problematic ways. But, to the extent most of these decisions lie with TSA, I want to make sure we focus on what that problem looks like from your point of view, and how the process can be improved.

And, Mr. Morange, we would welcome your chiming in any time you wish.

Mr. ECKLES. Would it be helpful if I gave you, like, the 2006 chronology kind of example of how this sequence of difficulties really goes about?

Mr. PRICE. Yes, very briefly, just to give us a sense of how that unfolded. Yes, that is exactly what I am asking for.

Mr. ECKLES. Grant guidance comes out, we have 45 days to submit investment justification. We submit that investment justification. 60 days, TSA has a requirement to give us an approval or nonapproval of our investment justification. That is the first grant authorization notice, but it doesn't authorize you to spend down.

Then we go through the haggling process of questions like "what is meant by multi-agency," "could you clarify this," "you are too detailed here," and it goes back and forth for an interminable amount of time until we get that second grant authorization that says, "Okay, we are done, you can spend the money now."

One of our biggest difficulties is the level of detail they want for something nobody has committed we are authorized to spend on: engineering drawings, specifications, a detailed budget of a project we have never done before. And nobody has the time or the energy to commit to developing engineering drawings and detailed budgets with any amount of certainty, which they keep asking for, when we don't have the money to afford the people to actually do that. We have never gone out and specced out this, or we have never gone out and drafted that, yet we are expected to have that kind of level of detail.

So this haggling and clarification goes back and forth until they finally settle on something that they will give us a spend-down grant authorization.

Mr. PRICE. Well, let me ask, I am sure you would agree that there is a certain due diligence which TSA should be exercising. I mean, even in urgent, emergency situations, we don't want to spend money recklessly or in ways that will not achieve the desired purpose. Yet it also seems very clear that the process you are describing goes way beyond that, in fact, is pretty dysfunctional in terms of getting money applied where it needs to be.

What would your suggestions be as to what an appropriate level of scrutiny is and an appropriate time frame? I know that is a very general question, but I am asking you to reflect on your experience and what, in your view, this process really should have looked like.

Mr. ECKLES. Well, they don't have to reinvent the wheel. My grants administrator that handles my transit security grants works with the Federal Transit Agency's grant process. And they have a Section 5307, which completely streamlines and structures a process where, you know, there is no expectation that you have draw-

ings on your table and that you are going to know exactly where every penny goes. They say, give us the concept, give us the idea, and does it fit into the criteria that we are looking for. You either have the concept and the project idea or you don't have it. Or if it needs to be adjusted, that shouldn't take any amount of time at all.

But the level of questioning, the level of detail—and, mind you, the level of questioning and detail is done by an analyst who has no idea about transit security, has no idea about engineering, but yet we have to answer these rather inane questions back and forth and change our grant and rewrite it.

So I would streamline it according to the FTA Section 5307 criteria.

Mr. PRICE. Mr. Sammon, do you have any response?

Mr. SAMMON. Was that 2006, or was that 2009? When were you referring to, this process of asking for detailed engineering drawings?

Mr. ECKLES. I used the 2006 timeline as an example, but we have run into that problem in 2007 supplemental and 2008, and we are on our fourth review in the 2008 right now.

Mr. SAMMON. Well, we will look into those details. But the idea with the working group is to get the concepts, rank them, score them, and say, here are the projects that are going to be approved. This is—I was referring to the \$35 million project—and then go back and get the justification.

After the project has been approved, it is on the books, ready to go. It is going to go through the hopper, but Ross and anybody else, any other fiduciary agent, would have to have more than, for instance, the project they refer to a one-line justification for construction costs.

Mr. ECKLES. Well, we submitted a project that had 54 pages.

Mr. SAMMON. Well, anyway, I don't have those. We can look into those things and see what they look like. But the process is designed to get that upfront, get the approval. And that is how we work with New York. It works very well in New York. It works very well in most regions. We will look in more detail at Los Angeles, but New York is the largest, most complicated one.

Mr. PRICE. Well, I am sure there are differences agency to agency, but you are not suggesting that Los Angeles's problems are isolated or unique, are you? I mean, we, after all, have been talking about aggregate numbers for the most part, right? Aggregate numbers, nationwide numbers—

Mr. SAMMON. Yes.

Mr. PRICE [continuing]. Numbers that you would agree are not acceptable for 2006, 2007, 2008 or even 2005.

Mr. SAMMON. Right. The numbers should be out the door.

Mr. PRICE. All right. So Mr. Eckles does have some, perhaps, unique circumstances. But on the face of it, it would appear that these process problems, whatever it is that is creating these interminable delays, are pretty much systemic.

Mr. SAMMON. But, I think the process has been changed to get as much of that on the front end—to agree on the projects and then have the justifications come in as the agencies can provide the justifications. So, it is upfront to say, I would like to train 420 people,

or I would like to do a camera system in a subway that is going to cost \$3 million. The regional working group ranks them, tiers them, and agrees on them. Then, the next step is the investment justifications have to go in. They have to be at a level of detail that can pass the test for future audits.

Mr. ASHLEY. Might I add something real quick, Mr. Chairman? Also, we are, to a large degree, dealing with sins of the past, if you will, when we talk about the dollars getting out the door. The 2006 processes, as you have heard from both of these gentlemen, were delayed considerably. The 2007 process was delayed considerably. What we are seeing now is a bottleneck, if you will, where all of those dollars are hitting up against a wall in a process to get them out the door rapidly.

The 2008 process, I would submit, both from FEMA's efforts and TSA's watching what is going on there, has been much improved. That is why I said we are not completely there, but we are getting better.

Also, I just had one quick comment. For the March 31st hearing, do you want the report prior to that date? We had two different requirements there. Just seeking a little clarification.

REPORT CLARIFICATION

Mr. PRICE. I think we would like the report a day or so in advance. We know it is a tight time frame but, we need to deal with this.

Mr. ASHLEY. I agree, sir.

Mr. ROGERS. But, Mr. Chairman, these two gentlemen will be here in person to answer any questions we might have on the report?

Mr. PRICE. Yes. That is the intent.

I am not going to prolong this back-and-forth at the moment. I think we have the picture. We will await your accounting of what is going on now. But, above all, we aren't looking for rationalization; we are looking for a concrete plan for improvement going forward.

And while we appreciate the chance to look more closely at these two systems, it seems quite clear that with these drawdown numbers, we are not just dealing with isolated problems. Each has its own peculiarities and particularities, but what we are talking about goes way beyond that.

Let's see. Mr. Rogers.

Mr. ROGERS. Mr. Chairman, I don't think I have anything further.

I appreciate the four of you testifying, especially the two gentlemen from the systems.

I was very impressed with Mr. Morange's concluding remarks, where he gives us eight specific recommendations. I like it when a witness gives us a cure for a problem. And we have not had the agency people respond to his recommendations, but perhaps they could do that for the record.

But we appreciate that, Mr. Morange. It was helpful.

[The information follows:]

The eight recommendations from Mr. Morange were outlined in both his written and oral testimony and were required by Chairman Price and Ranking Member

Rogers to be addressed as part of the FEMA-TSA report just submitted this week for the March 31 followup hearing on Rail and Transit Security Grant funding.

And, Mr. Eckles, I think we share your frustration with the process, and this chairman I think is determined to make things happen. And we expect a clarification and complete solution to this problem on March the 31st when these two gentlemen come back and give us a report that everything is smoothed out. And if they can't tell us that, we will have some questions for them.

Thank you, Mr. Chairman.

Mr. PRICE. Thank you.

Mr. Rodriguez.

9/11 ACT PROVISIONS

Mr. RODRIGUEZ. Thank you very much. And I apologize. I had another meeting, in fact, across the hall.

I have a question that was asked of me to ask Mr. Ashley, and it is from Congresswoman Lucille Roybal-Allard, who is sick today and wasn't able to be here. And she wanted me to see—and I am going to go ahead and read her question. And it is based on, actually, trying to get you to compel FEMA to make grant applicants aware of the responsibility to transit workers under the 9/11 Act.

And the question is that, "The 9/11 Act included several key provisions to safeguard the interest of transit workers. Specifically, it provided that the recipients of the grant funding should pay a prevailing wage and allow workers to bargain collectively. Unfortunately, FEMA neglected to mention these crucial requirements in the February 2008 guidance issued to grant applicants. "Will you take"—you know, according to her—"will you take action to rectify the error and ensure that the transit security programs are implemented in the way that Congress intended?"

Mr. ASHLEY. Sir, I can tell you that we actually already have. For the fiscal year 2009 guidance that we put out, we did rectify that issue. On page 39 of the guidance, we did require that all aspects of Davis-Bacon be adhered to for failing to pay prevailing wage rates. So we have dealt effectively with that problem, or that issue, sir.

Mr. RODRIGUEZ. Well, thank you for answering Congresswoman Roybal-Allard's question and concerns. I don't have any questions. I apologize for being late.

AGENCY PERFORMANCE ASSESSMENT

Mr. PRICE. That is all right. We have lots of activity here, and we appreciate your coming in.

Well, I am going to draw this to a close. We will want to formalize the request Mr. Rogers articulated, about explicit responses for the record to the recommendations actually that both gentlemen made regarding future improvements.

I want to bring up only one further matter, and it will just take a minute. It mainly involves a response for the record. But since I did cite in my statement a figure based on this, I want to circle back around just for a moment and ask about the evaluation process, Mr. Sammon, that TSA undertakes with respect to agency performance.

For the first time since TSA was formed in 2002 and as part of the DHS fiscal 2008–2010 performance report, TSA evaluated the percent of mass transit and passenger rail agencies that were in full compliance with the industry-accepted Security and Emergency Management Action Items to improve security.

In total, there were 17 action items, and TSA hoped that 50 percent of these entities would be in compliance. For this evaluation, you conducted 88 baseline security assessments, covering 48 of the 50 largest mass transit and passenger rail agencies. And on that basis, you concluded that only 23 percent of the 48 agencies met the target.

Now, according to TSA, the shortfall reflects thoroughness of assessments which far exceed prior security inspections. In 2009, you are going to undertake a second assessment and of course, you are hoping to improve on that performance.

I just want to ask you—and maybe you can respond briefly orally, but also for the record—I have before me these guidelines, 10 pages of quite straightforward action items, areas that would enable one, if you could assess them thoroughly, to come up with some measure of performance.

[The information follows:]

**TSA/FTA Security and Emergency Management Action Items
for Transit Agencies**

Management and Accountability

1. Establish Written System Security Programs and Emergency Management Plans:

- a. Ensure that Security and Emergency Management Plan(s) is/are signed/approved by senior level management
- b. Review plans at least annually and update as circumstances warrant
- c. Ensure the Security and Emergency Management Plan(s) integrate visibility, randomness, and unpredictability into security deployment activities to avoid exploitable patterns and to enhance deterrent effect
- d. Establish and maintain standard security and emergency operations procedures (SOPs/EOPs) for each mode operated, including procedures for operations control centers
- e. Establish plans and protocols that address specific threats from (i) Improvised Explosive Devices (IED), (ii) Weapons of Mass Destruction, and (iii) other high consequence risks identified in transit risk assessments
- f. Apply security design and crime prevention criteria through environmental design (CPTED) for major capital construction projects, system modifications, and procurements
- g. Ensure the Security and Emergency Management Plan(s) address(es) Continuity of Operations
- h. Ensure the Security and Emergency Management Plan(s) address(es) Business Recovery

2. Define roles and responsibilities for security and emergency management.

- a. Assign Security and Emergency Management Programs to (a) Senior Level Manager(s)

- b .Maintain a current record of the name and title of the Primary and Alternate Security Coordinator (includes Security Directors and Transit Police Chiefs)
 - c. Ensure that Security Coordinators report to senior level management
 - d Maintain accurate contact information for Security Coordinators and ensure they are accessible by telephonic and electronic communications means at all times
 - e. Ensure that management defines and delegates security duties to front line employees
 - f. Ensure that security and emergency management plan(s) is/are distributed to appropriate departmental personnel in the organization
 - g Hold regular senior staff and middle management security coordination meetings
 - h Hold informational briefings with appropriate personnel whenever security protocols are substantially updated
 - i. Establish lines of delegated authority/succession of security responsibilities and inform personnel
- 3. Ensure that operations and maintenance supervisors, forepersons, and managers are held accountable for security issues under their control**
- a. Hold regular supervisor and foreperson security review and coordination briefings
 - b. Develop and maintain an internal security incident reporting system
 - c. Ensure that a Security Review Committee (or other designated group) regularly reviews security incident reports, trends, and program audit findings, and makes recommendations to senior level management for changes to plans and processes
- 4. Coordinate Security and Emergency Management Plan(s) with local and regional agencies**
- a. Coordinate with Federal and State governmental entities associated with public transportation security (example: STSI Area Office, State

Office of Homeland Security, FTA Regional Office, JTTF, Office of State Safety Oversight etc) in the regional area of the transit agency

- b. Ensure consistency with the National Incident Management System (NIMS) and the National Response Plan (NRP)
- c. Establish Memorandums of Agreement or Mutual Aid Agreements with local government, fire, police and other entities with shared infrastructure (example: other transit agencies or rail systems)
- d. Maintain communications interoperability with first responders with security responsibilities in the transit system's regional area

Security and Emergency Response Training

5. Establish and Maintain a Security and Emergency Training Program

- a. Provide ongoing basic training to all employees in i) security orientation/ awareness and ii) emergency response
- b. Provide ongoing advanced i) security and ii) emergency response training by job function, including actions at incremental Homeland Security Advisory System (HSAS) threat advisory levels, to:
 - o Field Supervisors
 - o Controllers/Dispatchers
 - o Fare Inspectors
 - o Law Enforcement personnel
 - o Operators
 - o Maintenance personnel
 - Field personnel
 - Vehicle personnel
- c. Provide ongoing advanced security training programs for transit managers, including but not limited to CEOs, General Managers,

Operations Managers, and Security Coordinators (includes Security Directors and Transit Police Chiefs)

- d. Regularly update security awareness, emergency response, and counterterrorism training materials to address (i) Improvised Explosive Devices, (ii) Weapons of Mass Destruction and (iii) other high consequence risks identified through the transit agency's system risk assessments
- e. Ensure that security training programs reinforce security roles, responsibilities, and duties of employees, and ensure proficiency in their performance.
- f. Ensure security training programs emphasize integration of visible deterrence, randomness, and unpredictability into security deployment activities to avoid exploitable patterns and heighten deterrent effect
- g. Establish a system that records personnel training in i) security and ii) emergency response
 - o Initial training
 - o Recurrent training (periodic, refresher)
 - o Establish and maintain a security notification process to inform personnel of significant updates to security and emergency management plans and procedures

Homeland Security Advisory System (HSAS)

- 6. Establish plans and protocols to respond to the DHS Homeland Security Advisory System (HSAS) threat levels
 - a. Security and emergency management plans and procedures should identify incremental actions to be implemented at each HSAS threat level
 - b. Exercises should test implementation of the preventive measures for each HSAS threat level, including random application of security measures

Public Awareness**7. Implement and Reinforce a Public Security and Emergency Awareness program**

- a. Develop and implement a public security and emergency awareness program
- b. Prominently display security awareness and emergency preparedness information materials throughout the system (e.g., channel cards, posters, fliers)
- c. Incorporate general security awareness and emergency preparedness into public announcement messages (security messages and evacuation procedures)
 - o In stations (electronic message boards, voice)
 - o On board vehicles
- d. Post security awareness and emergency preparedness information on the transit agency website
- e. Ensure security awareness materials and announcements emphasize the importance of vigilance and provide clear direction to the public on reporting of suspicious activities
- f. Vary the content and appearance of messages to retain public interest
- g. Increase the frequency of security/emergency awareness activities (e.g. public address announcements) as the HSAS threat advisory level is raised
- h. Issue public service announcements in local media (e.g. newspaper, radio and/or television)
- i. Provide volunteer training to the public for system evacuations and emergency response

Drills and Exercises**8. Conduct Tabletop and Functional drills**

- a. Conduct tabletop exercises at least every six months to exercise system security programs and emergency management plans
- b. Participate as an active player in full-scale, regional exercises held at least annually
- c. Coordinate with regional security partners, including Federal, State, and local governmental representatives and other affected entities (example: other transit agencies or rail systems) to integrate their representatives into exercise programs
- d. Exercise plans and procedures for threat scenarios involving (i) improvised explosive devices (IEDs), (ii) weapons of mass destruction (WMD), and (iii) other high consequence risks identified through the transit agency's system risk assessments
- e. Conduct de-briefings for tabletop and full scale exercises
- f. Develop after-action reports and review results of all tabletop and full scale exercises
- g. Update plans, protocols and processes to incorporate after-action report findings, recommendations, and corrective actions

Establish a Risk Management and Information Sharing Process**9. Establish and use a Risk Management Process to assess and manage threats, vulnerabilities and consequences** (Note: Risk management includes mitigation measures selected after risk assessment has been completed)

- a. - Establish a risk management process that is based on a system-wide assessment of risks and obtain management approval of this process
- b. Ensure proper training of management and staff responsible for managing the risk assessment process

- c. Update the system-wide risk assessment whenever a new asset/facility is added or modified, and when conditions warrant (e.g. changes in threats or intelligence)
- d. Use the risk assessment process to prioritize security investments
- e. Coordinate with regional security partners, including Federal, State, and local governments and entities with shared infrastructure (example: other transit agencies or rail systems), to leverage resources and experience for conducting risk assessments (example: leverage resources such as the Security Analysis and Action Program operated by TSA's Surface Transportation Security Inspectors)

10. Participate in an information sharing process for threat and intelligence information

- a. Participate in information sharing networks or arrangements with:
 - o State and local law enforcement and homeland security officials
 - o DHS' Homeland Security Information Network (HSIN) and its mass transit portal (The HSIN portal enables secure information sharing among transit agencies and passenger rail systems at no cost to users)
 - o FBI Joint Terrorism Task Force (JTTF) and/or other regional anti-terrorism task force (e.g. Terrorism Early Warning Group (TEW), US Attorney's Office)
 - o TSA Surface Transportation Security Inspectors (STSI)
 - o Public Transportation Information Sharing and Analysis Center (PT-ISAC)

11. Establish and Use a Reporting Process for Suspicious Activity (internal and external)

- a. Through training and awareness programs, ensure transit agency employees understand the what, how, and when to report observed suspicious activity or items
- b. Use exercises to test employee awareness and the effectiveness of reporting and response procedures

- c. Ensure public awareness materials and announcements provide clear direction to the public on reporting of suspicious activity
- d. Maintain protocols to ensure that designated Security Coordinator(s) report threats and significant security concerns to appropriate law enforcement authorities and TSA's Transportation Security Operations Center (TSOC)
- e. Maintain protocols that ensure actionable security events are included in reports to the FTA's National Transit Database (NTD)

Facility Security and Access Controls

12. Control Access to Security Critical Facilities with ID badges for all visitors, employees and contractors

- a. Identify security critical facilities and assets
- b. Use ID badges for employee access control
- c. Use ID badges for visitors and contractors
- d. Develop a written policy and procedures for restricting access (e.g.: card key, ID badges, keys, safe combinations etc) to security critical facilities and assets. Ensure that policy is updated when new threats, audit findings or circumstances warrant.

13. Conduct Physical Security Inspections

- a. Conduct, monitor and document facility security inspections (e.g., perimeter/access control) on a regular basis, with increasing frequency in response to elevation of the HSAS threat advisory level
- b. Develop and use protocols for vehicle (e.g. buses and rail cars) inspections that correspond to HSAS threat advisory levels
- c. Develop and use protocols for inspections of rights-of-way corresponding to HSAS threat advisory levels
- d. Vary the manner in which inspections of facilities, vehicles, and rights-of-way are conducted to avoid setting discernible and exploitable patterns and to integrate unpredictability

Background Investigations**14. Conduct Background Investigations of Employees and Contractors**

- a. Conduct background investigations (i.e., criminal history and motor vehicle records) on all new front-line operations and maintenance employees, and employees with access to sensitive security information and security critical facilities and systems.
- b. Conduct background investigations on contractors, including vendors, with access to sensitive security information and security critical facilities and systems.
- c. Ensure that background investigations are consistent with applicable laws
- d. Document the background investigation process, including criteria for background investigations by employee type (operator, maintenance, safety/security sensitive, contractor, etc.)

Document Control**15. Control access to documents of security critical systems and facilities**

- a. Identify and protect documents on security critical systems, such as tunnels, facility HVAC systems, and surveillance, monitoring, and intrusion detection systems
- b. Limit access to documents on security critical systems to persons with a need to know
- c. Identify a department/person responsible for administering the document control policy
- d. Ensure that the security review committee (or other designated group) has meetings/briefings that include reviewing document control compliance issues

16. Process for handling and access to Sensitive Security Information (SSI)

- a. Be familiar with the requirements pertaining to the proper-handling of SSI materials (reference 49 CFR Parts 15 and 1520), such as security plans and risk and vulnerability assessments

- b. Ensure that the Security Review Committee (or other designated group) regularly reviews matters pertaining to the access to and handling of SSI material

Security Program Audits

17. Audit Program

- a. Conduct security program audits at least annually
 - o Internal
 - o External

- b. Ensure that the Security Review Committee (or other designated group) addresses the findings and recommendations from audits, and updates plans, protocols and processes as necessary. (see 3c)

Footnotes:

(1) These action items covers all modes directly operated or contracted by the transit agency (e.g., bus, bus rapid transit, light rail, heavy rail, commuter rail, paratransit etc.)

(2) For additional information please reference:

FTA Safety & Security website: <http://transit-safety.volpe.dot.gov>

(3) Contact MTActionItems@dhs.gov for Questions or Comments

December, 2006

It is not clear to me, and I wonder if it is clear to the agencies, how this assessment process works, what kind of weights are assigned to each of these items, how they relate to each other. It reminds me of some of the documents we have seen on risk assessment, where they are so complicated and so multifaceted that one wonders about their usefulness as very precise measurement tools.

So I cited and I am alarmed about the 23 percent figure. But the reason I wanted to bring it up again was that I am not terribly confident as to what that 23 percent figure really means.

Was it clear, do you think, to the transit and rail entities of what requirements they were being assessed on and what constituted a passing grade? Was it clear how all this was being calculated?

I would be interested in your oral response, but, more than that, I would be interested in a more detailed response for the record as to the way this is scored, the way this actually works, and maybe further refinements that you are considering to make this a more precise measurement tool.

Mr. SAMMON. Thank you. I am glad you asked that question.

The assessments are done by TSA transportation security inspectors voluntarily with the agencies. The 20 percent is actually—if you look at these—and I think the confusion here is looking at these as compliance standards versus excellence standards. The only way you were in that category, as terms of 23 percent, was if you had a greater than 90 percent score over all 17 measures. If any one of the 17 measures, any one, was below 70 percent, you didn't get credit in the category.

So, this is really the top of the top. It is kind of like looking at grading in school—that these are all “A”s. There is an elite group that are in that top category.

AGENCY PERFORMANCE ASSESSMENT CONT'D

And also what we do with our security inspectors and our sharing best practices among the agencies, our idea is: “Here is the top group. How do we get the others migrated to that level?” They are people—again, as you said, 23 percent in the top group—in the transit area, to work with the transit agencies on a voluntary basis to get them to improve. Maybe someone needs more people trained, maybe they need a better security plan, whatever. But it is an interaction, a constant interaction, with the agency to improve their overall level of security, to improve the scoring. And, as we have seen and the OIG report has addressed, where we have gone back to rescore, we have seen improvements with the agency.

So, it is not like you know, the airline compliance, where compliance is passing grade. This is an excellence grade. Our idea is to continue to work with the agencies and migrate them to excellence as opposed to passing and, frankly, if we had scored people in this thing and they had all passed, I would worry about the standards. So these are very high standards.

There are agencies who make the standards and achieve it, which are very good agencies; others which are close. But, if you have one miss on any of the 17, you don't get in the club.

Mr. PRICE. That is helpful. If you could detail a more elaborate account of how this works and how you plan to utilize it, going for-

ward. That is helpful, though, to understand the kind of tool this is.
[The information follows:]

**DHS ANNUAL PERFORMANCE REPORT
MASS TRANSIT AND PASSENGER RAIL PERFORMANCE MEASURE**

- a. How is it scored?
- b. How does it actually work?
- c. Is there any consideration for further refinements to make this a more precise measurement tool?
- d. How will it be utilized going forward?

Response:

- For FY08, DHS has published on its public website an Annual Performance Report presenting metrics in particular areas of critical infrastructure protection and security.
 - Among these is a long-term outcome measure for mass transit and passenger rail security derived from the results of the security assessments conducted under the Baseline Assessment for Security Enhancement (BASE) program.
 - The measure states the percentage of the largest 50 (in passenger volume) mass transit and passenger rail agencies that are in “full compliance” with the 17 Security and Emergency Management Action Items.
 - The Action Items encompass areas foundational to an effective security program, such as security and emergency management plans, accountability, planning coordination, training, public awareness, drills and exercises, HSAS threat level security protocols, risk management, information sharing and incident reporting, physical security, access controls, background checks, information and personnel security, and internal security audits.
- TSA Transportation Security Inspectors-Surface assess the level of performance in the Action Items comprehensively using a 200+ question checklist during a thorough review of the overall security program in which the mass transit or passenger rail agency’s security officials participate.
- The reported figure of 23% reflects those 11 of the 48 largest (in passenger volume) mass transit and passenger rail agencies assessed that achieved the high standard set by the measure. The “report” referenced in the January 29, 2009, USA Today story is a single table in the much longer Annual Performance Report of numerous performance measures.
- Essential considerations in the mass transit and passenger rail performance measure:
 - The performance standard is high – to be considered in “full compliance” a mass transit or passenger rail agency must achieve a 90% average score across all 17 Security and Emergency Management Action Items, with no one category scoring under 70%.
 - Though six additional agencies achieved a 90%+ average score on the BASE assessment, they did not meet the high standard because of their performance in a single category. These agencies, and all others ranked among the largest 50, will be re-assessed during 2009. To date, second assessments on five agencies have shown substantial improvements in performance.

- The overall average score on all 17 Action Items among the largest 50 agencies (the scope of the report) was 80% - quite solid performance for the first round of the most thorough security assessments these agencies have yet undergone.
 - The target for FY08 was to get 30% of the agencies to the high standard reported. Among the 48 assessed agencies, 11 achieved the objective - 23% - but, more notably, 77% of the target.
- Moving forward, TSA is acting to improve the measure based on the lessons of experience and review and recommendations provided by the Government Accountability Office (GAO). Steps taken include clarifying the current long-term performance measure to enhance understanding of its significance, as discussed above, as well as developing a succeeding measure that focuses on evaluating risk reduction, consistent with TSA's broader cross-modal approach to achieve objectively measured risk reduction.
- The proposed measure calculates BASE performance and a threat and consequence factor to produce an overall risk score for the system. Results can be calculated cumulatively or by Action Item. By comparing the risk score for a subsequent BASE assessment to that which resulted from the previous or initial assessment, a percentage in risk reduction will be determined.

With that, I am going to adjourn the hearing, with thanks to all of you. We clearly have a lot to work on. We will look forward to working together and seeing our witnesses here on the 31st.

And we wish our transit directors the best. We thank you for your contribution here today.

The Subcommittee is adjourned.

TUESDAY, MARCH 31, 2009.

**SECURING THE NATION'S RAIL AND TRANSIT SYSTEMS,
PART 2**

WITNESSES

**JOHN SAMMON, ASSISTANT ADMINISTRATOR OF TRANSPORTATION
SECTOR NETWORK MANAGEMENT, TRANSPORTATION SECURITY AD-
MINISTRATION**

**W. ROSS ASHLEY, ASSISTANT ADMINISTRATOR OF GRANTS PRO-
GRAMS, FEDERAL EMERGENCY MANAGEMENT AGENCY**

OPENING STATEMENT OF CHAIRMAN PRICE

Mr. PRICE. The Subcommittee will come to order. Good morning. Today we are reconvening our hearing on securing our nation's rail and transit systems.

On March 12, we heard from the Los Angeles Metropolitan Transportation Authority and the New York Metropolitan Transportation Authority on the difficulties they have had in getting DHS approval to spend their federal grant dollars in a timely fashion. At that time approximately 90 percent of the 2006 rail and transit security grant funds remained unspent because DHS and the transit agencies were still negotiating what would be eligible projects. Meanwhile, our rail and transit security vulnerabilities go unaddressed. That is not something that this subcommittee can accept.

I want to be clear. This is not just a New York and Los Angeles problem, although those were the systems we heard from directly in this forum. Other Tier 1 transit entities, those systems with the most riders and high security risks have also experienced problems with spending their grant awards.

Since the hearing, we have heard from other entities about their similar difficulties with DHS, and I will just cite a very few examples in their own words.

The Philadelphia Transit Authority has been promised resolution on how their 2006 transit security grant can be spent for the past six months, but because of confusion with the Pennsylvania Emergency Management Association, and FEMA, this process has moved "nowhere in months." This money funds projects in Philadelphia and in conjunction with New Jersey Transit. In the case of Philadelphia, if they do not receive the grant dollars their project will be incomplete. In the case of New Jersey, they are still waiting on approval to purchase 35 mobile trace units, with 10 of those units to be deployed to the Philadelphia Transit Authority.

The Washington Metropolitan Area Transit Authority has informed the Subcommittee that while they have had problems with the slowness of 2006 grant awards, it was largely because of the states—Virginia and Maryland—adding a layer of complexity that

delayed application approvals and alterations to their plans. This entity also expressed concern about the timeliness of the 2007 grants. At this time TSA has not yet completed its reviews.

Atlanta requested and received an extension to spend the remaining 37 percent of its fiscal year 2006 grants. According to that transit authority, there were delays in receiving the authorization to expend funds primarily because of the environmental process and requests for more information from DHS after the submittal of initial concepts.

Because of the extreme frustration expressed by Subcommittee members earlier this month about the slowness of actually spending grant dollars appropriated two or three years ago, Ranking Member Rogers and I asked TSA and FEMA to come back with some solutions to this problem. We believe this process needs to be streamlined.

So Mr. Ashley and Mr. Sammon, we welcome both of you back. We have your report in front of us, although I hate to say it was submitted only late yesterday afternoon. We do have the report, and we will spend time this morning discussing how DHS plans to remedy the slow spending of rail and transit security grants from 2006, 2007 and 2008, as well as how your agencies will reach 100 percent draw-down.

I am pleased to note that in 2009, when DHS announces the awards for Tier 1 rail and transit entities, there no longer will be any additional approval process required by TSA. In comparison, this TSA approval phase took 285 days after the 2006 announcement. This change alone would be a vast improvement because rail and transit entities could begin spending money on these critical projects much faster. We do want to know more about how this rather striking change is going to work.

And there is an additional problem. This report does not provide the requested timeline of how previously awarded funds will be 100 percent drawn down. So one might conclude that you are fixing the problem for 2009 while letting previous awards wither on the vine. We hope that is not true, but from reading the report, one would not know any different. So we get into this discussion right away.

Let me first recognize Ranking Member Hal Rogers for any statement he wants to make.

[The information follows:]



COMMITTEE ON APPROPRIATIONS

David Price (D-NC), Chairman, Subcommittee on Homeland Security

FOR RELEASE UPON DELIVERY
Tuesday, March 31, 2009
202-225-1784

Media Contact: Phil Feagan

OPENING STATEMENT OF CHAIRMAN DAVID PRICE
***Panel 1: Reconvened Hearing on Securing Our Nation's Rail and
Transit Systems***
March 31, 2009 / 10:30 am

This morning we are reconvening our hearing on Securing Our Nation's Rail and Transit Systems. On March 12th, we heard from the Los Angeles Metropolitan Transportation Authority and the New York Metropolitan Transit Authority on the difficulties they have had in getting DHS approval to spend their federal grant dollars in a timely fashion. At that time, approximately 90 percent of the 2006 rail and transit security grant funds remained unspent because DHS and the transit agencies were still negotiating what would be eligible projects. Meanwhile, our rail and transit security vulnerabilities go unaddressed, and that is not something that this Subcommittee can accept.

I want to be clear; this is not just a New York and Los Angeles problem. Other Tier 1 transit entities—those systems with the most riders and highest security risks—also have experienced problems spending their grant awards. Since this hearing, we have heard from other entities about their similar difficulties with DHS. Let me cite some examples (in their own words):

- The Philadelphia Transit Authority has been promised resolution on how their 2006 Transit Security Grants can be spent for the past 6 months, but due to confusion with the Pennsylvania Emergency Management Association and FEMA, the process has moved “nowhere in months”. This money funds projects in Philadelphia and in conjunction with

New Jersey Transit. In the case of Philadelphia, if they do not receive the grant dollars, their project will be incomplete. In the case of New Jersey, they are still waiting on approval to purchase 35 Mobile Trace units, with 10 of those units to be deployed to the Philadelphia Transit Authority.

- The Washington Metropolitan Area Transit Authority has informed the Subcommittee that while they have had problems with the slowness of 2006 grant awards, it was largely due to the states – Virginia and Maryland – adding a layer of complexity, which delayed application approvals and alterations to their plans. This entity also expressed concern about the timeliness of the 2007 grants. At this time, TSA has not yet completed their reviews.
- Atlanta requested and received an extension to spend the remaining 37 percent of its fiscal year 2006 grant. According to the transit authority, there were delays in receiving the authorization to expend funds due primarily to the environmental process and requests for more information from DHS after submittal of initial concepts.

Because of the extreme frustration expressed by Subcommittee Members earlier this month about the slowness of actually spending grant dollars appropriated two or three years ago, Ranking Member Rogers and I asked TSA and FEMA to come back with solutions to this problem. We believe that this process needs to be streamlined. Mr. Ashely and Mr. Sammon, we welcome you back. We have your report in front of us and will spend time this morning discussing how DHS plans to remedy the slow spending of rail and transit security grants from 2006, 2007, and 2008, as well as how your agencies will reach a 100 percent draw-down. I am pleased to note that in 2009, when DHS announces the awards for Tier 1 rail and transit entities, there no longer will be any additional approval process required by TSA. In comparison, this approval process took 285 days after the 2006 announcement. This change alone would be a vast improvement because rail and transit entities could begin spending money on these critical projects much faster. But this report does not provide the requested timeline of how previously awarded funds will be 100-percent drawn down. It appears you are fixing the problem for 2009 while letting previous awards wither on the vine.

Before we get into this discussion, let me recognize Ranking Member Rogers for any statement that he may wish to make.

###

OPENING STATEMENT OF RANKING MEMBER ROGERS

Mr. ROGERS. Gentlemen, it is not often that we have to go back a second time. You do not have the time, we do not have the time. So this ought to be good. It better be really good because we do not want to do it a third time.

In many ways TSA is the public face of Homeland Security. It is not only the agency millions of people interact with daily at the airports, but it is also what many of us think about when discussing our response to the attacks of 9/11, and since its creation shortly after those tragic and unforgettable events, TSA has made tremendous progress.

Screening and credentialing programs such as TWIC and Secure Flight, once symbols of ineffectiveness and disfunction, are now viable programs, properly identifying travelers and transportation workers. Just this past week, TSA issued its one millionth TWIC card, and since January, Secure Flight has begun screening operations.

But in spite of this laudable progress, many challenges certainly remain, and securing the surface transportation sector is one of those big challenges.

We can only do so much to secure these open systems and the federal government plays a limited role in what is primarily a state and local operating environment. Rail and transit grants jointly administered by FEMA and TSA represent what is perhaps the signature contribution of the federal government in this arena. But despite visible threats to transit systems around the world, and more than \$1.5 billion in appropriations over the last few years, we appear to be falling down on that front. So I look forward to hearing how we are going to get these grants back on track and get real security solutions in place.

And so Mr. Ashley, Mr. Sammon, we meet again. I enjoy being with you, but I hope this is the last time we are blessed with it this year, and I trust you both have come prepared so we can get to the bottom of why so little of the grant funding has moved out the door.

[The information follows:]

OPENING STATEMENT

CONGRESSMAN
Hal Rogers



FIFTH DISTRICT • KENTUCKY

Offices in
Washington, D.C.
Somerset, Prestonsburg,
Hazard

Contact: Stefani Zimmerman

202.225.4601

**Committee on Appropriations
Subcommittee on Homeland Security**

Opening Statement (Panel #1):

*Securing the Nation's Rail and Transit Systems and
Improving the Efficiency of the Aviation Security System*

Witnesses:

*Mr. John Sammon, Assistant Administrator of Transportation Sector
Network Management, TSA*

Mr. W. Ross Ashley, Director of Grants Program Directorate, FEMA

10:00 AM | Tuesday | March 31, 2009 | 2362-B

Thank you, Mr. Chairman, and welcome to our distinguished guests.

In many ways, TSA is the public face of homeland security. It is not only the agency millions of people interact with daily at our Nation's airports, but it is also what many of us think of when discussing our response to the attacks of 9/11.

And since its creation shortly after those tragic and unforgettable events, TSA has made tremendous progress.

Screening and credentialing programs such as TWIC and Secure Flight – once symbols of ineffectiveness and dysfunction – are now viable programs properly identifying travelers and transportation workers. Just this past week, TSA issued the one millionth TWIC and, since January, Secure Flight has begun screening operations.

But, in spite of this laudable progress, many challenges certainly remain.

Securing the surface transportation sector is one of those challenges. We can only do so much to secure these open systems and the Federal government plays a limited role in what is primarily a State and local operating environment. Rail and transit grants – jointly administered by FEMA and TSA – represent what is perhaps the signature contribution of the Federal government in this arena. But, despite visible threats to transit systems around the world and more than \$1.5 billion in appropriations over the past few years, we appear to be falling down on that front.

So, I look forward to hearing how we are going to get these grants on track and get real security solutions in place.

Mr. Ashley and Mr. Sammon, we meet again. I trust you both have come prepared so we can get to the bottom of why so little of the grant funding has moved out the door.

Thank you, Mr. Chairman.

###

Thank you, Mr. Chairman.

Mr. PRICE. Thank you. We have your joint statement which will be entered fully in the record, but we would like to have your five-minute summaries, and we will start with Mr. Sammon.

OPENING STATEMENT OF MR. SAMMON

Mr. SAMMON. Good morning, Chairman Price, Ranking Member Rogers, Distinguished Members of the Subcommittee, and my colleague, Mr. Ashley, from FEMA.

As the federal agency responsible for transit security, TSA shares the Subcommittee's concerns about draw down and expenditure rates. We want to thank you for providing us the opportunity to discuss what TSA has done to improve its portion of the transit grant process and what we expect to do to improve the flow of state and local grant expenditures.

TSA owns the front end of the process. We are responsible for identifying security priorities and assigning projects to achieve the highest risk reduction. We recognize the timeline involved in this, and we have taken steps to reduce that process down from 345 days in fiscal year 2006 to 60 days in 2009, and 60 days means all the grants as of Friday are out and over to FEMA. So the process chart that we passed out to this Subcommittee and have shown everyone is not an expectation or a plan or whatever else, it actually happened.

We have done that largely by taking the Investment Justification process and putting that up front rather than negotiating over a period of months.

So, TSA has fixed the front end. We have taken it down to 60 days, and we think that is a reasonable period of time to review grant applications, sort them, put them in proper order, make priorities, and determine awards.

Secondly, TSA is also committed to fixing the back end of the process. I know that transit agencies are conducting grant-related security activities, so I want to know why the draw-down rates are so low. This Thursday, I am beginning a series of meetings around the country to determine why the draw-down rates are so low and what can be done to expedite them. I am going to start with the largest agencies, the MTA in New York on Thursday; sit down with their folks, and map out the process in terms of determining where security projects are in the planning and execution process. We intend to map each state, local and federal process to identify the root causes of expenditure delay versus planned.

Finally, we have addressed the recommendations of Mr. Morange and Mr. Eckles and we agree with approximately 17 different recommendations. We agree with six; recommendation nine we agree with in principle, additional work has to be done; and we disagree with two recommendations, one being that we should contact only the transit grant agency and not the primary security provider, and the other involving of issuing guidance before the appropriation is enacted.

So, finally, I would like to leave this Subcommittee that TSA has reduced the front end of the process, the part that TSA is responsible for, and we are determined to find out where the money is

sitting in terms of the approximately three-quarters of a billion dollars between 2006 through 2008. Thank you, sir.

Mr. PRICE. Thank you. Mr. Ashley.

OPENING STATEMENT OF W. ROSS ASHLEY

Mr. ASHLEY. Good morning, Chairman Price, Ranking Member Rogers, Members of the Committee. Thank you for having us back here for round two.

Earlier this month I appeared at this Subcommittee with Mr. Sammon as well as representatives from New York and Los Angeles. During that hearing, Mr. Chairman, you and Congressman Rogers as well as other members of the Subcommittee, expressed concern over several issues. Among those—

Mr. PRICE. Mr. Ashley, make sure your microphone is on or you are speaking into it.

Mr. ASHLEY. How is that? Is that better?

Mr. PRICE. Good.

Mr. ASHLEY. Among these concerns were the following: the amount of time that is required to obligate and draw down critical transit security grant funds; the roles and responsibilities of TSA and FEMA; as Mr. Sammon mentioned, the specific responses to recommendations made both by L.A. and New York transit agencies; and solutions to facilitate rapid draw down on transit security grant funds.

At the Committee's direction, FEMA and TSA constructed and submitted our joint report on these concerns, and we are pleased to be here today to discuss the report. The report highlights areas of improved results as well as identified specific actions to be taken in order to continue to enhance programmatic results.

To illustrate this point, it has been said twice now, the report submitted includes a chart entitled "Processing Time for TSA Grants," clearly illustrating the substantial progress made in the time between application submission and when funds are available to draw down.

The report also identifies specific actions to be taken in order to continue to make funds available faster, measure results, increase capability, and finally, to facilitate increased draw down rates.

There is one final point I believe requires mention and I believe we talked about it briefly in our interoperable communications hearing we had as well. From discussions I have had with New York and Los Angeles these past weeks, it is not necessarily accurate to equate the rate of drawdown of rail and transit funds with the lack of activity by the recipient agencies to increase security and safety of their systems.

It is true that grant funds may have become available for use not as quickly as all of us would have liked, but that does not mean money is not being used. Critical grant-funded projects are underway in every state, and they are being executed today.

Again, I would like to thank you for the opportunity to appear before you to discuss these matters, and I am happy to take questions.

[The information follows:]

105

JOINT STATEMENT

OF

THE HONORABLE W. ROSS ASHLEY

**ASSISTANT ADMINISTRATOR
GRANTS PROGRAM DIRECTORATE
FEDERAL EMERGENCY MANAGEMENT AGENCY
U.S. DEPARTMENT OF HOMELAND SECURITY**

AND

JOHN P. SAMMON

**ASSISTANT ADMINISTRATOR
TRANSPORTATION SECTOR NETWORK MANAGEMENT
TRANSPORTATION SECURITY ADMINISTRATION
U.S. DEPARTMENT OF HOMELAND SECURITY**

BEFORE

THE

**SUBCOMMITTEE ON HOMELAND SECURITY
COMMITTEE ON APPROPRIATIONS
U.S. HOUSE OF REPRESENTATIVES**

MARCH 31, 2009

WASHINGTON, D.C.

Chairman Price, Ranking Member Rogers, Members of the Subcommittee, my name is Ross Ashley and I serve as Assistant Administrator of the Grants Program Directorate within the Department of Homeland Security's (DHS) Federal Emergency Management Agency (FEMA). Earlier this month I appeared before this Subcommittee along with Mr. John Sammon, the Assistant Administrator of Transportation Sector Network Management at DHS' Transportation Security Administration (TSA) to discuss the security of the nation's rail and transit systems and the effectiveness of the federal funding that has been provided to protect these systems from acts of terrorism or man-made disasters. This statement reflects a joint communication to the Committee from both FEMA and TSA.

At that time we were also joined by Mr. Bill Morange, the Deputy Executive Director, Director of Security of the New York Metropolitan Transportation Authority, and Mr. Jack Eckles, the Deputy Executive Officer, System Safety, Security, of the Los Angeles County Metropolitan Transportation Authority.

During that earlier hearing Mr Chairman, both you and Congressman Rogers, as well as other Members of the Subcommittee, expressed concern over several issues. These included the amount of time it takes to obligate and draw down transit and rail grant funds; the roles and responsibilities for FEMA and TSA in administering these grant funds and managing these programs; the grant process itself; and solutions for how FEMA and TSA can reach 100 percent draw down rates on the grant funding.

To address these concerns, the Subcommittee directed FEMA and TSA to jointly develop an efficiency review that focuses on the following issue areas:

- A brief description of the problems related to the slowness of spending rail and transit security grants. The Subcommittee had requested that this report include the current status of the obligation and draw down numbers from 2006, 2007, and 2008. The Committee had also requested a detailed status of California and New York activities relating to the obligation and draw down of grant funds.
- A description of FEMA's and TSA's roles in the administration of rail and transit grant funds including a discussion of responsibilities for approving the authorization of fund draw downs and solutions for hastening the draw down process. A detailed flow chart of the grant process.
- A discussion of solutions for hastening the draw down process, including addressing the recommendations made by Mr. Morange and Mr. Eckles.

That report is complete and was submitted to the Subcommittee. I am pleased to appear before the Subcommittee today to discuss that report and to continue our earlier discussions. As the report discusses, substantial progress has been made, and continues to be made in providing funding and approving security investments for our nation's rail and transit systems.

To illustrate this point, the report submitted to the Subcommittee includes a chart entitled "Processing Time for TSGP Grants" clearly illustrating the substantial progress made in

hastening the amount of time between the awarding of grant funds and the ability of recipient agencies to use those funds.

In summary the chart shows the amount in days from when applications are received to when agencies have access to the funds. TSA has significantly revised the process to review and approve Tier I projects, resulting in substantial improvements in approval times each fiscal year. After applications are received, DHS has 60 days to act on the awards, per Congressionally-mandated timelines. After the 60-day period, DHS announces the awards. In FY06, it took approximately 285 days after awards were announced to Tier I project approvals. That timeline has been reduced to 0 days for FY09, meaning that all Tier I projects will be approved when the awards are announced. After project approval, FEMA takes approximately 60 to 90 days to complete budget reviews and the award package/obligation process. After the FEMA review is complete, agencies are issued "Release of Funds" memos allowing them to begin drawing down on the funds.

FEMA and TSA continue to work within our authorities to hasten the availability of these funds. One area of focus is FEMA's legally-required environmental planning and historic preservation (EHP) compliance review. As the Subcommittee is aware, and as the report discusses in additional detail, FEMA is required to consider the potential impacts to the human and natural environment of construction projects proposed for FEMA funding. FEMA's EHP review ensures that grant-funded activities comply with various Federal laws including: the National Environmental Policy Act (NEPA), the National Historic Preservation Act, the Endangered Species Act, and Executive Orders on Floodplains, Wetlands and Environmental Justice. The goal of these compliance requirements is to protect our nation's water, air, coastal, wildlife,

agricultural, historical, and cultural resources, as well as to minimize potential adverse effects to children and low-income and minority populations.

As you know, these grant programs transitioned into FEMA in the spring of 2007. FEMA and TSA are working closely with grant recipients to provide these recipients a clearer understanding of Federal EHP requirements, through training, outreach, improved and more detailed grant guidance, and development of a stakeholder working group. FEMA is also working internally to improve the integration of EHP requirements and processes into these grant programs, so that EHP considerations are addressed early on, rather than as an afterthought. Grant recipients are required to provide FEMA with a detailed project description, so that FEMA can identify and assess any potential impacts the project may have on environmental resources and/or historic properties. The key is for grant recipients to be aware of and to take EHP considerations into account during project formulation; consideration of EHP requirements during project formulation and a detailed project description will help ensure that impacts to environmental and historic resources are minimized during project implementation which in turn means the EHP review process is completed in a timely manner and grant funds are not delayed. Fortunately, projects funded under these rail and transit programs involve security enhancements at existing facilities, and therefore are not the types of projects expected to have adverse impacts on the environment and are projects that qualify for a Categorical Exclusion under NEPA. To date, a total of only 14 TSGP projects have required review by FEMA's EHP Specialists, the majority of which were reviewed in less than 30 days once FEMA received adequate information from the grant recipient about the nature and extent of proposed projects. Improving grant recipients' awareness of EHP requirements and collecting project information as soon as possible are two important steps in improving the timeframe of FEMA's EHP review.

Mr. Chairman, during today's hearing we will discuss these and additional aspects of the joint FEMA and TSA report in greater detail. However there is one point I believe requires our attention. That point is not to equate the rate of the draw down of rail and transit funds with a lack of activity by recipient agencies to increase the security and safety of their systems. It is true grant funds may not become available for use as quickly as all of us would like, but that does not mean that the money is not be designated for use and that the money is not being used. Grant-funded projects are underway in every state and are being executed today. The reality is that it does take time for states to draw down grant funds. The report addresses this in more detail.

Mr. Chairman, Congressman Rogers, Members of the Committee, this concludes my statement. I look forward to discussing our report in more detail and addressing any questions the Committee may have.

APPROVAL OF PROJECTS BEFORE AWARD AND BACKLOG

Mr. PRICE. Thank you. We will turn directly to questions, and I will start with a couple of questions that I pretty well telegraphed in my opening statement because I think they are very obvious questions from the report you have submitted.

Your testimony in particular, Mr. Sammon, restated that you intend to move the approval process to zero days after DHS announces how much each transit entity is awarded in fiscal 2009. Now, that would mean going from 285 days for the distinctive TSA part of this process, to zero days in 2009.

Now, we know, of course, that TSA and FEMA have been part of this statutorily-required 60-day process that precedes the 285 days you are talking about, and then the TSA process kicked in. So presumably in going from 285 days to zero you plan to move the work and the review that you do into that initial 60 days, assuming you are still going to review and approve all the projects before award. I think we need some clarification of that. How exactly is it going to work.

Now, if you are truly able to review and approve projects prior to award, then this is obviously a step in the right direction to avoid the lengthy delays between your award time and when you actually allow transit agencies to spend the funding. Nonetheless it is a major change.

And my second point is that it leaves largely unaddressed the process that remains from the previous years of funding. So the second question is what are you doing to clear the backlog? Has TSA approved all projects for 2006, 2007, 2008? I suspect the answer to that is no. If not, what is the sense in releasing current year funds without dealing with the older projects? Unless I missed it, the report does not deal with that.

So two questions: How are you going to make this rather extraordinary turnaround? What does it imply in terms of the sequencing and the content of the review process? And then secondly, what about the pre-2009 years?

Mr. SAMMON. Those are two very good questions. Thank you, Mr. Chairman.

First of all, in terms of what we have done the chart is showing what we have actually done for the 2009 process, and we have turned over all during that 60-day period. We have gone through the review of the projects down through the ranking of the projects. But, the one big change that has happened is the projects are going directly to the agency, we do not have the state involvement in it. We have been able to move the investment Justifications up into that 60 day period and by doing that, we have basically cut the cord, award and rank the projects, and send them to FEMA.

In the past, after the initial period, the states were awarded funds and the Investment Justification process went back and forth between TSA and the agency for months. We have completed the review in 2009—this is done. This is not a plan that we intend to do for all the 60-day projects, we have met and sent over to, the award, the grant award we sent to FEMA on Friday afternoon. So, TSA is done with our portion of the process, and we were able to do that by moving the Investment Justification process the ana-

lysts who put the project priority on a ranking system, a numerical ranking system, which makes it very easy to rank and order these projects. We do not have to go through a complex period of paneling and so on and so forth by working with the agencies throughout the year to get their project priorities in line. So for the front end of the process, we have taken down the time significantly.

The interim years, starting with fiscal year 2006, was a mess. It was a hands-off process, and there was no communication allowed back and forth between the agencies, and that was a messy, messy process. Fiscal year 2006 would have been lower—TSA is composed of the blue and red bars in this chart. I believe that 2007 would have been lower. A supplemental appropriation was enacted and in the supplemental, TSA pushed for increased use of operational funds. The capital grant programs and projects take the most time because there is engineering involved and bidding and outsourcing. We have pushed to include things like the canine teams, paying for canine, paying for mobil screening teams, paying for train surges, bus surges and so on, which agencies do not have to outsource or bid; they simply do it with their own people, and we have pushed for that recommendation. But that change that slowed the process down in 2007. I think 2007 would have been better.

And, in 2008, because Congress—I think it was a good thing to do, that Congress did in terms of eliminating the match, the people for a number of the previously applied projects went back and said, well, gosh, if I do not have a match requirement let me resubmit my projects and we worked with them to do that.

So, in 2009, with a clean process, everyone knew the rules upfront and, we were able to take it down to 60 days.

Now, as you said, that still does not address the approximately three-quarters of a billion dollars sitting out there, and that is why I am personally going to go, starting in New York, to identify where the money is sitting in terms of between the local planning, the local procurement process, then the state and the state processes—the previous money from 2008, back to 2006—because it all went through the state, the state process and the federal process, we will determine the root cause of where the money sits versus plan, and identify those delays because that is the issue—what is the cause of the delay. In two weeks we simply did not have enough time to go around the country and do this.

The good thing about this process, getting it down, getting back to you and reporting back to you where this is, there are only approximately seven states and approximately 15 or 16 agencies that represent the vast majority of this money. So, we should be able to get back to you and tell you where this is, where it is sitting according to their plan, what we think the delays are, and what we think we ought to do to speed up this backlog of money. If we hit the front end process, the new process is improved, what do we do with the old process, and we are going to have to tell you that, and today we did not have enough time in two weeks to be able to tell you that.

TSA APPROVAL OF BACKLOG PROJECTS

Mr. PRICE. So TSA has not approved all the projects for these previous years—2006, 2007, 2008? What you are telling me, as I

understand it, is that this approval is still tied up in these consultations with the major states involved?

Mr. SAMMON. All of the 2008s are approved. All of the 2007s are redos. What we want to do is go through a detailed examination. For instance, I am going to meet with Rob Marciano and Mr. Morange on Thursday; sit down and take their projects and outline where they are, what is their expenditure plan, where is the money versus their expenditure plan, so we can map out and get back to you and say, here is the stuff that they plan to spend, here is where they are in actual spending, and if there is a federal delay, a state delay or a local procurement delay, or whatever else, we will be able to outline that to you.

The issue they have explained to us, the capital projects they have to do, they have to do design work. Once the grant order is made, then they start the design process, the procurement process, the actual construction process, so those things do take time, and they do have a plan for how they expect to spend it. But, what we want to know is versus that plan what are the inherent—what are the inherent delays. What kind of delays are being imposed on them from being unable to spend the money before they plan to spend it? We want to do that.

Mr. PRICE. All right. I think case by case one can understand what these discussions are about, but I am still having trouble with this transition that you are proposing, to basically go to zero days of this kind of TSA review you are talking about beyond that initial 60 days. Are we to assume that these kinds of protracted discussions that you are involved in with regard to these monies from 2006, 2007 and 2008 will no longer be necessary or somehow they will be telescoped into that first 60 days?

I do not understand why the process you are proposing for 2009 has so little relevance apparently to clearing up this backlog.

Mr. SAMMON. The previous money that is hanging out there, and the numbers are from the GAO in terms of what is approved, and what the bars represent is the close of the application period. So when the application closes, everybody has to have their application closed by the time that money is available for the agency to spend.

But, we have taken the closed, the TSA portion, from the close of the applications to the time we approve the applications and move them to FEMA, the 60 days. The TSA portion takes 60 days. We think that is a reasonable period of time going forward.

The previous years' money, most of those awards have been made except there are, again in 2008 a number of people when they saw that they did not need a match anymore due to the appropriation act, have been going through a process of trying to re-negotiate projects and move money around from one project to another. We expect to have that cleaned up pretty shortly.

Mr. PRICE. Well, we will want to figure out with you what is a reasonable timeframe for getting your full accounting of this.

Mr. SAMMON. We expect to do this as quickly as possible. I am personally going to New York, and going to California next week.

Mr. PRICE. What is a reasonable timeframe? Thirty days?

Mr. SAMMON. I think it will take more than 30 days. What I would like to do is report back to the Committee staff in 30 days

to tell you where we are. We may, with hitting four or five agencies, account for 50 percent of the money, for instance, and I think we should report to you under those intervals and get back to it, commit to it. All 44—44 agencies account for 92 percent of the money, but as I said, 50 agencies account for the vast majority of the money, and we will see the process breakdown or delays, I think, pretty quickly.

Mr. PRICE. Well, we will return to this.

Mr. ROGERS, your questions?

INTERIM REPORT AND FINAL REPORT

Mr. ROGERS. I want to follow up on that. We need a timeline here. You are going to report interinely in 30 days, right?

Mr. SAMMON. Yes, sir.

Mr. ROGERS. And when can we expect a final report?

Mr. SAMMON. I think we should be able to get the vast majority of this accounted for and have a report cleared out through the Federal Government in perhaps about 120 days.

Mr. ROGERS. I am sorry?

Mr. SAMMON. About 120 days, have it cleared through DHS so on and so forth. The clearance process is also a significant portion of getting the report to you.

Mr. ROGERS. So four months from today.

Mr. SAMMON. Yes.

Mr. ROGERS. We should have this all clear?

Mr. SAMMON. You should know where the money is and what we think can be done to get it out faster, yes.

Mr. PRICE. If that is agreeable, that will be our expectation.

Mr. SAMMON. One correction. What I would like to do is get the vast majority of the money—again those 15 or 16 agencies in seven states—as opposed to every last penny of it, but that will tell you where the problems are and where most of the problem is.

Mr. ROGERS. All right, 120 days?

Mr. SAMMON. Yes.

Mr. ROGERS. Deal.

Mr. SAMMON. Good. Thank you.

Mr. ROGERS. Well, now the last time we were here you said you would have a report to us by Friday, March 27, and we did not get it until 4:45 yesterday afternoon. You will be more prompt next time on the 120 days.

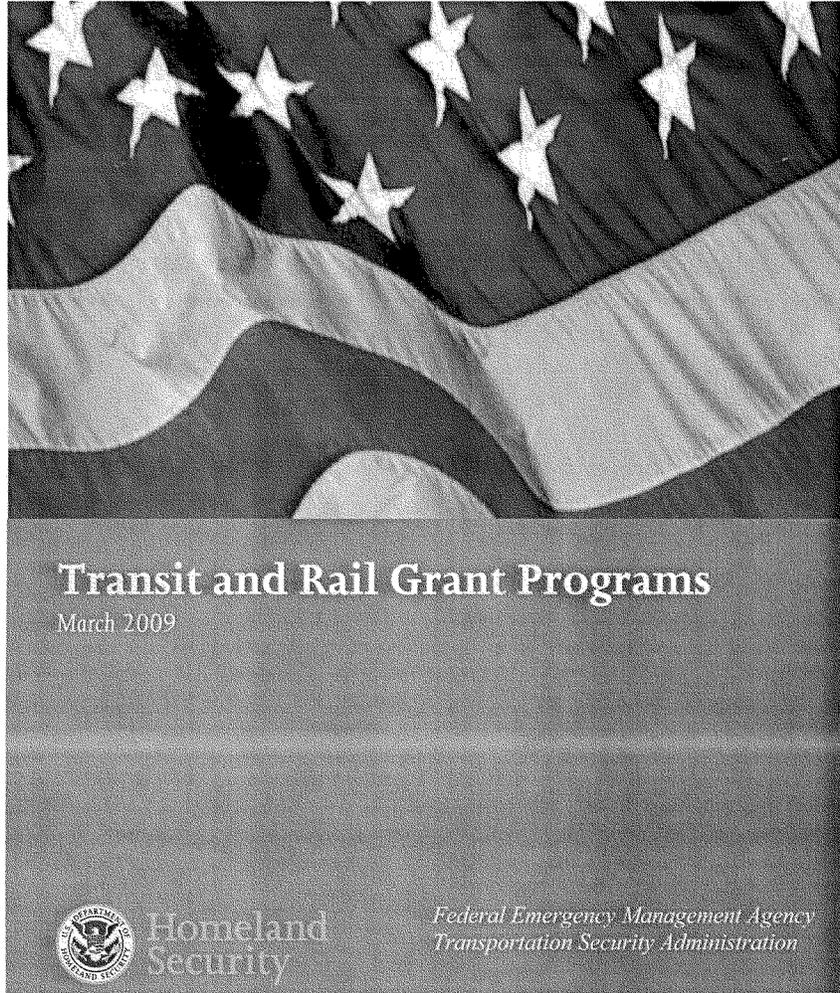
Mr. SAMMON. We will get it to you in 120 days, yes.

Mr. ROGERS. Because we have not had time to digest this report—

Mr. SAMMON. Yes.

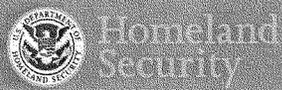
Mr. ROGERS [continuing]. And we do not want to do business that way.

[The information follows:]



Transit and Rail Grant Programs

March 2009



Federal Emergency Management Agency
Transportation Security Administration

Message from the Acting Administrator

The following report, "Transit and Rail Grant Programs," has been prepared jointly by the Federal Emergency Management Agency and the Transportation Security Administration at the Department of Homeland Security.

This report addresses specific questions regarding transit and rail grant programs, resulting from a recent congressional hearing before the House Appropriations Committee Subcommittee on Homeland Security. It will be transmitted to the following Members of Congress:

The Honorable David E. Price
Chairman, House Appropriations Subcommittee on Homeland Security

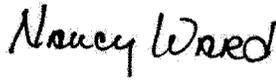
The Honorable Harold Rogers
Ranking Member, House Appropriations Subcommittee on Homeland Security

The Honorable Robert Byrd
Chairman, Senate Appropriations Subcommittee on Homeland Security

The Honorable George V. Voinovich
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

Inquiries relating to this report may be directed to me at (202) 646-3900 or to the Department's Acting Chief Financial Officer, Peggy Sherry at (202) 447-5751.

Sincerely,



Nancy Ward
Acting Administrator
Federal Emergency Management Agency

Executive Summary

On March 12, 2009 W. Ross Ashley III, the Assistant Administrator of the Grant Programs Directorate at the Federal Emergency Management Agency (FEMA), and Mr. John Sammon, the Assistant Administrator of the Transportation Sector Network Management at the Transportation Security Administration (TSA), testified before the House Appropriations Committee's Subcommittee on Homeland Security on the security of the Nation's rail and transit systems.

Two additional witnesses, Mr. Bill Morange, the Deputy Executive Director, Director of Security of the New York Metropolitan Transportation Authority, and Mr. Jack Eckles, the Deputy Executive Officer, System Safety, Security, of the Los Angeles County Metropolitan Transportation Authority, accompanied Mr. Ashley and Mr. Sammon on the witness panel.

The purpose of the hearing was to discuss the status of rail and transit security programs, and the effectiveness of the federal funding that has been provided to protect the users of such programs from acts of terrorism or man-made disasters.

During discussions throughout the proceeding, the Chairman and Ranking Member of the Subcommittee expressed concern over several issues, including the amount of time it takes to obligate and draw down transit and rail grant funds; the roles and responsibilities for FEMA and TSA in administering these grant funds and managing these programs; the grant process itself; and solutions for how FEMA and TSA can reach 100 percent draw down rates on the grant funding.

To address these concerns, the Subcommittee directed FEMA and TSA to jointly develop an efficiency review that focuses on the following issue areas:

1. A brief description of the problems related to the slowness of spending rail and transit security grants. The report should include a current status of the obligations and draw down numbers from Fiscal Years (FY) 2006, 2007, and 2008. The funding fact sheet from February should be used as a base since that's what the Members were working from. If those change by your submittal time, then you can note that. You should also detail the status of CA and NY with regard to obligation vs. draw down.
2. A description of FEMA's role vs. that of TSA's including who is responsible for approving authorizations for draw downs.
3. A detailed flow chart of the grant process.
4. Solutions for getting the funding drawn down with goals of reaching 100 percent draw down (should include a clear timeline). Those solutions should detail what needs to be done at FEMA and TSA (acknowledging there are bottlenecks at the local level as well).
5. The solutions also need to address Mr. Morange and Mr. Eckles recommendations.

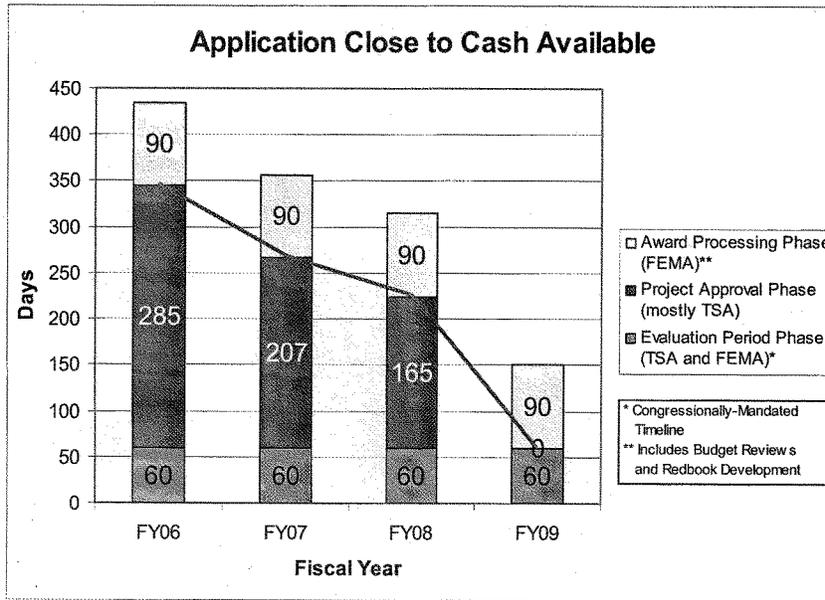
The report is due to the Subcommittee by March 27, 2009. Mr. Ashley and Mr. Sammon were also directed to report back to the Subcommittee in person at a follow-up hearing to further discuss these issues on March 31, 2009.

Table of Contents

I.	Issues Associated with Spending Rates for Rail and Transit Grants	4
II.	Roles and Responsibilities of FEMA and TSA	9
III.	Overview of Grant Process	12
IV.	Proposed Solutions for Drawing Down Grant Funds	13
V.	Response to NY and CA Recommendations	16
VI.	Conclusion	22

I. Issues Associated with Spending Rates for Rail and Transit Grants

The Transit Security Grant Program (TSGP) in its brief history has been complicated by a few issues as the program evolved. This is expected with any new program. As the program has matured, significant process improvements have been made.



Notes:
 * FY 2007 Project Approval Phase consists of both base and supplemental funding resulting in longer average approval times.
 * FY 2008 Project Approval Phase partially impacted by FY 2009 Appropriation Language eliminating FY 2008 match which resulted in most grantees resubmitting their investment justifications.
 * FY 2009 Project Approval Phase completed prior to the end of the Evaluation Period Phase resulting in zero impact on the award schedule.

The above chart shows the time in days from when applications are received to when agencies have access to the funds. TSA has significantly revised the process to review and approve Tier I projects, resulting in decreases in approval times each fiscal year. After applications are received, DHS has 60 days to act on the awards, per Congressionally-mandated timelines. After the 60-day period, DHS announces the awards. In fiscal year (FY) 2006, it took approximately 285 days after awards were announced to Tier I project approvals. That timeline has been reduced to 0 days for FY 2009, meaning that all Tier I projects will be approved when the awards are announced. After project approval, FEMA takes approximately 90 days to complete

budget reviews and the award package/obligation process. After the FEMA review is complete, agencies are issued "Release of Funds" memos allowing them to begin drawing down on the funds.

Environmental and Historical Preservation (EHP) issues do not result in delay of funding for the majority of these grant proposals. A limited number of more complex applicant proposals, such as those involving construction projects, can require extensive review for consideration of EHP issues. Funds for these more complex proposals may not be available for drawdown until the review is completed.

Over the years, the following issues have been identified as contributing factors to the slow drawdown rates for transit and rail grants. The explanation of each issue includes its resolution.

Issue 1: Access to draw down post-award funds is impeded due to statutory and regulatory review processes required after DHS announces awards, including: budget reviews to ensure reasonableness, allowability, and allocability of funds.

In FY 2006, TSGP Tier I grantees were unable to access funds due to the lengthy competitive grant application and review process, including formal submissions, reviews by a National Review Panel, and the necessary formal feedback and resubmission process. Project approval did not occur until several months into the period of performance. In addition, several statutory requirements, such as EHP Review, were not fully integrated into the application review process which added additional time before grantees could implement projects and incur expenses.

These grant programs transitioned within DHS into FEMA in the spring of 2007. DHS has increased the transparency of statutory and regulatory requirements that exist for all Federal grant programs (excluding block grants or those with exemptions) by providing more information through guidance and outreach. In addition, DHS and FEMA have determined that most of the projects funded under these rail and transit programs are not the types of projects expected to have significant adverse impacts on the environment and, therefore, an expedited EHP review is frequently performed within the normal application review time. To seek further process improvements, FEMA regularly runs parallel reviews in an effort to fine tune the efficiency of this process. Funds are also released at the individual project level to make funding available for grantee drawdown at the earliest possible time. The adoption of a cooperative agreement was implemented to streamline the process and to allow for faster drawdowns.

Issue 2: Period of performance extensions enable some agencies to catch up for lagging project implementation and slow drawdown rates.

All grantees receiving Federal funding must expend grant dollars within the approved period of performance, as required by OMB Circular A-102 for State, Tribal and Local grantees (codified by FEMA in 44 CFR Pt. 13). Grantees can receive extensions to the approved 3 year period of performance for TSGP grants by submitting a request to FEMA providing the necessary justification.

FEMA is in the process of implementing more transparent and more stringent controls over period of performance extensions that encourage grantees to draw down funds within the period of performance. FEMA has strengthened requirements for extensions to include accountability criteria and requires submission of updated project plans and timelines before extensions are approved. A consideration when approving an extension is the grantee's past performance on completing projects in a timely manner.

Issue 3: Budgetary, drawdown and procurement processes vary by state and local jurisdiction which contribute to inherent differences in project implementation, and ultimately drawdown.

DHS has a clear understanding of the hurdles that arise as implementation progresses from award through drawdown. Prior to FY 2009 the TSGP funding passed through the State Administrative Agency (SAA), adding an additional layer of approval and governance. The SAA office also provided a connecting point for regional collaboration and a source for coordinating funding. In many cases, transit agencies cannot procure in a timely manner because of the legal requirement to enter a competitive procurement process to award contracts. The procurement time is not required to be included in project plans. Other local issues affecting timelines include required local government approval, authority to spend, and state and local environmental requirements.

DHS encourages stakeholders to incorporate the procurement process as part of the Investment Justification (IJ) timeline and add detailed milestones including internal review processes in order to provide more accurate timelines. DHS leadership and program managers continue to develop better awareness of State and local procurement and reimbursement processes and continue to develop methods to review and implement plan adjustments as required, and relate to specific State and local laws and regulations. In addition in FY 2009, TSGP grant awards will be made directly to the Transit Agencies. Therefore, Transit Agencies can request their funding directly from FEMA using our on-line payment and reporting system which provides funding via electronic funds transfer (EFT) within 72 hours of the submitted request for drawdown.

Issue 4: Guidance and outreach does not emphasize the correlation between timely project implementation and drawdown rates.

Stakeholders have various interpretations of the relevance of drawdown as an indicator of successful project implementation. TSA and FEMA endeavor to improve the transparency of the grant guidance and encourage better planning by grantees to complete projects or phases of projects within the project period of the award. FEMA continues to develop more efficient ways for grantees to capture and report data including the implementation of the Cost to Capability initiative, a more robust on-line grants management system, and by awarding grants direct to the transit agencies, allowing grantees to drawdown directly from FEMA and requiring quarterly submission of electronic financial status reports detailing grant dollars encumbered.

Despite the challenges presented above, DHS diligently works to streamline the TSGP program processes. In FY 2006, management of the program was transitioned from a single agency to a split responsibility with two DHS agencies to appropriately include agencies with the transit security subject matter expertise, and with the grants administrative expertise. However, this

transition was not simple and resulted in process delays that have since been addressed. Since then, DHS fully engaged in improving the process and reducing the time frames by streamlining the process and clearly defining FEMA and TSA roles and responsibilities.

In FY 2007, the addition of Tier I cooperative agreements, clarified Grant Adjustment Notices (GANs), and improvement in overall processes enabled the TSGP to become more efficient and reduce time frames. In FY 2008, TSA and FEMA were heavily involved in outreach and stakeholder interaction to gather input on improving the processes. FEMA introduced an improved Release of Funds Memorandum and expedited several process improvements, including hiring additional staff to support the grant review processes and the issuance of improved guidance to applicants. Also, TSA revised its approval process and reduced project approval times.

During FY 2009 efficiencies have been made by placing more stringent timelines in the Tier I process and through the use of greater accountability and tracking for all processes. Using the FY 2006 performance as a baseline, there is continued improvement in the grant process with each successive grant cycle. DHS is committed to further improvements and is continuing to address process and guidance issues.

The following tables provide the total awarded and drawdown amounts for fiscal years 2006 through 2008 for TSGP, as well as for California and New York.

Table 1: Total Obligated and Drawdown Amounts for TSGP.

Fiscal Year	Amount Awarded	Balance	Amount Drawdown
FY 2006	\$135,998,093	\$127,783,693	\$8,214,400
FY 2007	\$162,870,670	\$159,363,177	\$3,507,493
FY 2007 Supplemental	\$100,000,000	\$93,632,368	\$6,367,632
FY 2008	\$359,489,800	\$354,439,744	\$5,050,056
Total	\$758,358,563	\$735,218,982	\$20,279,442

Table 2: Total Obligated and Drawdown Amounts for California.

Fiscal Year	Amount Awarded	Balance	Amount Drawdown
FY 2006	\$19,122,397	\$18,349,581	\$772,816
FY 2007	\$21,644,096	\$21,626,340	\$17,756
FY 2007 Supplemental	\$14,639,639	\$14,629,429	\$10,210
FY 2008	\$41,760,804	\$41,760,804	\$0
Total	\$97,166,936	\$96,366,154	\$800,782

Table 3: Total Obligated and Drawdown Amounts for New York.

Fiscal Year	Amount Awarded	Balance	Amount Drawdown
FY 2006	\$53,974,305	\$51,277,405	\$2,696,900
FY 2007	\$63,291,783	\$61,677,290	\$1,614,493
FY 2007 Supplemental	\$37,200,000	\$33,285,853	\$3,914,147
FY 2008	\$178,945,851	\$174,782,407	\$4,163,444
Total	\$333,411,939	\$321,022,955	\$12,388,984

Note:

* Funds not available are held due to EHP or budget reviews.

II. Roles and Responsibilities of FEMA and TSA

The roles for the DHS, FEMA, and TSA with respect to transit and rail grant programs are prescribed, to a certain degree, in legislation. DHS policy has also stipulated guidelines for the roles and responsibilities of DHS and TSA on these programs.

Section 101 of the Aviation and Transportation Security Act (P.L. 107-71) sets forth the duties and powers of the TSA Administrator, including the authority to assess threats to transportation; develop policies, strategies and plans for dealing with threats to transportation security; to make other plans related to transportation security including coordinating countermeasures with other appropriate departments, agencies and instrumentalities of the United States Government; to serve as the primary liaison for transportation security for the intelligence and law enforcement communities; and to carry out such other duties and exercise such other powers relating to transportation security as the Under Secretary considers appropriate, to the extent authorized by the law.

Section 503(b)(2)(G) of the Post-Katrina Emergency Management Reform Act (P.L. 109-295) provides the Administrator of FEMA with the authority to “provide funding, training, exercises, technical assistance, planning, and other assistance to build tribal, local, State, regional, and national capabilities (including communications capabilities), necessary to respond to a natural disaster, act of terrorism, or other man-made disaster.”

Section 1406 (Public Transportation Security Assistance) of the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) directs the Secretary of DHS to carry out the TSGP by determining the requirements for recipients of transit grants, selecting the recipients of transit grants based solely on risk, and establishing the priorities for which transit grants may be used.

Furthermore, Section 1513 (Railroad Security Assistance) of P.L. 110-53 directs the Secretary of DHS, in consultation with the TSA Administrator, to make grants to eligible recipients of rail grant funds.

Annual appropriations for the TSGP are made to FEMA, and are administered through the Grant Programs Directorate (GPD).

Language from Division D of the Joint Explanatory Statement (JES) which accompanied the Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009 (P.L. 110-329), further defines expected roles and coordination between TSA and FEMA. It states in part, “FEMA is expected to continue to fully engage agencies with subject matter expertise within the Department...in the development of grant guidance and the determination of awards. Such agencies include the Coast Guard, TSA...” The JES further states, “FEMA is directed to assume all coordination functions of grant programs for the Department and be the primary point of contact for all grantees.”

Since 2006, DHS policy has determined the roles of FEMA in managing the TSGP. FEMA's GPD serves as the one-stop-shop for programmatic and financial grants management expertise. As such, FEMA has the lead for designing and operating the grants management mechanisms needed to implement and manage the TSGP, and serves as the programmatic point of contact. Additionally, FEMA is responsible for ensuring compliance with all relevant Federal grant management requirements and delivering the appropriate grant management tools, financial controls, audit resolution, and program management discipline needed to support the TSGP.

FEMA is responsible for executing the risk formula utilized for the TSGP, as well as ensuring consistency in the risk formula across grant programs. Eligible applicants under the TSGP are divided into Tier I (highest risk) and Tier II agencies. These agencies are identified by using a comprehensive, empirically-grounded risk analysis model, taking into account intelligence community assessments of threat, potentially affected passenger populations, and the economic impact of attack.

Consistent with ATSA, TSA provides transit system subject matter expertise and determines the primary security architecture for the TSGP. TSA subject matter experts have the lead in crafting all selection criteria associated with the application review process. TSA is also responsible for convening review panels.

Different review and approval processes are in place for Tier I and Tier II applicants. Tier I agencies receive a "targeted" allocation and awards are made in the form of cooperative agreements. Under cooperative agreements, DHS partners with eligible transit agencies and their security providers in each Tier I region to address risk in that region. The cooperative agreement provides for increased federal involvement in the projects and use of funds as compared to a competitive grant.

Tier I proposed projects are reviewed by TSA subject matter experts. Once approved by TSA, a formal letter is sent to FEMA, whereupon FEMA conducts a budget review and programmatic review as outlined in the grantees award documentation. A major component of programmatic review is compliance with EHP requirements. All construction grant dollars must have EHP approval. Once these reviews are complete and approved, a Release of Funds memorandum is issued and sent to the grantee. At this point, the grantee has these funds available for drawdown and may request payment at anytime through FEMA's Web-based Payment and Reporting System (PARS).

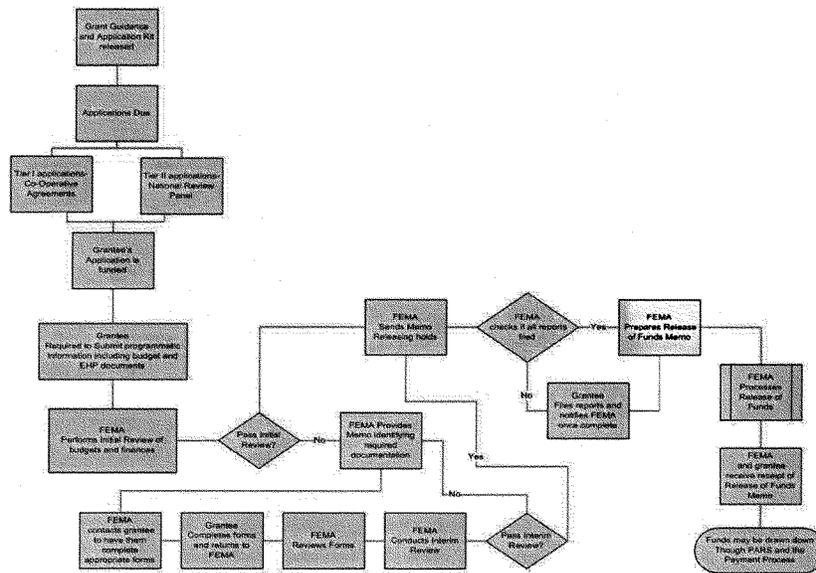
Tier II agencies compete in a funding pool and projects are reviewed by a National Review Panel (NRP), consisting of TSA, FEMA, and other subject matter experts. The NRP makes funding recommendations that are reviewed and approved by DHS leadership. Once approved, FEMA initiates the same processes as identified above for releasing funding to the grantee.

Once funding is released, grantees utilize PARS to request payments. After a grantee submits a payment request, the funding is transmitted via Electronic Funds Transfer to the grantee's bank account within 72 hours. FEMA does not direct grantees when to draw down grant funds. This is a state and/or local regulatory decision. Funding remains available for draw down for the entire grant award period and may be extended upon request and justification by the grantee. In

cases where the State Administrative Agency is the grantee, they are the responsible party to request draw-down of funds and transfer of funds to the transit agency (as the subgrantee).

III. Overview of Grant Process

The flow chart below shows the general process by which the TSGP grant funding is allocated and awarded:



IV. Proposed Solutions for Drawing Down Grant Funds

The Department proposes stronger technical assistance and outreach components to help TSGP grant recipients increase draw-down rates. GPD will offer financial grant management technical assistance to recipients of Transit Security Grant Program Funds. GPD will work with existing staff to ensure each state and each transit agency clearly understands the procedures for drawing down funds. Additional specific actions include:

1. GPD will transmit an Information Bulletin through our Centralized Scheduling and Information Desk to remind grantees of the processes for accessing the automatic payment systems and associated procedures. We will also remind grantees that due to the Cash Management Improvement Act exemption, funds may be drawn down when they are encumbered, rather than when they are expended. An important part of the communication process will be to re-iterate to grantees that our programs fall under the legislative exemption to the Cash Management Improvement Act (CMIA). Under the exemption, grantees can access funds up to 120 days in advance of payment. This means that grantees can draw funds down when they are encumbered (such as placing a purchase order), rather than waiting for the invoice to be paid. This exemption can save a significant amount of time for grantees, and all eligible grantees should be aware of this opportunity. However, it should be noted that FEMA's exemption will not overrule state and/or local regulations for drawdowns. It should also be noted that funds must be placed in interest bearing accounts and the interest (over certain limits) must be remitted quarterly.
 - Specific action: Information Bulletin transmitted
 - Specific action implemented by: April 30, 2009
2. After the initial communication, each of GPD's Transit Program Analysts will reach out via telephone, email and previously scheduled meetings to their assigned customers within the States and transit systems to follow up on any additional questions.
 - Specific action: Contact is made with each SAA, Tier 1 and Tier 2 transit agency
 - Specific action implemented by: May 31, 2009
3. TSA and FEMA GPD will formulate integrated project teams (IPT) of programmatic subject matter experts and grants management specialists to visit SAAs and Tier 1 and 2 public transit agencies to review their specific issues related to draw-down of grant funds, provide tailored technical assistance in grant financial management and cooperatively develop action plans to expedite draw-downs. FEMA representatives on the IPTs may consist of program analysts from GPD TSGP and Homeland Security Grant branches as well as financial grant management specialists from the FEMA regions.
 - a. Specific action: IPTs visit 100% of Tier 1 transit agencies to provide technical assistance and formulate action plans to expedite draw-downs.

- Specific action implemented by: June 30, 2009
- b. Specific action: IPTs visit 100% of SAAs in conjunction with annual monitoring visit to provide technical assistance and formulate action plans to expedite draw-downs.
 - Specific action implemented by: September 30, 2009
 - c. Specific action: IPTs visit 100% of Tier 2 transit agencies to provide technical assistance and formulate action plans to expedite draw-downs.
 - Specific action implemented by: March 31, 2010
4. GPD will leverage existing GPD grants management technical assistance as well as that which was developed for the Public Safety Interoperable Communications Grant Program and use those outreach teams and resources, as requested, to make contact with grantees and discuss their issues related to draw-downs.

GPD currently offers an *Enhancing Grant Management* Technical Assistance Program. This program is designed to improve the ability of grantees to administer grant funding programs awarded by GPD. Improving the ability of grantees to effectively manage these programs directly impacts the ability of grantees to improve efficiency at the grant recipient level, including efficiency in the award, obligation, and draw-down processes.

State Administrative Agencies (SAAs) and individual transit agencies may request this technical assistance through GPD at any time. GPD can provide meeting facilitation, direct guidance and consultation, intensive, short-term, site-specific work shops (multi-state, host-site, and peer subject matter presentations). The duration of the delivery varies depending on the requestor's needs.

GPD can deliver this technical assistance on a state or regional level, by way of conference and/or workshop to ensure the maximum participation and benefit.

GPD will deliver blocks of instruction on grant financial management at the TSGP After Action Conferences, GPD National Conference and other outreach opportunities that present themselves.

- Specific action: Provide grants management technical assistance to 100% of the SAAs and transit agencies that so request
 - Specific action implemented by: December 31, 2009
5. TSA and FEMA will research the viability of including language in future years grant guidance to incentivize behavior for grantees that encourages higher draw-down rates. TSA and FEMA will engage stakeholders in that discussion as well
 - Specific Action: Review programmatic guidance
 - Specific action implemented by: September 30, 2009

6. FEMA and TSA will review the efficacy of actions taken during FY 2009 and the first half of FY 2010 determine whether additional actions are needed.
 - Specific action: Evaluate results of prior actions
 - Specific action implemented by: June 30, 2010

V. Response to NY and CA Recommendations

DHS has reviewed and considered the proposed recommendations presented by Mr. Eckles and Mr. Morange during the March 12, 2009 hearing. The following tables outline the consolidated recommendations, the responsible Agency within the Department, the Department’s response to the recommendations, as well as the required actions necessary to implement the recommendations.

The consolidated recommendations are groups according to the following comment type:

1. Stakeholder Engagement
2. Funding Priorities
3. Composition of the RTSWG
4. Grants Management
5. Project Approval Process
6. Grant Guidance

In general:

- DHS agrees with six of the consolidated recommendations and have either acted on those or have taken action to clarify the policy to stakeholders. Of these, four are the responsibility of TSA and two are a joint responsibility between TSA and FEMA;
- DHS agrees in principle with nine of the consolidated recommendations and will conduct further research and work with Mr. Morange and Mr. Eckles as to how they will be implemented. DHS will report back to the committee on their resolution. Of these, four are the responsibility of TSA, two are the responsibility of FEMA, and three are a joint responsibility between TSA and FEMA; and
- DHS disagree with two recommendations. Of these, one is the responsibility of TSA and one is a joint responsibility between TSA and FEMA.

Recommendation	Responsible Agency	DHS Response	Action
Increased transparency in grant allocations to regions. (LA MTA)	TSA and FEMA	Stakeholder Engagement DHS strongly supports transparency in grant allocations. The risk formula is published in the grant guidance, is consistent with other DHS grant programs and has been scrutinized over 5 grant cycles. In addition, several regions, including LA, have been briefed on how regional allocations are determined.	FEMA and TSA will provide regular briefings on the TSGP risk formula with stakeholders to ensure transparency. DHS will continue to work with TSGP grantees to improve these efforts.
Regarding the Industry Peer Panel from grant guidance development roundtables, transit agencies should be allowed to put forth their concerns and issues and ensure that at the completion of the	TSA and FEMA	TSA holds roundtables twice a year with FTA to discuss any new DHS/TSA priorities and security emphases. TSA has also met on average 4 times a year in the individual regions to discuss new DHS/TSA priorities and security emphasis. TSA holds a monthly transit peer advisory group conference	FEMA and TSA have begun to hold regional after action conferences rather than one national after action conference to solicit transit agency recommendations, providing senior DHS leadership with those

Recommendation	Responsible Agency	DHS Response	Action
conference all parties understand what the next grant guidance will be. (LA MTA)		call to solicit security concerns and brief new developments and as exigent circumstances occur TSA holds calls and meetings. In 2008, TSA held its first after action conference to allow transit agencies to put forth their concerns. Transit agency concerns are well known in the regional transit security working groups that TSA attends. TSA has a transit blog which continuously solicits stakeholder input.	recommendations and feasibility of implementing them for the next grant cycle. DHS will continue to work with TSGP grantees to improve these efforts.
TSA should only contact the transit agency's designated representative regarding security initiatives – not a subordinate or contracted law enforcement department or agency. (LA MTA)	TSA	DHS believes an active partnership between federal, state and local security entities is critical to an effective national transit security program. Thus, DHS actively engages with security partners from various organizations in a variety of capacities both within and outside the grants process.	TSA disagrees with this recommendation. TSA has a broad security mandate under the ATSA and will continue to engage all security partners in a region. We will revisit to ensure that we include representation from both the law enforcement and operations community. Recommend that the functions of operations and security continue to be worked in a collaborative fashion.
Funding Priorities			
Tier I members should qualify for Tier I projects. (LA MTA)	TSA	DHS/TSA seeks to allocate funds based on risk. To that aim, the Department and Agency have prioritized and applied generous resources toward the development of a fairly robust risk methodology. By allowing agencies with small ridership numbers to qualify for projects that would otherwise belong to a grantee that faces a more significant threat, the Department would undermine its ability to operate transparently and reduce its reliance on risk in guiding resources where they are most needed.	No further action required.
Detection, response and recovery projects (including chemical and biological detection) should be an available project in a specific category. Due to the	TSA	Chemical and Biological Detection sensors are eligible uses of grant funding. They are currently available in at least two different project types. They are funded for installation and maintenance up to the three year period of the grant. The DHS Office	No further action required. All types of chemical, biological, radiological, nuclear, and explosives (CBRNE) projects are eligible in the FY 2009 TSGP.

Recommendation	Responsible Agency	DHS Response	Action
extensive nature of the current technology of chemical and biological detection, the project should be funded for not only installation, but also ongoing maintenance. (LA MTA)		of Health Affairs has the lead in determining the efficacy of particular systems and TSA defers to them as to what specific systems can be deployed in the transit environment.	
<p>More predictability and flexibility in implementing priorities: allow agencies to engage in more long-term projects covering multiple grant years. (LA MTA)</p> <p>Consistency in grant guidelines from year to year. (NY MTA)</p>	TSA	Long term projects are one of Secretary Napolitano's priorities. TSA encourages the planning and funding of long-term projects by working with transit agencies to identify specific and discrete phases that can be completed with the funding available through the Transit Security Grant Program (TSGP) and within the grant period of performance. The priorities in the TSGP have remained consistent for the past several grant cycles, focusing on the Transit Security Fundamentals. The level of funding appropriated for the TSGP has increased since fiscal year 2006, and this increase in funding has allowed transit agencies to undertake larger capital projects, such as for bridges and underwater tunnels, that they were previously unable to due to resource constraints.	Agree with Recommendation and it has already been acted on.
The Regional Transit Security Program should broaden its emphasis areas. Areas in need of Federal funding include consequence management projects to enhance egress, lighting, and signage; interoperable communications for police and regional partners; back-up power redundancy; chemical, biological and radiological detection devices. (NY MTA)	TSA	TSGP focus to date has been on anti-terrorism activities. Funding priorities were determined in collaboration with the national peer advisory group and within the regions, with the New York region providing strong national leadership. Back up power redundancy was a lower priority in that TSGP funds would be used to replace existing systems that are aging. These systems existed long before a terrorist threat and have always been focused on restoration of service after routine incidents such as minor flooding, transformer outages an electrical grid overload. Consequence management projects and Interoperable Communications are both eligible uses of grant funding in 2009. Chemical and Biological Detection sensors are eligible uses of grant funding.	Agree in principle with parts of the recommendation and have taken action to include several of the project types highlighted. Further expanding eligible uses of funds requires more research and DHS will continue to work with all TSGP grantees to addresses concerns and take stakeholder input into consideration for future program development.

Recommendation	Responsible Agency	DHS Response	Action
Should utilize threat/vulnerability assessments for each agency to determine priorities. TSA should use these assessments to measure performance and progress made toward identifiable and quantifiable risk reduction. (LA MTA)	TSA	TSA has used the BASE Assessment to determine national priorities and has made adjustments to the grant program priorities based on that information. As the BASE Assessment matures, it will become more of a factor to determining individual agencies priorities. TSA concurs that we need to make progress toward quantifying risk reduction.	Agree in principle with the recommendation and DHS will work with all grantees to address concerns and take stakeholder input into consideration. TSA will do more research on incorporating the BASE assessments in the grant process and report back to the committee.
Flexibility to use Federal funds for design, project management, and construction management tasks conducted in-house. Flexibility to fund all in-house flagging and track access work, which is currently fully reimbursable only when conducted by a third party. (NY MTA)	FEMA	DHS is reconsidering the eligibility of these costs.	More research is required to determine how to incorporate the recommendation. Specific requests will be evaluated on a case-by-case basis for approval, in compliance with all applicable laws.
Composition of the RTSWG			
Argues that allocations that are directed to local municipal law enforcement agencies have the potential for a negative impact on the core objectives of the grant program. (NY MTA)	TSA	DHS agrees that the funding sources under the TSGP process are designed to support the security needs of the Transit Agency. We also support Chief Morange's contention that TSGP funds should support an agency's primary law enforcement provider within the statutory limitations.	FEMA and TSA will continue to collaborate with transit agencies to address the role of security providers.
Proposes the State SAA be formally part of the TSGP, and chair Regional Transit Security meetings. SAAs should be involved in the process and receive TSGP funding. (NY MTA)	TSA	DHS has always been a strong supporter of the role that states have in the grant process. Each state does have a different level of engagement, New York is one of the most engaged states in the TSGP. Mandating State involvement may adversely effect some of the regions where there is little to no state involvement and presents a challenge in multi-state regions. TSA has already proposed that each RTSWG allow the state to chair the RTSWG meetings. Legislative changes would be required for states to receive TSGP funding.	Agree with Recommendation. Statutory changes have resulted in grants going directly to the transit systems. However, the SAA is part of the RTSWG and may serve as co-chair.
Grants Management			
Regarding management and administration costs,	FEMA	If the amount available for M&A is increased, the amount of available	No further action required. Would require a statutory

Recommendation	Responsible Agency	DHS Response	Action
argues that the current 2.5% is way too low; argues that 10-15% is more realistic. Also notes that guidance on how this is to be calculated needs to be clearer. (LA MTA)		funding for risk-reducing projects would decrease. However, with the removal of the SAA from the process in FY 2009, the M&A that the agency can keep was raised from 2.5% to 3%.	change.
TSGP should not be used to supplement UASI grants. (LA MTA)	TSA		No further action required. The 9/11 Act allows for up to 30% of total FY09 grant funding to be used for operational costs. That number goes to 20% for FY10 and 10% for FY11. Supplanting and comingling of funding is strictly prohibited.
Argues that grant program management should be handled by FEMA or TSA, not both. (LA MTA) Supports the creation of a "One Stop Shopping" mechanism for better coordination between FEMA and TSA. (NY MTA)	TSA and FEMA	DHS is a strong supporter of "One-Stop Shopping" and has identified one agency for Security "One-Stop Shopping," - TSA, and one agency for grants management "One-Stop Shopping," - FEMA. We will work to further clarify the roles and responsibilities. Specifics of the roles and responsibilities are published on the web. www.tsa.gov/grants through process diagrams.	TSA has statutor responsibility for security in the transit sector. FEMA has the grants management expertise and capabilities for grants and provides consistency across all Homeland Security Grants programs. Utilizing the areas of expertise within both agencies provides for the most efficient management of the TSGP.
Project Approval Process			
Expedited approval process similar to the FY 2007 "Expedited Training Requests" for all projects. (LA MTA)	TSA and FEMA	Agree that this was a very successful approach and is exploring the application of a similar expedited approval process to the 2009 ARRA funds.	A similar process to expedite funding will be explored for the FY 2009 ARRA.
Investment Justifications should be allowed to reference security sensitive documents instead of including them. (LA MTA)	TSA and FEMA	Agree with this recommendation as a method to reduce the administrative burden upon grantees. It should be noted that at some point the Sensitive Security Information (SSI) documents referenced have to be validated. In the past this has been a challenge that has slowed the review process in that SSI documents referenced by grant applications did not exist or could not be produced. The burden will remain on the grantee to file a complete application.	Agree with the recommendation. Allow Investment Justifications to include only references to SSI and develop a process to validate the SSI during the process.
More streamlined	TSA and	Agree with a more streamlined IJ and	Continue to streamline the

Recommendation	Responsible Agency	DHS Response	Action
Investment Justification consistent with general guidelines of FTA's Section 5307 will provide agencies with a broader range of eligible costs and streamline the grant process. (LA MTA)	FEMA	application approach. Between FY 2008 and FY 2009, the IJ was shortened by 8 questions, and we will continue to evaluate the IJ each grant cycle moving forward. Different purpose and different rules would be required to convert to the FTA grant guidelines. Appropriations language has always been very specific as to the uses and guidelines for TSGP funding.	Investment Justification process to further reduce the information collection burden on grantees.
Grant Guidance			
Recommends that the annual grant guidance be issued before the Federal Fiscal Year. (NY MTA)	TSA and FEMA	Guidance is tied to an appropriation. DHS has no objection to issuing guidance prior to the beginning of a fiscal year if there is an appropriation that supports the guidance. The way guidance is currently structured, to issue prior to an appropriation would be very speculative. DHS is looking at a suite of options to support multi-year programs and guidance is one of many areas of the grant process that may be affected. Long term projects are one of Secretary Napolitano's priorities and we are working on appropriate programmatic adjustments for FY 2010.	If FEMA releases guidance prior to an appropriation, it must be released subject to the availability of funds and subject to changes required by appropriations language. Releasing guidance in a realm of such uncertainty may prove to be less efficient than the current process which is already on a very aggressive timeline.

VI. Conclusion

The Department's analysis of the proposed recommendations outlined in this report sets the stage for process improvement for transit and rail grants administered by DHS. While the data presented shows a concerted effort by both FEMA and TSA towards streamlining existing grant processes whenever possible, this does not consider the totality of the program. Accordingly, we will look for further improvements through our state and transit process improvement teams. The comprehensive analysis of the proposed recommendations outlined in this report highlight the Department's commitment to engaging with our numerous stakeholders from the transit and rail agencies.

The Department recognizes the importance of engaging all stakeholders when undertaking process improvements. Of crucial importance is to alleviate the problems associated with the drawdown process, and to find a way to improve this process that satisfies both the needs of the transit and rail agencies and the needs of the Department. We believe that continuing the education process with our grantees will result in a better understanding of the automated payment process, as well as identify any new areas of concern. FEMA will work closely with TSA to ensure that these processes are improved in the most effective, efficient ways possible.

We look forward to continually engaging our state and local counterparts for recommendations on process improvements and to gain a greater understanding on how we may best serve these agencies. We believe we have made an excellent start in this area by hosting the regional Transit After Action Conferences last year, and we will continue to build upon that success. FEMA and TSA are committed to working together to eliminate undue burden imposed on these agencies, and to finding common solutions to the issues that we face. Above all, we reiterate our commitment to getting grant money quickly spent on appropriate security enhancements that ensure the safety and security of our Nation's transit and rail systems.

Mr. PRICE. Yes.

FUNDS FOR FY 2010

Mr. ROGERS. Now, the \$1.5 billion that has been appropriated for rail transit and intercity bus grants, only \$192.4 million, about \$12.5 percent has been spent, leaving more than \$1.3 billion, 87 percent unspent. That means we do not have to provide any funds for 2010 then, right?

Mr. SAMMON. Well, looking at the timeframe, I think one of the recommendations we would like to make back to the subcommittee in terms of there are activities taking place. I know, for instance, there are lots of security-related activities taking place. The MTA, for instance, is conducting security searches five days a week in six locations with our grant money. They have trained their front-line police force and a number of other people in terms of security awareness training.

In Los Angeles, the Sheriff's Department conducts mobile search and screening operations three times a day as a result of this grant money. They also do bag checks and sweeps on Metrolink, which is a commuter agency. Washington, D.C. has provided their bus operators with security.

So, there is activity taking place, and the question may be when you look at the operational funds, what we want to know is how quickly the operational funds are being drawn down versus the capital funds because it is a very different issue and I think we ought to get insight on that here pretty quickly to get—

Mr. ROGERS. I mean for grant monies.

Mr. SAMMON. Yes.

Mr. ROGERS. For making grants.

Mr. SAMMON. Yes.

Mr. ROGERS. You have got the \$1.3 billion laying around. You do not need any extra money piled in that hopper for 2010, do you?

Mr. SAMMON. I think that is one of the recommendations we will make back to you.

Mr. ROGERS. What recommendation?

Mr. SAMMON. In terms of the question you have asked me in terms of—

Mr. ROGERS. Whether or not you will need more money?

Mr. SAMMON. Yes.

Mr. ROGERS. There is no way you can spend the \$1.5 billion in 2010, is there?

Mr. SAMMON. The \$1.5 billion will not be spent, I doubt it, in 2010 because they are multi-year capital projects.

Mr. ROGERS. So if we need money elsewhere in this bill—

Mr. SAMMON. Yes.

Mr. ROGERS [continuing]. Why put more money in a hopper that is not operating?

Mr. SAMMON. I think that is what we have to be able to tell you is how quickly it can be operated, sir.

UNSPENT FUNDS

Mr. ROGERS. Well, now, what you have recommended to us are fairly obvious recommendations. I mean, there is nothing rocket

science about what you are proposing. Why have we not done this before?

Mr. SAMMON. In terms of going through the grant analysis?

Mr. ROGERS. Yes.

Mr. SAMMON. That is a very good question. We have been—again, TSA in terms of our role, in terms of talking to the agencies and security providers, we see activity happening. We know that the capital projects take longer. We have been pushing since the supplemental appropriation in 2007 to get more money for operational funds, which we know can be on the street quickly. One of the things we have been doing, recognizing that, one of the reasons we changed the grant guidance significantly in 2007, to provide for operational funds and also to make sure that the operational funds provide the highest priority, meaning those projects are going to be put to the top because we know that it takes a long time to get capital projects funded.

Mr. ROGERS. Mr. Ashley, what do you think?

Mr. ASHLEY. A couple of things. One, I would like to comment on the part about the money that is sitting around in the budget that is unspent. From talking with these transit agencies, and I am sure if you talked to the transit agencies that have been speaking with the notion that the money is not spent or drawn down does not mean that the funding is not obligated to valid security projects that are ongoing.

Now, one could make the argument on how big the funnel ought to be going in, but every dollar that has been appropriated is going towards valid security projects that are obligated to them.

The second part about this, as mentioned by Mr. Sammon, vast improvements have been made on the front end of this process. The part about doing the investment justification at the very beginning of the process (during the application process) is consistent to the way that we do the Homeland Security Grant Program. It allows for those funds to become available for draw down faster.

Having talked to the transit agencies now over the last couple of weeks on this issue, the issue is not on the back end of the process of how long it takes from a cash management standpoint; it is on the front end of the process, on how long it has taken to make these funds available, and we have made marked improvement in that area.

What we deem to do now, as Mr. Sammon mentioned, is a couple of different things. One is to reach out to the transit agencies and determine what is specific to the individual agency or state. One size does not fit all. There is not one plan that fits for New York, that fits for Los Angeles, that fits for Philadelphia. They each have different procurement systems. They have different state laws. They each have different abilities to take advantage of our cash management exemption from the Cash Management Act. So we are going to reach out to each one of them and identify these points to help them develop plans to draw down the funds faster.

In our monitoring plans on the back end, we plan to include an explanation of the use of our cash management exemption to allow folks to get the funds out of the Federal Treasury and into the states and transit coffers much more rapidly. But again, this will be a state by state, transit agency by transit agency-specific issue.

CONGRESSIONAL DIRECTION TO ACCELERATE EFFORTS

Mr. ROGERS. With all of these monies not spent, and realizing that these grants are supposed to be purchasing greater security, we put in the 2009 bill a direction that FEMA accelerate efforts to develop tools for measuring the achievement and effectiveness of its grant programs to give us some yardstick to measure whether or not the money being spent is doing what it is supposed to, a cost to capability is what you now call it, and we put money in there. Where are we on that?

Mr. ASHLEY. Yes, sir. You all were good enough to put \$5 million in for the first time to measure the effectiveness of grant programs, not just in transit, but across the \$27 billion or so at this point that has been appropriated to date. The project has two different components to it. One was a look back over the last five years at the accomplishments that have been made from the data that we have available, whether from TSA partners and FEMA, or whether from Coast Guard and the Port Security Grants, what has been accomplished over the last five years with the existing data. From that, we learn what kind of questions are we asking; are we asking the right questions of our state and local partners to find out how we could better measure that capability going forward on a year-over-year basis so that we can begin to allocate grants not just upon the risk but the ability to determine the return on investment of addressing that risk?

We are in the final process of clearing the Grant Accomplishments Report, which is the first phase of that project. It has been cleared out of FEMA and is at DHS now—to look at that five-year look back.

More importantly, we are kicking off in the next three weeks a pilot with 20 UASI and state jurisdictions, 18 to 20, that will be specifically looking at the year-over-year return on investments all across grant programs for those individual jurisdictions on an automated basis, and we have been working with your staff on that.

Mr. ROGERS. When will we hear something?

Mr. ASHLEY. With the new team in place, it has taken a little bit longer to coordinate reports out. I would anticipate within the next two to four weeks we will have the first phase report out of final clearance. Then we will report to your staff who will be the pilot participants moving forward on the—for the 2010 process.

Mr. ROGERS. Thank you, Mr. Chairman.

Mr. PRICE. Thank you. Mr. Rothman.

OBLIGATION OF FUNDS

Mr. ROTHMAN. Thank you. Mr. Ashley, can you tell me if, if I heard you correctly, every dollar appropriated has been obligated. Did I understand that correctly?

Mr. ASHLEY. That is correct.

Mr. ROTHMAN. For 2006, 2007, 2008, and 2009?

Mr. ASHLEY. 2009, not yet. We will announce the FY09 grants on April 8. The Secretary will be announcing them.

Mr. ROTHMAN. So as of April 8th it will be 100 percent from 2006 to 2009?

Mr. ASHLEY. For 2009, it will take approximately 60 to 90 days after the award is made to do the fiduciary programmatic work, after which they will be obligated.

Mr. ROTHMAN. I will tell you there might have been a lot less heat last time if we had heard that sentence.

Mr. ASHLEY. Right.

ACCELERATION OF PROJECT APPROVAL

Mr. ROTHMAN. But I want to first thank the Chairman and the Ranking Member for calling the first hearing on this subject, and I would like to thank you gentlemen for calling the second hearing. I believe it did get everyone's attention and refocused on this. There has been a lot of work done by the TSA and FEMA, obviously, in a whole host of areas very important to our national security, but on the rail security we have a ways to go.

I am grateful, I think I am grateful that this middle part, this project approval phase of TSA has been eliminated. I say I think I am grateful because I am not sure what is lost by going from 285 days worth of work, evaluation and thought to zero, or have that work combined with work that was already being undertaken in the initial 60-day phase.

Mr. Sammon, you said that what allowed for this progress, this rather remarkable process, was that investment justifications were moved up between TSA and the Agency. Do you mean FEMA?

Mr. SAMMON. The applying agency.

Mr. ROTHMAN. The applying agency.

Mr. SAMMON. Yes, sir.

Mr. ROTHMAN. And you said the ranking was moved up.

Mr. SAMMON. When we issued guidance back for the fiscal year 2008, we made a simplified process in terms of putting in five categories of projects, and each category, depending upon which one you wanted to apply for, received a different score. So, for instance if you wanted to train employees, you get a score of five. If you wanted to put cameras in suburban bus yards, you might get a score of two or one. So, it is very transparent. The agencies can see it up front. They understand if I apply for this, here is how I will score.

Mr. ROTHMAN. And how was it done previously?

Mr. SAMMON. Previously, people would submit complex applications, lots of paperwork, and then a whole room of experts would sit around the table and look at them, judge them, and argue about them. It was a complex process.

Mr. ROTHMAN. Are you saying that a group of people do not evaluate them before they put the number on them?

Mr. SAMMON. The numbers are assigned—there is a 60-day period from when the application is closed until TSA is finished with them.

Mr. ROTHMAN. And who puts the numbers on them?

Mr. SAMMON. TSA looks, for example, if it is training, they will put a five.

Mr. ROTHMAN. Okay. So you feel you do not need that room full of folks that you relied on previously. You can now do that with a different group?

Mr. SAMMON. It is still a set of subject matter experts, but they get to the answer much quicker than they did before.

Mr. ROTHMAN. And how is that, sir?

Mr. SAMMON. Because, for instance, if you are applying for training, training is in the first category, the highest priority. If it is a training application, they see it is someone wants to train 500 bus drivers with security awareness training, the project is scored a five, and now it moves along.

Mr. ROTHMAN. So in other words you have set up a system where certain categories of work are automatically assigned a number.

Mr. SAMMON. Yes, sir.

Mr. ROTHMAN. So now all you have to do is find out where the application plugs in.

Mr. SAMMON. Yes.

Mr. ROTHMAN. Whereas before you on an ad hoc individual basis—

Mr. SAMMON. Yes.

Mr. ROTHMAN [continuing]. Decided what the number would be.

Mr. SAMMON. And they would all have to compare all the voluminous number of applications to one another to see where they ranked and how they fit.

Mr. ROTHMAN. And so now you compare the five, four, three, two, ones with each other.

Mr. SAMMON. Yes.

Mr. ROTHMAN. And then you rank them.

Mr. SAMMON. We also look at the rank, the agency's risk score. So, for instance, the New York Transit Agency would have a higher score than a smaller—

FUNDING FOR FY2010

Mr. ROTHMAN. One other fast question if I may. It is more of a comment. You know, coming from the Northeast, Mr. Chairman, Mr. Ranking Member, New Jersey, in particular, probably one of the highest risk target centers in the country, I am not certain that I would want to zero out the 2010 capital budget for rail security, especially since, as Mr. Ashley said, every penny of 2009 has been obligated—excuse me—of 2006, 2007, and 2008 have been obligated, and 2009 will be obligated within 60 days from April 8th?

Mr. ASHLEY. If I could also add, in the process that TSA has taken place in 2009, all of the projects for 2009, as Mr. Sammon mentioned, are approved. These are projects that are being obligated. They are not financially obligated, but they have identified needs that are moving forward.

Mr. ROTHMAN. Okay. So all the more reason if I may make the plug for not zeroing out the capital budget for 2010, that we keep this progress going, and provide sufficient resources for capital projects as well as operational. Thank you, Mr. Chairman.

Mr. PRICE. Thank you. Mr. Carter.

MEETING WITH GRANTEES ON EXPENDITURES

Mr. CARTER. Thank you, Mr. Chairman.

So you can go have these meeting with these folks around the country to find out how they are spending the money, is that right?

Mr. SAMMON. Yes, sir.

Mr. CARTER. That was not thought of in 2006? We just laid it out there and forgot about it, or what happened there?

Mr. SAMMON. Well, I do not think anyone forgot about it. FEMA is the fiduciary agency for the money in terms of where the money is spent. The money is drawn against their account and that is what they primarily do. What we wanted to do is make sure, however, and I also see on an ongoing basis when talking to MTA, Los Angeles Sheriff's Department, Tom Lambert down in Houston, for instance, he trained 2,200 of his front-line employees with transit grant money. So in our normal conversations we have with agencies, people are doing things. In terms of their insight, in terms of their capital projects, where they are in terms of between the state and the local entities and design, engineering, construction, those things do take longer; however we do believe that the length of the draw is lengthy and the Committee deserves a complete understanding of where the money is and what we are doing to speed it up.

RAIL TRANSIT SECURITY

Mr. CARTER. When you say transit, is it a priority on rail and bus that we are talking about?

Mr. SAMMON. It is.

Mr. CARTER. We spent lots of money on air.

Mr. SAMMON. Yes. This is for intracity rail and bus.

Mr. CARTER. I unfortunately took the train from Texas to Washington because of surgery I had, and I thought about it the entire way because they stopped in—well, I got on in Taylor, Texas.

Mr. SAMMON. Yes.

Mr. CARTER. And I can assure you there was zero security in Taylor, Texas. And I put two very heavy bags on there because my wife was with me. [Laughter.]

We are not on television, are we?

And I thought about that. I mean, I thought this is not any different than traveling on the train when I was a little kid going to visit my grandmother in Tennessee from Houston, Texas. I saw no security whatsoever anywhere. And it did not worry me because I just figured I am one of these fatalists, it either will happen or it will not. But it really ought to worry us because I had to go all the way to Chicago, from Chicago all the way across the top of the country to Washington. Never saw any security anywhere.

Mr. SAMMON. Sir, I went to New York last week from D.C. Amtrak security at Union Station, you see they have guards and they have other security traveling on the train to New York. A police officer with a dog is checking, stopping the dog at the bags. So, Amtrak does look at what they perceive to be higher threat locations, and they tend to concentrate all the security resources there. For instance, they have also spent a lot of time and money, you know, hardening the tunnel into New York. They are looking at what do they think the highest target threats would be, and I think they focus their resources there. And they do, particularly in the Northeast corridor.

Mr. CARTER. I will be corrected. I did see security in Chicago. I will say that.

Mr. SAMMON. Okay.

MEETING WITH GRANTEEES ON EXPENDITURES

Mr. CARTER. But I guess what I am wondering about is that if I am hearing what you are saying, you are going to go find out how they are spending the money and how they are processing it out, and I am just assuming that some places you go the plan is going to be how you secure Amtrak, and it seems to me that ought to be reported to you on a, I would think, monthly basis or at least a quarterly basis from the start of the program so you know what they are doing, and that is why it is curious for me that it seems to me you are going to go back and check on how they are spending the money.

Mr. SAMMON. Yes, Amtrak does have a direct grant in terms of the appropriation. There is a direct amount for Amtrak that is carved out of the overall grant appropriation for transportation. We have worked with Amtrak closely for the past number of years to encourage them, particularly, to do things such as more dogs, more patrols, those kinds of things. Again, that is the kind of money you can spend faster. You get more up-front security.

Back in 2007, for instance, in the process we brought the New York Police Department to enter the grant process to get the people who are actually providing the front-line security into this process so we get those applications for funds to folks who are securing subways in New York, Chicago, and Los Angeles.

Mr. CARTER. Thank you, Mr. Chairman.

Mr. PRICE. Thank you. Ms. Lowey.

DELAYS IN DRAWDOWN OF FUNDS

Ms. LOWEY. Thank you, Mr. Chairman, and thank you for holding this second hearing. I just want to clarify a couple of points. While a significant amount of money waiting to be drawn down could be problematic, that does not mean that the local governments are ignoring their responsibilities, and I encourage my colleagues to not simply look at drawn down figures and make conclusions about the effectiveness of certain programs. I am really confident that if you would examine security operations in New York, which Chairman Price and I did in November, you would be truly impressed with how the grants have been spent in the area that is the likeliest target of an attack.

However, I would like to share an example that provides insight into the delays from when money is appropriated to when it is drawn down. For the fiscal year 2008 transit grant, New York State submitted investment justifications in August 2008. Until last week, maybe because you knew you were coming before the Committee, until last week the state heard nothing from TSA or FEMA, and last week FEMA sent the state a letter claiming that transit security funds had been released in November.

The problem is no one contacted the State in November, and it took five months from the time DHS has issued the grant award notice to when it notified the State that money could be spent.

COMMUNICATION WITH GRANTEEES

Now, I understand the need to be a rigid system in place and I have been reviewing this and the recommendations, but DHS just

has to do a better job communicating with grantees, and when grants are awarded recipients should be notified immediately. Would either of you care to comment on that?

Mr. ASHLEY. Sure. I can comment on it, and part of this is the confusion of when the grant is made. We have a competitive process and in the transit programs for the Tier 1 agencies there is a target allocation given, and then we award. Last year, I believe, New York State was awarded \$175 million, and an announcement of that award took place on May 16th or so last year.

In the process, the investment justifications as Mr. Sammon was talking about earlier took place after the fact. After that award was made, TSA in New York went back and forth with the development of what that was. We received from TSA at that point an "authorization to spend," if you will: "projects are good—move forward."

Also what occurred, as referring to in that November letter, is when we obligate the funds in the financial system and say those funds are now committed in the federal fiscal year they are notified that those funds are committed to New York. Those funds are obligated and cannot be taken away. At the same time that is going on (while FEMA is doing its fiduciary management), TSA is currently working on the programmatic of the grant to make approval on a project-by-project basis. That is also the part that Mr. Sammon spoke about that has now been accelerated up to the front end of the process, eliminating that dual (what you are referring to) notification to the State.

Ms. LOWEY. That does not make any sense to me at all. Does it make sense to you?

Mr. ASHLEY. Okay.

Ms. LOWEY. Do you think that is a great system that the justifications were submitted—I mean—

Mr. ASHLEY. In 2008, it was not a great process in taking that two-step process.

Ms. LOWEY. But why did it take until—I am just reading from these notes here—why did FEMA send a letter last week that the transit security funds can be released in November? In other words—

Mr. ASHLEY. Because we—

Ms. LOWEY [continuing]. You messed up?

Mr. ASHLEY. No, ma'am. We just received the authorization from TSA within the last couple of weeks for the 2008 funds, to release those funds to New York to be spent.

Ms. LOWEY. Well, I am glad you are reviewing the process. I will not belabor the point, but I also want to make it clear to my distinguished Chairman because he was in New York with me, that nearly all the funds have been obligated to New York. Now, there may be some areas of the country, and we have talked before about formulas and risk, that do not feel the urgency that we feel in New York. We know what the threat is. I am thrilled when I see those dogs at Grand Central Station. I am delighted that the feeder routes have dogs, not on all of them, they rotate, and I think it is important.

So as I understand it, because we checked, nearly all of the funding in New York has been obligated and I think it is very important that you do not hold the state and locals responsible for fed-

eral problems. So I would hope that the federal government is working aggressively to streamline the program, but in areas of the highest risk I think it is essential that the money keep flowing because, boy, we could use more dogs. It really works very well.

FEMA'S RISK FORMULA

And I wanted to mention another program. FEMA's risk formula used to distribute the grants values threat at 20—I am finished with that, okay, but I would be interested to know, Mr. Chairman, and perhaps they can respond to me, why is the actual threat of an attack worth only one-fifth of the risk formula? I think that is pretty important when you are putting together—

Mr. PRICE. It is important. Please respond briefly, and then you can elaborate for the record if you wish.

Mr. SAMMON. Again, the threat is one part of it that is very important. The threat information comes and goes, but it is a very important portion. The vulnerability and consequence of the formula take into account underground riders, passengers, and so forth. So, in that formula, New York always scores very high because the MTA has the higher passenger density and is many times more than any system in the whole country. And of those that are very high, threat kind of adds on top of that as another item.

You can quantify it clearly by the passenger density, and underground tunnel, and miles and so on and so forth, and threat is more of a qualitative thing, so it is kept in that proportion.

Ms. LOWEY. I will not pursue that but you still have to convince me that threat should not be more than—should not be more than 20 percent.

Mr. SAMMON. And that is a very good observation to discuss.

Ms. LOWEY. Thank you, Mr. Chairman.

DRAW-DOWN FIGURES FOR NEW YORK

Mr. PRICE. Thank you, and I would say to my colleague the draw-down figures for New York are part of the reason we are having these hearings. Yes, the funds have been obligated but the draw-down is alarmingly slight, and so these monies need to flow and, of course, New York City needs to have the highest priority in terms of addressing these needs.

Ms. LOWEY. Mr. Chairman, we are looking at that as well because I understand part of the problem is that the locals have not been reimbursed, so we are trying to figure out what the issue is here, and maybe the whole system, because as I understand it, it was explained to me when I asked the question, it does not mean that these programs are not being carried out. They have not necessarily been reimbursed in the most effective responsible way.

So, Mr. Chairman, I think you bring up a good point, and that is what we are looking at as well, so the funding has been obligated, and that does not necessarily mean that the security programs have not been accomplished. They just have not been reimbursed.

Mr. SAMMON. And Rep. Lowey, that is why I will be in New York on Thursday morning.

Mr. PRICE. New York obviously has a major stake in this review process. We have asked the agency to expedite, you know, within this four-month timeframe.

Ms. LOWEY. Thank you, Mr. Chairman.

Mr. PRICE. Thank you. Mr. Ruppertsberger.

REDUCING APPROPRIATIONS

Mr. RUPPERSBERGER. Thank you. I was not here when the comment was made, so maybe it was not made exactly how I heard it or someone else told me that they heard it. One of the issues was raised that because we cannot move the money quickly enough, then maybe we should not be appropriating as much money, and that it was something that you were going to look at or that might be an option to look at. If that is the case, I want to try to address the issue.

To begin with, management is about getting the best people you can get, getting the resources to do the job, and then holding people accountable. Now, a lot of times things like an issue such as grants is you do not have enough people, you do not have enough technology, or management is not doing their job, so, you know, that is something that we would try to find out from an oversight point of view, but I am going to get parochial to an extent.

I represent a district that has NSA in the district, Fort Meade, BWI Airport, Port of Baltimore, Aberdeen. It is considered the Washington Metropolitan Area, including Virginia and Maryland. If we do not deal with the issue probably of mass transit, it will be worse than California, and it is getting close to that right now. So there is going to be a lot of activity in rail, there is a lot of activity, as you know, with homeland security. I was just at BWI Airport yesterday meeting with a lot of employees at the TSO at TSA.

FUNDING PRIORITIES

So I would like you to respond. I think there are numerous needs and, unfortunately, I believed strongly when Homeland Security was stood up, that there was a lot of mismanagement of money going to places that were not really where they needed to be, and I believe now it is coming around a lot better and focusing on reality of where the money is supposed to go.

Could you respond to the issue of what you are going to look at as far as the money is concerned because I would like to take you on a tour of my district. New York is a big city, I love New York, and what is the song, I love New York. I am a bad singer. But I really think the needs are there, and it is unfortunate if we cannot get the money to the front-line as quickly as possible.

I was in local government for 18 years, and I always had a problem when the feds pressed down the state with grants, the state presses down on the locals, and the locals do not have any place to press. So the quicker and the better we can get that money is going to be helpful. Could you respond?

Mr. SAMMON. Yes. Well, in terms of Baltimore, it is included in the National Capital District in terms of for grants, which is a highly rated district. It shares Baltimore. By doing so it shares the risk rating and the threat rating that Rep. Lowey is referring to at the national level, that Washington, D.C. has. So, in terms of

being in the group because we want to look at this as a regional process because obviously Maryland transportation agencies interface, coming back and forth to Washington. We have been working closely with the folks in Maryland to get transit priorities and grant money to them, working with them more in terms of operational funds, getting the kinds of things—people on the ground kind of funds that we think are important to get to secure the system because, again, the issue, when I think we get into this in terms of process-wise, looking at how long it takes to build a capital project, we are going to see more time. But we believe we can get money flushed out more quickly for operational costs in terms of paying for police, paying for overtime, paying for dogs, paying for mobil screening, those kinds of things.

TESTING AND DEPLOYING SCREENING EQUIPMENT

Mr. RUPPERSBERGER. There is another issue too—do I have enough time? On the recovery bill, I believe there is \$1 billion to TSA. We talk about resources to do the job to protect our citizens. Detection capabilities, detection systems that have been used and on a test basis I know there is one at BWI Airport as an example. We need to do more than that. Is there a focus in Homeland Security working with the manufacturers of this equipment and has testing been done so that we can start using more of this equipment which will help our people on the front-line protecting us?

Mr. SAMMON. Well, I think we are looking at acquiring more of the whole body imagers which gives us the capability to see threat items on folks in a—

Mr. RUPPERSBERGER. My question, I want to get specific, there is detection equipment out there.

Mr. SAMMON. Yes.

Mr. RUPPERSBERGER. Are we on top of it? Are we starting to put it out there? Have we tested it? Is it where we should go?

Mr. SAMMON. With the whole body imagers what we are seeing is that the key thing we were worried about that is the throughput time. We are seeing through-puts raise significantly. The other piece you will see more is AT X-ray. The advantage of AT X-ray is it is a programmable platform that we can—as we see threat streams changing, we can put those kinds of materials, different liquids, other kinds of things into the machines to detect. If it only sees metal, it only sees—

Mr. RUPPERSBERGER. There are a lot of—how about an electronic baggage screening program?

Mr. SAMMON. Well, a large portion of that billion dollars I believe is going for in-line EDS systems in airports.

Mr. RUPPERSBERGER. Now you are talking about intelligence. Intelligence is very important—

Mr. SAMMON. Yes.

Mr. RUPPERSBERGER [continuing]. In protecting us against terrorism and there needs to be a lot of communication, but from an intelligence point of view when you are moving forward with this equipment you have pilot programs at most airports.

Mr. SAMMON. Yes.

Mr. RUPPERSBERGER. Are you using your intelligence to put it in places such as New York, such as other high-risk areas.

Mr. SAMMON. Yes. In terms of looking at the priorities and the rankings of those airports, and we also use intelligence. We talked about the program, the AT X-rays, to see what people are looking for on the Internet in terms of folks looking at possible threat streams and able to program those kinds of materials into those x-ray machines.

GRANT PROGRAM ADMINISTRATION

Mr. RUPPERSBERGER. Finally, my time is up, the other issue is I asked the question at the beginning, but I really would like you to focus on the fact when you have an administrative situation that you are not getting out the grant or there is a breakdown, in my opinion you do not put that money into a situation—

Mr. SAMMON. Right.

Mr. RUPPERSBERGER [continuing]. That is not going to work, but I think you need to come back and focus on where the money needs to go. Money is a priority in programs that have worked, programs that make a difference. And so I would hope when you are evaluating this do not use it as an excuse not to give money when in fact it is the mistake of administration.

Mr. SAMMON. I agree 100 percent, and that is why we pushed in 2007 for the supplemental appropriation to add the operational costs for deterrence. There was a RAND report in October of 2007, if you look at the—as was mentioned by Mr. Ashley—the cost/benefit return on investment, those kinds of things were the first level of priorities that you get the best bang for your buck.

Mr. PRICE. Thank you. I am happy to say that some of the gentleman's questions provide a nice segue into our next hearing.

Mr. RUPPERSBERGER. Well, that is why I did it.

[Laughter.]

Mr. PRICE. Thanks for your help. Many of them do pertain, obviously, to aviation security; maybe even more than rail and transit security.

With that, we are going to segue into our second panel. I do appreciate your gentlemen appearing. Let me just underscore a couple of things in terms of our remaining questions and also our expectations. We obviously greet as good news the streamlined process that you announced this morning for the 2009 grant funds. However, Mr. Rothman was getting into some important questions and I want to ask you to, in a more systematic way, provide for the record an accounting of exactly what we are gaining and losing in terms of the substance of that review process.

Going from 285 days to zero is of course what we have been asking for in a way, but seems to me legitimate questions have been raised and remain about the state role, for example, in this kind of expedited process you are describing, the place of the kind of peer review that you have conducted and that you have from time to time touted as a value and perhaps other things that we have not raised.

Are these processes simply being compressed? Are they going to be eliminated or going to be modified? We would like a more systematic accounting for the record of what this rather dramatic change is going to entail in terms of not just the timing of the process, but also the content of the TSA component of this process. And

then secondly, we do look forward to your accounting of the disposition of these 2006 through 2008 grant funds.
[The information follows:]

TSGP Tier I TSA Process and Improvements

By implementing process improvements, working with transit agencies so that they are able to respond to grant guidance more efficiently and by working concurrently with the FEMA processes rather than sequentially, TSA has eliminated the impact of the TSA review process on the FEMA 2009 grant timeline.

Average Approval Process Time	Fiscal Year	Process Notes
285 Days	2006	<ul style="list-style-type: none"> • Competitive process within the region; projects were reviewed by a National Review Panel consisting of TSA, FEMA, and FTA • Nature of the competitive process required very formal communications, project reviews, feedback, and resubmissions • Necessary formality of project review, feedback, and resubmissions led to long timeframes for final approval of several projects • Improvements: <ul style="list-style-type: none"> ○ Implemented new, cooperative agreement process in FY07 to address communications issues and lengthy timeframes ○ Cooperative agreement process allows for upfront, open, and continuous dialogue on projects and funding
207 Days	2007	<ul style="list-style-type: none"> • Cooperative Agreements between DHS and the regions rather than a competitive process; discuss projects as a region and address any concerns in real-time discussions (rather than through formal feedback) • Timeframe was longer than anticipated due to learning curve of new process, but still shorter than FY06 • Introduction of the FY 2007 Supplemental also added time because of new negotiations and discussions that had to occur because of additional funds after the regional project lists had been developed • Improvements: <ul style="list-style-type: none"> ○ Overall timeframe for approvals was shortened by approximately 3 months from FY06 (per GAO draft Statement of Fact, TSGP) ○ Process was refined for FY08, as explained below
165 Days	2008	<ul style="list-style-type: none"> • Cooperative Agreement process was refined based on lessons learned from FY07: <ul style="list-style-type: none"> ○ Meet with the regions earlier, and more often in the application process ○ TSA had agencies submit “project concepts” upfront, so that agencies would not invest time in writing complete Investment Justifications (IJs) that had significant issues and/or were not eligible • Timeline still did not have final agency IJs due until 90 days after awards were announced • Retroactive elimination of the match affected the approval timeframe, as several agencies chose to revise their IJs

Average Approval Process Time	Fiscal Year	Process Notes
		<ul style="list-style-type: none"> • Overall approval timeframe shortened from FY07 process: 6 months after retroactive elimination of match (October 2008), all Tier I projects have been acted on
0 Days	2009	<ul style="list-style-type: none"> • TSA met with each region before the guidance was released to discuss with the agencies the aggressive timelines that would be pursued in FY09. This initial outreach was critical in meeting deadlines later in the process. • TSA met with each region several times during the application period phase, allowing for more security and grant funding discussions upfront, and thereby generating higher quality projects quickly. • TSA imposed more stringent deadlines for FY 2009. IJs and Detailed Budgets were due much earlier in the FY 2009 process than in previous years <ul style="list-style-type: none"> ○ In previous years, Tier I final IJs were not due until 90 days after awards were announced ○ In FY09, Tier I final IJs were submitted approximately 6 weeks in advance of award announcement • Eliminated redundant TSA detailed review of budget. FEMA alone reviews budget. • TSA approved final IJs from the Tier I agencies in advance of the award announcements

QUESTIONS FOR THE RECORD SUBMITTED BY

CHAIRMAN DAVID PRICE

**John Sammon, Assistant Administrator of Transportation Sector
Network Management, Transportation Security Administration
Securing the Nation's Rail and Transit Systems**

Transit and Passenger Rail Grants

Question: TSA and FEMA are both involved in the grant process: TSA determines the criteria and what is eligible to receive a grant while FEMA distributes the funding. According to GAO, transit agencies have reported that the lack of predictability in how TSA will assess grant projects against funding priorities makes it difficult to engage in long-term planning of security initiatives. Specifically, transit agencies have reported receiving funding to begin projects—such as retrofitting their transit fleet with security cameras or installing digital video recording systems—but are not able to finish these projects in subsequent years because TSA had changed its funding priorities. Mr. Sammon, who's responsible for deciding priorities, FEMA or TSA?

ANSWER: The Transit Security Grant Program (TSGP) is administered by the Department of Homeland Security (DHS) through a partnership between the Federal Emergency Management Agency and the Transportation Security Administration (TSA). Within this partnership, and consistent with the *Aviation and Transportation Security Act* (Public Law 107-71), TSA provides transit system subject matter expertise and determines the primary security architecture for the TSGP. TSA's subject matter experts set program and funding priorities, craft all selection criteria, and review the security components of grant applications.

Question: Please explain how transit agencies are to complete long term projects, which usually address large vulnerabilities, if the rules of the game continue to change?

ANSWER: Projects that address large vulnerabilities, such as hardening measures for bridges and tunnels, can be complex and expensive, requiring several phases and funding sources across multiple fiscal years. The Transportation Security Administration (TSA) encourages the planning and funding of long-term projects by working with transit agencies to identify specific and discrete phases that can be completed with the funding available through the Transit Security Grant Program (TSGP) and within the grant period of performance. The priorities in the TSGP have remained consistent for the past several grant cycles, focusing on the Transit Security Fundamentals, which include operational activities such as training, public awareness, visible and unpredictable deterrence, and drills/exercises; and protection of high risk/high consequence assets and systems such as underwater and underground rail assets, tunnels, and bridges.

Question: The Committee has heard numerous complaints from mass transit and passenger rail entities that TSA does not support investments in complex infrastructure hardening projects which require multi-year funding. States have also noted that without the ability to plan and undertake long term projects, funds will be used for off-the-shelf technologies, such as closed circuit television cameras, which may not mitigate risk as much as more ambitious projects would do. How do you respond to these concerns? How does TSA fund multi-year, complex infrastructure investments?

ANSWER: The uncertainty about future grant availability and levels of funding can be an obstacle when transit agencies plan for funding large projects. However, the process that the Transportation Security Administration (TSA) undertakes to work with the transit agencies to help them plan for larger projects in discrete and separate phases helps agencies recognize security benefits through the current funding even if future funding may not be available. In addition, TSA is currently exploring options for committing to fund multi-year projects. Such approaches, however, are dependent on whether, and at what level, grants are appropriated in future years. TSA is committed to identifying options that will help reduce the uncertainty of future funding.

The Transportation Security Administration (TSA) encourages the planning and funding of long-term projects by working with transit agencies to identify specific phases that can be completed with the funding available through the Transit Security Grant Program. TSA works with the transit agencies to help them plan for larger projects in discrete and separate phases, which helps agencies recognize security benefits through the current funding even if future funding is not available.

Question: Mr. Sammon, please describe the risk methodology used to award transit and rail grants.

ANSWER: The risk methodology used to award transit and rail grants under the Transit Security Grant Program (TSGP) has been consistent over the past several grant cycles, and is consistent with the risk methodology used to determine eligibility for the core Department of Homeland Security (DHS) State and local grant programs.

Within the TSGP, eligibility and target funding levels are predicated on a systematic risk analysis that aggregates all of the eligible transit agencies within a given metropolitan area, and then rates these clusters of eligible systems for comparative risk. The TSGP risk formula is based on a 100 point scale comprised of threat (20 points) and vulnerability/consequence (80 points) variables. Each variable set is assigned a weight as part of the overall formula, and all eligible jurisdictions are empirically ranked in each instance on a numerical scale from lowest to highest.

The DHS risk assessment methodology considers critical infrastructure system assets, and characteristics that might contribute to their risk, such as: intelligence community assessments of threat, potentially affected passenger populations, and the economic impact of attack. The relative weighting of variables reflects DHS' overall risk assessment and program priorities. Specific variables include, but are not limited to, the unlinked passenger trips for rail and bus systems, the number of underground track miles, the number of underwater tunnels, and the location-specific intelligence community risk analysis. We would be happy to review the risk methodology in more detail in a setting that supports sensitive security information and discussions.

Question: According to Mr. Eckles during the hearing, the Federal Transit Authorities' (FTA) grants process is often less burdensome than DHS' grants process. Has TSA or FEMA ever considered operating the Transit Security Grants more like FTA grants to simplify the process?

ANSWER: The Transportation Security Administration (TSA) has been in contact with the Federal Transit Administration to learn more about its award processes in order to determine which practices could be adopted, recognizing that TSA also has a responsibility to ensure that Transit Security Grant Program (TSGP) funds are awarded to projects that are effective at reducing risk. In addition, TSA is continually evaluating ways in which to streamline and simplify the application and funding process for the TSGP. In the fiscal year (FY) 2007 cycle, TSA introduced a "fast-track" funding approach for training projects, which greatly simplifies the application, approval, and award processes. TSA has received very positive feedback on this process from several agencies, including the Los Angeles County Metropolitan Transportation Authority. Based on the

success of the “fast-track” training program, TSA is exploring how the “fast-track” approach can be applied to other project types, such as operational deterrence, closed-circuit television, and fencing, for the FY 2010 cycle.

Working with the Department of Transportation

Question: The title of this hearing is “Securing the Nation’s Rail and Transit Systems”. That has never been more important given the infrastructure investments that will take place in this country over the next few years as a result of the American Recovery and Reinvestment Act-- \$8.4 billion was provided for Transit grants and \$1.4 billion for Amtrak. GAO said it best “The nation’s economic vitality and the quality of life of its citizens depend significantly on the availability, dependability, and security of its surface transportation network.” Given the relatively small amount of funds DHS has for Transit Security grants, \$400 million in FY 2009 and \$150 million in the American Recovery and Reinvestment Act, what is DHS doing to leverage these security resources to ensure our nation’s growing infrastructure remains safe?

ANSWER: The Transportation Security Administration (TSA) has placed a priority on funding Transit Security Grant Program projects which protect multi-user, high density key infrastructure such as tunnels, high density stations, and train control systems; single user, high density key infrastructure, such as stations and bridges; and key operating asset protection such as bus and rail yards and maintenance facilities.

The Department of Homeland Security will coordinate closely with the Department of Transportation to ensure that security considerations are integrated into capital improvements, transit system expansions, and new starts implemented through the expanded investment in rail and transit development under the American Recovery and Reinvestment Act.

Question: Mr. Sammon, what is your relationship with the Department of Transportation (DOT), given that the majority of transit infrastructure grants are funded through them?

ANSWER: The Transportation Security Administration (TSA) maintains a close and professional working relationship with the Department of Transportation (DOT) on matters relating to security in the various transportation modes. Formal coordination occurs through the Transportation Sector Government Coordinating Council (GCC) and each of the modal GCCs. Formed under the National Infrastructure Protection Plan, TSA chairs these councils. Annexes to the Department of Homeland Security/DOT Memorandum of Understanding address respective roles and responsibilities and set the parameters of coordinated actions. Most importantly, the General Managers of the modal security divisions at TSA and their staffs regularly consult and coordinate with their counterparts in the DOT modal administrations.

Question: Mr. Sammon, how is DHS working with DOT to deal with our rail and transit vulnerabilities?

ANSWER: The Transportation Security Administration (TSA) works closely and collaboratively with the Federal Transit Administration (FTA) to advance security strategies and programs to mitigate vulnerabilities and manage risk in mass transit and passenger rail systems. These efforts include:

- Developing Security Guidelines and Action Items: In 2007, TSA and FTA, in coordination with the Mass Transit Sector Coordinating Council updated the action items developed by FTA in the aftermath of September 11, 2001. The effort resulted in 17 Security and Emergency Management Action Items encompassing areas foundational to effective security programs in mass transit and passenger rail. TSA and FTA also collaborated to update and expand the Recommended Protective Measures for the threat levels under the Homeland Security Advisory System.

- Assessing Critical Systems and Conducting Vulnerability Assessments: Critical mass transit and passenger systems and assets have been identified via a collaborative effort among multiple public and private entities including TSA and FTA. TSA's Transportation Security Inspection-Surface Program continued these efforts with the Baseline Assessment and Security Enhancement (BASE) program, which was jointly developed by TSA and FTA in coordination with the Mass Transit Sector Coordinating Council. The program reviews transit systems implementation of the 17 Security and Emergency Management Action Items.
- Conducting Security Reviews and Audits: In conjunction with FTA, TSA initiated joint security reviews and audit activities with the State Safety Oversight Agencies.
- Providing Public Transportation Emergency Preparedness Workshops: This joint TSA/FTA initiative brings the Federal transportation security partners together with State, local, and tribal government representatives and the local first responder community to discuss security prevention and response efforts and ways to work together effectively to prepare and protect their communities.
- Conducting Security and Safety Roundtables: TSA and FTA partner in Transit Security and Safety Roundtables, which bring together security coordinators and safety directors from the nation's 50 largest transit facilities.
- Inspecting Bus and Rural Public Transportation Systems: A joint effort with FTA through the Bus Safety and Security Program integrates TSA inspectors to conduct BASE assessments on bus-only systems in smaller cities and rural areas.
- Providing Public Awareness and Training: TSA partners with FTA to advance the Mass Transit Security Training Public Awareness/Transit Watch.
- Facilitating Information Sharing: The Mass Transit and Passenger Rail Security Information Network facilitate regular coordination of intelligence and security-related information through meetings, teleconferences, and message exchanges.

Question: The budget blueprint for 2010 highlights \$25 million for integrated planning at DHS and the Department of Transportation to inform the development and modernization of intermodal freight infrastructure linking coastal and inland ports to highway and rail networks. How do you envision this process working? Will this work more closely link security to safety and mobility programs at DOT?

ANSWER: DHS is to receive \$10 million of the \$25 million for integrated intermodal freight infrastructure planning. This funding will support the creation of a Securing Coordination Office within DHS Policy to provide integrated planning between DHS components (including the Transportation Security Administration, the Office of Infrastructure Protection, and the United States Coast Guard) and the Department of Transportation in the area of maritime transportation, as well as in other homeland security mission areas. The first deliverables for this office in FY 2010 will be as follows:

- A coordinated strategic plan and strategic metrics to guide development and modernization of intermodal freight infrastructure linking coastal and inland ports to highways and rail networks.
- Intermodal freight infrastructure needs and capability gaps
- Recommendations to address the needs and capability gaps

The recommendations to address intermodal freight infrastructure needs and capability gaps will be incorporated into DHS's 5-year programming and budgeting guidance as appropriate, and tracked to ensure they are achieved. Similar recommendations for the Department of Transportation will be developed jointly with DHS, for disposition within the Department of Transportation's programming and budgeting process.

Yes, this will work more closely link security to safety and mobility programs at DOT. In FY 2010 and beyond, the Securing Coordination Office will continue to coordinate the modernization of freight infrastructure with the Department of Transportation, as well as developing strategic plans and metrics and identifying capability gaps for other areas within the Securing functional area, such as securing critical infrastructure and key resources. This will provide better coordination of DOT's existing safety and mobility programs, including those dealing with highways, hazardous materials, railroads, pipelines, and aviation, with related homeland security efforts, enabling both DHS and DOT to meet their missions more effectively and efficiently.

Surface Transportation Inspectors

Question: TSA's transportation security inspectors work with mass transit and freight rail entities to review and assess their security programs for gaps. These assessments aid in the allocation of grant funds and the formulation of future regulations. The inspectors also participate in Visible Intermodal Prevention and Response (VIPR) exercises, which is an unannounced, high-visibility presence in a mass transit or passenger rail environment. A February 2009 Inspector General report made a number of recommendations on how to improve the effectiveness of TSA's surface transportation security inspectors, including assessing how VIPR exercises can be improved and expanding the number of inspectors. In this report, the IG noted that surface transportation security inspectors do not add as much value in a VIPR exercise as other TSA participants, such as air marshals or screeners, because they are not trained in behavior detection, have no training in passenger screening, are unable to detect explosives and are not law enforcement authorities. However, within the last year TSA has hired 75 inspectors specifically to participate in the VIPR exercises and the 2010 budget blueprint seeks \$50 million to fund 15 additional VIPR teams solely dedicated to surface transportation modes. Why does TSA plan on focusing these inspectors on VIPR activities if their presence is not as valuable as other participants? What is TSA doing to make sure they are not underutilized in these exercises?

ANSWER: Most often, Surface Transportation Security Inspectors as well as the Assistant Federal Security Directors for Surface have the best working relationships with the host transit agencies and provide a sense of credibility. Inspectors have in-depth knowledge of transit personnel, systems, and operations and can advise law enforcement authorities and other entities on operational requirements and safety issues. Inspectors also routinely conduct security and criticality assessments, including station profiles, and can provide insight garnered from routine system observations. Accordingly, the Surface Transportation Security Inspectors bring expert domain knowledge of the transit system to the table. The VIPR teams that would be funded by the \$50 million in the 2010 budget blueprint would include Surface Transportation Security Inspectors along with Transportation Security Officers and other personnel.

The Transportation Security Administration's Surface Transportation Security Inspection Program recently placed one dedicated full time position at the Visible Intermodal Prevention and Response (VIPR) Joint Coordination Center at the Freedom Center. This position assists in VIPR coordination, including local and regional concept of operations planning and implementation. The position also assists in identifying areas in which surface inspectors can add unique value to deployments, such as in providing a high level of surface transportation domain awareness and subject matter expertise.

Question: The IG points out that TSA's inspector workforce (175) is very small compared to other federal agencies with inspectors. This level may result in inadequate staffing to carry out current assessment

duties, which grew dramatically after the enactment of the 9/11 Act, or future compliance duties. Do you concur with this assessment? If so, what are you doing to address this concern?

ANSWER: The Transportation Security Administration (TSA) has begun hiring an additional 50 surface inspectors with funds provided for the implementation of the 9/11 Act. In addition, TSA has initiated a staffing study to assist in determining the overall number of Surface Transportation Security Inspectors needed. TSA anticipates that the staffing study will be completed in the near term.

Question: In the Department's most recent monthly obligation report, 47 percent of surface transportation security dollars carried over into fiscal year 2009. The majority of this carryover is in staffing and operations--over \$16 million. While I recognize that some of this funding may reflect the transfer from the 9/11 Act funding provided in fiscal year 2008, not all of it may be from this transfer. Please explain for the Committee why TSA carried over \$16 million in staffing and operations, as well as how and when this will be obligated.

ANSWER: The \$16 million consists of \$14.8 million received in fiscal year (FY) 2008 9/11 Act implementation funding and \$1.2 million in operating funds. Because the FY 2008 9/11 funding was received later in the fiscal year, contracts were not awarded in FY 2008. However, TSA is confident it will obligate the funds in FY 2009.

The Transportation Security Administration fully intends to obligate the remaining fiscal year (FY) 2008 funds for the implementation of the 9/11 Act in FY 2009. These funds will be obligated for surface initiatives specified in the 9/11 Act.

Question: In addition, there is also a large carryover for rail security inspectors and canines but not nearly of the same magnitude. In fiscal year 2008, TSA planned to hire additional inspectors. Were these positions not filled in a timely fashion? If so, how many inspectors are on-board now and what is the agency's plan to fill the remaining vacancies?

ANSWER: To date, the Transportation Security Administration (TSA) has been successful in hiring 60 of the 75 surface inspector positions provided for in fiscal year 2008. TSA continues to work diligently to fill the remaining 15 positions.

To date, the Transportation Security Administration has been successful in hiring 60 of the 75 surface inspector positions provided for in fiscal year 2008.

The Transportation Security Administration continues to work diligently to fill the remaining 15 positions by posting job listings and actively recruiting applicants from both the public and private sectors.

Question: The expenditure plan to implement recommendations of the 9/11 Act includes funding for 50 additional surface transportation inspectors. What is your plan to hire these inspectors? When will they be onboard?

ANSWER: Job announcements for the majority of the additional 50 Surface Transportation Security Inspector positions funded under the 9/11 Act have opened and closed. The Transportation Security Administration (TSA) is working diligently to fill these positions. TSA has increased efforts to recruit new Surface Transportation Security Inspectors that have relevant transportation security experience as required by the 9/11 Act, including notifying key surface transportation industry officials of posted job announcements.

The Transportation Security Administration anticipates the vacancies will be filled by the end of fiscal year 2009.

Question: Because TSA had a difficult time hiring the last 75 surface transportation inspectors, what will you be doing to entice people to apply for and accept the 50 new surface transportation inspector jobs in a timely fashion?

ANSWER: The Transportation Security Administration has increased efforts to recruit new Surface Transportation Security Inspectors that have relevant transportation security experience as required by the 9/11 Act, including notifying key surface transportation industry officials of posted job announcements.

Question: Does the funding contained in the expenditure plan carry through fiscal year 2010?

ANSWER: The Transportation Security Administration anticipates full expenditure of the funds in fiscal year 2009.

Question: On average, how much time do surface transportation inspectors devote to rail and transit security assessments, Visible Intermodal Protection and Response (VIPR) operations, training, and other activities? Please answer by category and for the last three fiscal years.

ANSWER: The following table outlines the average percentage of work time surface inspectors expended on activities in the field. Please note that data is available only after fiscal year (FY) 2007, as the program was primarily in its initial developmental, staffing, and training phase in FY 2006. Additionally, many of the current activities being conducted in the field were implemented in or after FY 2007. For the Administrative activity, approximately 80 percent of administrative time is in support of pre-inspection/assessment planning activities and post-activity report writing. A smaller portion of reported administrative time (approximately 20 percent) is attributed to preparing travel paperwork such as authorizations and vouchers, completing time and attendance reports, and monthly expense reports.

Administrative	18.0%	17.9%	22.5%
Travel ²	12.6%	12.9%	11.1%
Site Visits/Security Observations ³	7.4%	7.2%	11.9%
Station Profiles ⁴	7.9%	6.9%	5.2%
Security Analysis and Action Program ⁵	0.1%	<0.1%	<0.1%
Stakeholder Outreach ⁶	9.6%	9.1%	8.4%
Training ⁷	11.9%	15.5%	22.0%
Baseline Assessment for Security Enhancement (BASE) ⁸	6.6%	5.5%	2.3%

1 Data shown is from October 2008-January 2009.

2 Time expended traveling in support of all field inspection/assessment activities or required training.

3 Time expended on site visits to transportation facilities/stations to review and/or observe security operations (other than Station Profiles, BASEs, SAs, etc.)

4 Time expended on conducting a profile of a passenger/transit rail or bus station, or other critical infrastructure.

5 Hours dedicated to completing a Security Analysis and Action Program assessment.

6 Hours expended attending committee, stakeholder, and internal meetings as well as conferences and conference calls.

7 Time expended attending basic and recurrent training courses or sessions (includes TSA training, FLETC, Railroad Operations training at TTCI in Pueblo, etc.)

8 Time dedicated to conducting Baseline Assessment for Security Enhancement (BASE) reviews in mass transit.

Security Action Item Review Freight) ⁹	14.3%	15.1%	3.9%
Visible Intermodal Prevention and Response (VIPR) ¹⁰	N/A ¹¹	2.2% ₃	4.6%
Corridor Assessments ¹²	N/A ¹³	0.2%	1.1%
Other Field Activity ¹⁴	11.7%	7.5%	6.8%

Visible Intermodal Protection and Response Teams

Question: How much time do inspectors devote to other surface transportation modes, such as commercial vehicles or highway programs and what specifically does this work entail?

ANSWER: Surface Transportation Security Inspectors, and the related security programs they execute, have primarily focused on passenger rail (including mass transit) and freight rail. In addition, beginning in fiscal year 2009, the Surface Transportation Security Inspection Program provided Surface Transportation Security Inspectors with training on conducting Corporate Security Reviews of motor carriers and shippers of hazardous materials.

On March 24, 2009, Surface Transportation Security Inspectors began conducting Corporate Security Reviews (CSRs) on companies that have agreed to participate in the program. Currently, the number of CSRs being conducted by surface inspectors is minimal and does not significantly impact their current workload. Once the initial CSRs are completed, a review of the program will be performed to determine the level of future support surface inspectors can offer in conducting additional CSRs.

Question: The budget blueprint for fiscal year 2010 indicates that TSA plans to hire enough inspectors to form 15 additional VIPR teams. In total, how many additional inspectors will these be to fill 15 VIPR teams?

ANSWER: The Transportation Security Administration is currently developing the plan to implement the budget blueprint for fiscal year 2010.

Question: Since TSA has had a difficult time filling its current inspector positions, what is the estimated timeline to hire these new VIPR inspectors and when do you anticipate them being on board?

ANSWER: Once the team composition has been finalized, the Transportation Security Administration anticipates filling all the new Visible Intermodal and Prevention Response positions in fiscal year 2010.

Question: To date, how many VIPR deployments have there been? As part of this response, please break out these deployments by fiscal year as well as list the cities these operations occurred in

⁹ Time dedicated to conducting Security Action Item (SAI) reviews in freight rail.

¹⁰ Time dedicated to planning and supporting VIPR operations.

¹¹ Data for VIPR was not tracked until February 2008.

¹² Time dedicated to conducting Corridor Assessments in freight rail.

¹³ Data for Corridor Assessments was not tracked until September 2008.

¹⁴ Time for incident response, airport operations support, program development/research, participation in security exercises, and other field activities.

ANSWER: The tables that follow illustrate the Visible Intermodal Prevention and Response (VIPR) operations by fiscal year and by mode. Also listed are the city locations at which VIPR operations have been conducted.


Visible Intermodal Prevention and Response (VIPR)

JOINT COORDINATION CENTER (JCC)

VIPR MODE TOTALS

October 01, 2005 - September 30, 2006

Area	Hwy	Ft/ Rail	Pipeline	Mass Transit	Maritime	Cargo	Comm AV	Gen AV	Total
Central									30
East	0	0	0	77	11	0	30	0	118
West	0	0	0	12	0	0	15	0	27
Total	0	0	0	114	11	0	45	0	175

SURFACE MODE TOTAL: 130

AVIATION MODE TOTAL: 45

GRAND TOTAL: 175


Visible Intermodal Prevention and Response (VIPR)

JOINT COORDINATION CENTER (JCC)

VIPR MODE TOTALS

October 01, 2006 - September 30, 2007

Area	Hwy	Ft/ Rail	Pipeline	Mass Transit	Maritime	Cargo	Comm AV	Gen AV	Total
Central									50
East	4	0	0	85	5	0	71	0	165
West	2	0	0	24	13	0	19	0	58
Total	17	0	0	136	18	0	100	0	273

SURFACE MODE TOTAL: 170

AVIATION MODE TOTAL: 103

GRAND TOTAL: 273


Visible Intermodal Prevention and Response (VIPR)

JOINT COORDINATION CENTER (JCC)

VIPR MODE TOTALS

October 01, 2007 - September 30, 2008

Area	Hwy	Ft/ Rail	Pipeline	Mass Transit	Maritime	Cargo	Comm AV	Gen AV	Total
Central									312
East	32	4	4	221	85	1	164	85	596
West	3	3	0	55	11	11	122	71	276
Total	46	29	4	337	100	16	412	239	1184

SURFACE MODE TOTAL: 517

AVIATION MODE TOTAL: 667

GRAND TOTAL: 1184


Visible Intermodal Prevention and Response (VIPR)

JOINT COORDINATION CENTER (JCC)

VIPR MODE TOTALS

October 01, 2008 - March 24, 2009

Area	Hwy	Ft/ Rail	Pipeline	Mass Transit	Maritime	Cargo	Comm AV	Gen AV	Total
Central	7	2	1	72	10	3	128	8	231
East	105	0	1	252	29	16	204	54	662
West	1	0	0	52	10	6	75	11	155
Total	114	2	2	376	49	25	407	73	1048

SURFACE MODE TOTAL: 643

AVIATION MODE TOTAL: 405

GRAND TOTAL: 1048

VPR Operations by City/State																	
1200-202																	
Total-272 Cities																	
#	CITY	STATE	#	CITY	STATE	#	CITY	STATE	#	CITY	STATE	#	CITY	STATE			
1	Anchorage	AK	51	Anaheim County	CO	101	Moline	IL	151	Lebanon	NH	201	Ulster	NY	251	Arlington	VA
2	Juneau	AK	52	Colorado Springs	CO	102	Brownsville	IN	152	Manchester	NH	202	Valley Stream	NY	252	Chesterfield	VA
3	Seward	AK	53	Denver	CO	103	Indianapolis	IN	153	Atlantic City	NJ	203	Warren	NY	253	Dallas	VA
4	Birmingham	AL	54	Jefferson County	CO	104	Zionsville	IN	154	Astoria	NJ	204	White Plains	NY	254	Hendon	VA
5	Mobile	AL	55	Watkins	CO	105	Wichita	KS	155	Bayonne	NJ	205	Yonkers	NY	255	Jonestown	VA
6	Barronville	AR	56	Hartford	CT	106	Elstange	KY	156	Belford	NJ	206	Cincinnati	OH	256	Leesburg	VA
7	Little Rock	AR	57	New Haven	CT	107	Hobson	KY	157	Belmar	NJ	207	Cleveland	OH	257	Marion	VA
8	Buckley	AZ	58	New London	CT	108	Lexington	KY	158	Camden	NJ	208	Columbus	OH	258	Newport News	VA
9	Chandler	AZ	59	Norwalk	CT	109	Louisville	KY	159	Cape May	NJ	209	Dorton	OH	259	Norfolk	VA
10	Phoenix	AZ	60	South Norwalk	CT	110	Baton Rouge	LA	160	Deerpark	NJ	210	Toledo	OH	260	Richmond	VA
11	Scottsdale	AZ	61	Windsor Locks	CT	111	New Orleans	LA	161	Edison	NJ	211	Oklahoma City	OK	261	Stafford	VA
12	Tempe/Mesa	AZ	62	Washington	DC	112	Boston	MA	162	Essex County	NJ	212	Eugene	OR	262	Westminster	VA
13	Tucson	AZ	63	Dover	DE	113	Fresno	MA	163	Elmer	NJ	213	Portland	OR	263	Williamsburg	VA
14	Anahaim	CA	64	New Castle	DE	114	Hingham	MA	164	Hoboken	NJ	214	Toledo	OH	264	Burlington	VT
15	Antiochia	CA	65	Wilmington	DE	115	Culter	MA	165	Jackson	NJ	215	Easton	PA	265	Seattle	WA
16	Burlington	CA	66	Cape Canaveral	FL	116	Westwood	MA	166	Jersey City	NJ	216	Erie	PA	266	Spokane	WA
17	Calico	CA	67	Clewiston	FL	117	Woods Hole	MA	167	Kearny & Bayonne	NJ	217	Lancaster	PA	267	Green Bay	WI
18	Corona	CA	68	Dade	FL	118	Baltimore	MD	168	Linden	NJ	218	Philadelphia	PA	268	La Crosse	WI
19	Covina	CA	69	Dania Beach	FL	119	Rochville	MD	169	Newark	NJ	219	Reading	PA	269	Madison	WI
20	Emeryville	CA	70	Fort Lauderdale	FL	120	Saugor	ME	170	Pleasant County	NJ	220	West Milton	PA	270	Milwaukee	WI
21	Fresno	CA	71	Fort Myers	FL	121	Bar Harbor	ME	171	West Deptford	NJ	221	San Juan	PR	271	Sturtevant	WI
22	Glenfield	CA	72	Fort Lauderdale	FL	122	Deer Valley	MI	172	Albuquerque	NM	222	Block Island	RI	272	Cheyenne	WY
23	Golconda	CA	73	Hollywood	FL	123	Detroit	MI	173	Las Vegas	NV	223	Bridgeport	RI			
24	Industry	CA	74	Jacksonville	FL	124	East Lansing	MI	174	Reno	NV	224	Kingston	RI			
25	Irvine	CA	75	Key West	FL	125	Frost	MI	175	Albany	NY	225	Narragansett	RI			
26	Long Beach	CA	76	Marathon	FL	126	Fresno	MI	176	Buiston Spa	NY	226	Providence	RI			
27	Los Angeles	CA	77	Miami	FL	127	Grand Rapids	MI	177	Bronx	NY	227	Warwick	RI			
28	Montclair	CA	78	Opa-Locka	FL	128	Lansing	MI	178	Rochester	NY	228	Westerly	RI			
29	Moorestown	CA	79	Orlando	FL	129	Mackinaw City	MI	179	Buffalo	NY	229	Charleston	SC			
30	Newhall	CA	80	Palm Beach	FL	130	Fort Huron	MI	180	Farmingdale	NY	230	Brookings	SD			
31	Northridge	CA	81	Pensacola	FL	131	Romulus	MI	181	Flushing	NY	231	Sioux Falls	SD			
32	Oakland	CA	82	Port Canaveral	FL	132	Saginaw	MI	182	Herkon	NY	232	Tea	SD			
33	Ontario	CA	83	Fort Everglades	FL	133	St. Ignace	MI	183	Hudson County	NY	233	Memphis	TN			
34	Orange	CA	84	Punta Gorda	FL	134	Traverse City	MI	184	Jamaica	NY	234	Austin	TX			
35	Orange County	CA	85	Sacramento	FL	135	Fridley	MN	185	Long Island	NY	235	Casper	TX			
36	Orland	CA	86	Sanford	FL	136	Minneapolis/St. Paul	MN	186	Manhattan	NY	236	Dallas/Fort Worth	TX			
37	Palm Springs	CA	87	Sarasota	FL	137	Kansas City	MO	187	Mt. Vernon	NY	237	El Paso	TX			
38	Palmdale	CA	88	Tampa	FL	138	St. Louis	MO	188	Nassau	NY	238	Galveston	TX			
39	Pomona	CA	89	Atlanta	GA	139	Outpost	MS	189	New Hyde Park	NY	239	Houston	TX			
40	Rialto	CA	90	Savannah	GA	140	Jackson	MS	190	New Rochelle	NY	240	Irvington	TX			
41	San Diego	CA	91	Guam	Guam	141	Belgrade	MT	191	New York	NY	241	Levado	TX			

42	San Francisco	CA	52	Honolulu	HI	142	Charlotte	NC	192	Pittsburgh	NY	242	Lowland	TX			
43	San Pedro	CA	93	Kahului	HI	143	Durham	NC	193	Queens	NY	243	Lubbock	TX			
44	San Ysidro	CA	94	Lihoe	HI	144	Greensboro	NC	194	Ramapo	NY	244	McAllen	TX			
45	Santa Ana	CA	95	Mazt	HI	145	Havelock	NC	195	Rochester	NY	245	San Antonio	TX			
46	Santa Barbara	CA	96	Des Moines	IA	146	Raleigh	NC	196	Rome	NY	246	St. Croix	USVI			
47	Santa Clarita	CA	97	Boise	ID	147	Wake County	NC	197	Ronkonkoma	NY	247	St. Thomas	USVI			
48	Sylmar	CA	98	Nampa	ID	148	Bismarck	ND	198	Saratoga	NY	248	Farmington	UT			
49	Van Nuys	CA	99	Bloomfield	IL	149	Omaha	NE	199	Saratoga Springs	NY	249	Layton	UT			
50	Ventura	CA	100	Chicago	IL	150	Laconia	NH	200	Syracuse	NY	250	Salt Lake City	UT			

Question: It is my understanding that TSA dramatically increased the number and frequency of VIPR deployments beginning in July 2007 from an average of one exercise per month to one or two exercises per week. What led to the increase in exercises? Is TSA still conducting one or two VIPR exercises per week?

ANSWER: Intelligence related to the attacks on transit systems in Madrid and London, along with Transportation Security Administration’s (TSA’s) analysis of the risk associated with transit systems, served as the catalyst to establish a formal Visible Intermodal Prevention and Response (VIPR) program in 2007 and resulted in an increase in VIPR operations. TSA also created the Joint Coordination Center (JCC), which serves as the nationwide coordination element for TSA and all of its VIPR operations. The JCC coordinates asset deployment during times of crisis and non-routine operations through specific taskings sent to field elements to conduct VIPR operations.

In addition, TSA embarked on a robust outreach campaign to its internal and external stakeholder/partners, committing additional resources and increasing Federal, state and local transportation stakeholder/partner awareness of, and commitment to, VIPR deployments.

TSA’s current VIPR deployment methodology utilizes existing intelligence reporting, empirical data, and security and threat-based assessments and analysis. In addition, VIPR deployments incorporate elements of randomness and are unpredictable in frequency, location, and duration. VIPR teams, deployed after thorough planning with Federal, state and local security and law enforcement officials, supplement existing resources in response to an intelligence-driven threat or provide a deterrent presence through risk-based deployments. VIPR teams are also deployed to provide event response and recovery capabilities during unplanned events.

Currently, an average of 40 to 50 Visible Intermodal Prevention and Response operations are conducted weekly by dedicated and non-dedicated assets, with a majority of the deployments being generated locally by the Federal Security Directors and Federal Air Marshal, Special Agents-in-Charge.

Currently, an average of 40 to 50 Visible Intermodal Prevention and Response operations are conducted weekly by dedicated and non-dedicated assets, with a majority of the deployments being generated locally by the Federal Security Directors and Federal Air Marshal, Special Agents-in-Charge.

Question: The report accompanying the fiscal year 2009 Appropriations Act required TSA to report on performance standards to measure the success of its VIPR teams in detecting and disrupting terrorism. In addition, the report was also to identify the methodology used to determine the distribution of VIPR resources and personnel among the various modes of transportation. What is the status of this report? When can we expect to see it? What are some of the preliminary findings that you have?

ANSWER: A draft of the Visible Intermodal Prevention and Response Teams report is currently undergoing executive level clearance within the Transportation Security Administration.

After Transportation Security Administration (TSA) approval of the draft Visible Intermodal Prevention and Response Teams report, it will be reviewed by the Department of Homeland Security and the Office of Management and Budget. TSA anticipates that a final report will be ready for delivery to Congress during the third quarter of fiscal year 2009.

The report cannot be forwarded prior to the Department of Homeland Security and the Office of Management and Budget approval.

Question: According to a 2008 Inspector General report, "participants and outside observers question the value of VIPR exercises....In particular the Federal Law Enforcement Officers Association described the VIPR exercises as "clearly a waste of scarce Federal Air Marshal resources. Transportation security inspectors (TSI) also considered their participation in VIPR exercises unproductive". The IG noted that in their survey of TSIs, 70 percent selected VIPR exercises as one of two duties they performed that were least effective use of their time. Since this report was completed, TSA has requested additional resources to expand VIPR teams. Who should we fund this request? What has TSA done to improve the VIPR program?"

ANSWER: Visible Intermodal Prevention and Response (VIPR) teams provide a tool with unique capabilities to the transportation system. Deterrent effect is best achieved through development and implementation of a joint plan for periodic random, unpredictable deployment of varying force packages at differing times and locations. VIPR teams also augment security during periods of heightened threat as well as during special events, such as political conventions, major sporting events, and other forums of national or regional significance that raise security concerns. Extensive Transportation Security Administration (TSA) outreach has proven effective to break down any pre-existing barriers and establish lasting partnerships within the transportation security and law enforcement community. Transportation stakeholders/partners have reacted positively to the VIPR concept and often request TSA to augment their forces.

TSA's current VIPR deployment methodology supports the Department of Homeland Security's risk-based model to maximize the use of limited assets. TSA utilizes existing intelligence reporting, empirical data, and security and threat-based assessments and analysis. In addition, VIPR deployments incorporate elements of randomness and are unpredictable in frequency, location, and duration. VIPR teams, deployed after thorough planning with Federal, state and local security and law enforcement officials, supplement existing resources in response to an intelligence-driven threat or provide a deterrent presence through risk-based deployments. VIPR teams are also deployed to provide event response and recovery capabilities during unplanned events.

Through the Joint Coordination Center, the Transportation Security Administration (TSA) has developed a Visible Intermodal Prevention and Response (VIPR) Operational Deployment Methodology whereby VIPR deployments are planned and implemented on a risk-based approach utilizing existing intelligence reporting, empirical data, and security and threat-based assessments and analysis. In addition, VIPR operations incorporate elements of randomness and are unpredictable in frequency, location, and duration.

By consistently exercising and deploying assets in a preventative posture, visibly deterring potential criminal and/or terrorist planning and actions, TSA is able to deploy VIPR participants to unplanned (e.g., Hurricane Gustav) or incident driven events to provide event response and recovery capabilities. TSA has also initiated a partnership with the Department of Homeland Security Domestic Nuclear Detection Office to train and equip its VIPR teams with Preventative Nuclear Radiological Detection devices.

Ability of Transit Agencies to Meet Security Requirements:

Question: For the first time since TSA was formed in 2002 and as part of the DHS fiscal year 2008-2010 annual performance report, TSA evaluated the percent of mass transit and passenger rail agencies that were in full compliance with industry-accepted security and emergency management action items to improve security. In total, there were 17 action items and TSA hoped that 50 percent of these entities would be in compliance. For this evaluation, TSA conducted 88 baseline security assessments covering 48 of the 50 largest mass transit and passenger rail agencies. Of the 48 agencies, only 23 percent met the target. According to TSA, the shortfall reflects thoroughness of assessments which far exceed prior security inspections. The 50 largest mass transit and passenger rail agencies will undergo their second assessment in 2009, and TSA hopes to meet or exceed a 40 percent goal. If only 23 percent were in full compliance with industry accepted security and emergency action items in 2008, was it clear to the transit and rail entities what requirements they were being assessed on and what constituted a "passing grade"?

ANSWER: Prior to the assessments, the Transportation Security Administration (TSA) provided mass transit agencies information on the Baseline Assessments for Security Enhancements program and an assessment checklist. Assessed mass transit and passenger rail agencies are very familiar with the 17 Security and Emergency Management Action Items as well as the TSA- and FTA-recommended security actions that were developed in coordination with the mass transit and passenger rail community. In addition, the agencies have received the full report, including ratings in each of the 200+ questions in the assessment checklist and the percentage score in each Security and Emergency Management Action Item.

The 23 percent that were in full compliance includes 11 of the 48 largest (in passenger volume) mass transit and passenger rail agencies assessed. These agencies were able to achieve the high standard set by the measure. To be considered in "full compliance," a mass transit or passenger rail agency must achieve a 90 percent average score across all 17 Security and Emergency Management Action Items, with no one category scoring under 70 percent. The average score on all 17 Security and Emergency Management Action Items among the largest 50 agencies (the scope of the report) was 80 percent. This is a rather significant achievement for a first-time assessment.

Question: What were the common problems TSA security inspectors found when they completed these security assessments?

ANSWER: Based on these assessments, areas of concern included: security training, plans and protocols to respond to various threat levels, public security awareness, exercises and drills, proper handling of Sensitive Security Information, and conducting internal security audits.

Question: TSA has set a goal of having 40 percent of the major mass transit agencies be in full compliance with the industry-accepted security and emergency action items in 2009; almost a doubling of the 2008 results. How is TSA working with these entities to assure the 2008 problems are addressed prior to the 2009 evaluation?

ANSWER: The Transportation Security Administration is:

- 1) Expanding partnerships for security enhancement through regional coordination;
- 2) Elevating the security baseline through the Baseline Assessment for Security Enhancement program and applying these results toward the development of security programs and the evaluation of resource allocations;

- 3) Building security force multipliers through security training of employees and law enforcement, terrorism prevention and response exercises and drills, and public awareness campaigns;
- 4) Leading information assurance by fostering information sharing networks that integrate Federal security partners with mass transit and passenger rail agencies and State and local entities to facilitate timely exchange of intelligence products and security implications at both classified and unclassified levels; and
- 5) Protecting high risk assets and systems through development, testing, and validation of new technologies for the transit environment and targeted application of security grants to achieve the most substantial mitigation of risk and enhancement of security.

Question: According to your performance plan, TSA expects agencies to exceed this target. Why do you believe the largest transit entities will exceed this target the second time around? Is this goal too easy?

ANSWER: The Transportation Security Administration anticipates significant progress from the largest transit entities in performance improvement. Each agency received the complete report from the first Baseline Assessment Security Enhancement (BASE) assessment and has had the opportunity to act upon the results to refine and enhance their security plans, programs, and activities. In many cases, an effort to improve may include submitting project proposals under the Transit Security Grant Program to address concerns identified in the BASE assessment. A second round of BASE assessments conducted on several transit agencies has already shown progress and improvements in multiple areas.

The performance standard is high – to be considered in “full compliance” a mass transit or passenger rail agency must achieve a 90 percent average score across all 17 Security and Emergency Management Action Items, with no one category scoring under 70 percent. Though six additional agencies achieved a 90 percent+ average score on the first Baseline Assessment Security Enhancement assessment, they did not meet the high standard of “full compliance” because of their performance in a single category.

Secretarial Action Directives:

Question: During Secretary Napolitano’s confirmation hearing, she announced that she would focus on surface transportation security because “we have done an awful lot in the aviation world.” Secretary Napolitano followed this up with a Secretarial directive tasking TSA to review current strategies, plans and programs for security of the air, surface, and maritime transportation sectors. The report was also to include a side by side comparison of the threat environment, resources and personnel devoted to each transportation sector. An oral report was due to her by the end of January. What are the largest threats you currently see in the rail and transit environment? How do those threats translate in the grant allocations?

ANSWER: According to a Transportation Security Administration threat assessment published on February 5, 2009, the most significant threats to the passenger rail and transit environment are from improvised explosive devices and improvised incendiary devices. The assessment also cited a commando-style assault as a viable tactic that could be used, such as the terrorist attacks in Mumbai in late November 2008.

Based upon continuous intelligence analysis, extensive security reviews, consultation with operations and security officials of mass transit and passenger rail agencies, State and local government officials, and Federal security partners, the Department of Homeland Security has focused the bulk of the available transit grant dollars in fiscal year (FY) 2009 on the highest-risk systems in our country’s largest metropolitan areas, known as Tier I regions. As a result, the Tier I regions in the Transit Security Grant Program received 93 percent of the FY 2008 grant allocations and a similar percentage of the FY 2009 allocations, respectively. These investments

advanced a range of operational, technological, and hardening capabilities to implement a layered security approach for the mass transit and passenger rail systems at higher risk.

Question: What advice did you provide Secretary Napolitano in response to her Action Directive that may be utilized to strengthen surface transportation security? Will we see some of the recommendations in the near term?

ANSWER: The Transportation Security Administration's suggested areas of emphasis included:

- Risk-based approach to hardening critical infrastructure, underwater passenger rail tunnels, and high volume stations;
- Expanding operational deterrence capabilities;
- Worker training in security awareness, behavioral assessment, and immediate actions to address a threat or security incident;
- Drills and exercises;
- Surface transportation worker security threat assessments;
- Integrated, cost-effective chemical and biological detection solutions at key facilities;
- Timely sharing of accurate intelligence and security-related information; and
- Expanding regional security collaboration among surface transportation providers and local, State, and Federal authorities.

The Transportation Security Administration anticipates that the Secretary will set security priorities based on a thorough evaluation of several factors and priorities, as defined by the Secretary, all of which will drive security program development and allocations of resources, including transportation security grants.

Regional Transit Security Working Groups:

Question: In the FY 2008 grant guidance, TSA made itself a co-chair of the Regional Transit Securing Working Groups for all Tier 1 grantees. These working groups used to be chaired by a State or local transit entity prior to this requirement set by TSA. The Federal government often participated, but the goal of the working group was to have transit entities and States set priorities and hold each other accountable. What precipitated the change in policy? Has there been any benefit to having TSA co-chair these groups? Shouldn't States and local transit agencies have the ability to set regional priorities prior to submitting grant requests?

ANSWER: Beginning in fiscal year (FY) 2007, the Regional Transit Security Working Group (RTSWG) began partnering with the Department of Homeland Security through a cooperative agreement, allowing more robust security discussions to take place about risk, regional priorities, and funding priorities of the Transit Security Grant Program (TSGP). In an attempt to formalize and define the Transportation Security Administration's (TSA's) role in the RTSWG for all regions, the FY 2008 grant guidance included a provision that TSA would serve as a co-chair alongside other co-chairs selected by the region. Naming TSA as a co-chair of the RTSWG was an effort to solidify the relationship between TSA and the regional transit agencies to promote dialogue and security discussions. This approach also allows TSA to actively work with the agencies and participate in the RTSWGs in a way that makes sense for each region, thereby further maturing the cooperative agreement process and fostering continuous dialogue.

Although none of the transit agencies disagreed with TSA's role or participation in the RTSWGs, some expressed concern with the name of "co-chair" that TSA had taken. The importance of TSA in the RTSWGs is not in the name, but in the relationship and participation. Therefore, the FY 2009 TSGP grant guidance

removed the provision that TSA was a "co-chair," and instead let the regions work with TSA to define the leadership and coordination role TSA should take based on their unique needs.

The Transportation Security Administration (TSA) offers security subject matter expertise and is an engaged Federal partner and resource for the transit agencies in the Regional Transit Security Working Groups (RTSWG). Through TSA's role on the RTSWGs, transit agencies have an open, direct, and continuous avenue of communication with the Department of Homeland Security. This dialogue ensures that Federal help and assistance is always within reach.

TSA also provides extensive assistance with the Transit Security Grant Program (TSGP) through its role in the RTSWGs. Through the RTSWGs and other forums, transit agencies can gain guidance and insight into the TSGP process, an important source of funding for many of the nation's most at-risk transit agencies. TSA's presence in the RTSWGs guarantees that the TSGP is a dynamic grant program, responsive to the needs of those it is intended to serve.

States and transit agencies do have the ability to set regional priorities through the Regional Transit Security Working Groups (RTSWG) and the regional approach to transit security. The Transportation Security Administration (TSA) works with the regions to help set regional priorities through the cooperative agreement process. TSA shares risk information with the RTSWGs and discusses the Federal funding priorities of the Transit Security Grant Program (TSGP). This helps to shape and guide the internal regional decisions concerning which projects to apply for funding through the TSGP. TSA meets with each region prior to submitting grant requests to discuss the projects and to work with the region in developing a prioritized list of proposed grant projects.

Access to the TSGP project scoring methodology allows each transit agency to see how its proposed projects rank in order of priority. TSA preliminarily ranks the projects based on risk and effectiveness, and discusses the results with the RTSWG. Through this discussion, the RTSWG has the opportunity to identify certain projects that may be ranked lower on the list, but are of a higher priority to the agencies in the region, and make priority changes to the final ranking of projects that will be funded. This regional collaboration enables the RTSWG to make decisions at the State and local transit agency level within the national priority framework established by the Department of Homeland Security (DHS). This process ensures that the region's concerns are addressed and provides each region with the ability to set their own priorities while still working within the TSGP funding process established by DHS for the nation as a whole.

9/11 Commission Act

Question: The 9/11 Commission Act gave DHS authority to issue fines to mass transit agencies if the agency was found in violation transportation security regulations and directives because they did not address security vulnerabilities. In order to assess these fines, it is my understanding that TSA must develop specific comprehensive compliance regulations for mass transit systems to follow and transportation security inspectors to enforce. Has this been done? If so, please detail for the Committee what compliance activities transit entities must undertake.

ANSWER: The Department of Homeland Security/Transportation Security Administration has a rail Transportation Security Regulation, 49 C.F.R. part 1580, covering freight rail and passenger rail (including mass transit). 49 C.F.R. §§ 1580.5 and 1580.200-203 apply to mass transit (rail) agencies. Mass transit (rail) agencies must appoint a Rail Security Coordinator (49 C.F.R. § 1580.201) and they must report Significant Security Concerns (49 C.F.R. § 1580.203) to DHS.

Question: Please highlight for the Committee what types of fines DHS can assess, how often (to date) TSA has assessed these fines, for what violations, and what these funds are used for upon receipt.

ANSWER: The Department of Homeland Security/Transportation Security Administration may impose civil penalties on any covered person who violates any provision in 49 C.F.R. part 1580. The Implementing Recommendations of the 9/11 Commission Act of 2007 outlines the maximum amounts for civil penalties below in Section 1302. ENFORCEMENT AUTHORITY:

(3) ADMINISTRATIVE IMPOSITION OF CIVIL PENALTIES-

(A) IN GENERAL- The Secretary of Homeland Security may impose a civil penalty for a violation of a regulation prescribed, or order issued, under an applicable provision of this title. The Secretary shall give written notice of the finding of a violation and the penalty.

(B) SCOPE OF CIVIL ACTION- In a civil action to collect a civil penalty imposed by the Secretary under this subsection, a court may not re-examine issues of liability or the amount of the penalty.

(C) JURISDICTION- The district courts of the United States shall have exclusive jurisdiction of civil actions to collect a civil penalty imposed by the Secretary under this subsection if--

(i) the amount in controversy is more than--

(I) \$400,000, if the violation was committed by a person other than an individual or small business concern; or

(II) \$50,000 if the violation was committed by an individual or small business concern; (ii) the action is in rem or another action in rem based on the same violation has been brought; or

(iii) another action has been brought for an injunction based on the same violation.

(D) MAXIMUM PENALTY- The maximum civil penalty the Secretary administratively may impose under this paragraph is--

(i) \$400,000, if the violation was committed by a person other than an individual or small business concern; or

(ii) \$50,000, if the violation was committed by an individual or small business concern.

To date, the Transportation Security Administration (TSA) has not assessed any civil penalties to mass transit (rail) agencies. The current TSA regulation that pertains to mass transit (rail) entities is 49 CFR Part 1580, which became effective on December 26, 2008. The compliance enforcement process for this regulation has not yet been initiated. TSA is currently in the process of training its regulatory workforce on the new regulation and inspection, compliance and enforcement procedure for mass transit. Training for inspectors is scheduled to be completed in May 2009. Furthermore, the Implementing Recommendations of the 9/11 Commission Act of 2007 stipulates that certain requirements must be met before assessing civil penalties against publicly funded transit agencies.

To date, the Transportation Security Administration has not assessed any civil penalties to mass transit (rail) agencies.

Question: The fiscal year 2009 Appropriations bill included \$20 million for TSA to continue to implement recommendations of the 9/11 Act. How the funding was to be spent was left to the Assistant Secretary's discretion but TSA recently submitted a plan allocating these funds. Of the \$20 million provided for these activities in 2009, what percentage will be focused on enhancing rail and transit security?

ANSWER: Of the \$20 million provided, 69 percent (\$13.825 million) will directly focus on enhancing rail and transit security. This will occur through expanded vulnerability and threat assessments, additional security exercises with rail and transit providers, hiring 50 additional surface transportation security inspectors, and

reimbursing the reasonable costs of the existing public transit Information Sharing and Analysis Center (ISAC). Additionally, with the proposed creation of a multi-modal, broad based Transportation Security ISAC that will directly benefit rail, transit, and pipeline stakeholders as well as the aviation community, the percentage increases to 81 percent (\$16.325 million).

Question: For the record, please detail how much of the \$20 million was surface transportation related, including surface transportation inspectors, vulnerability assessments of high risk public transportation agencies, and security exercises. How does this compare to the previous fiscal year?

ANSWER: More than \$16 million of the \$20 million is surface transportation related. The Transportation Security Administration (TSA) is allocating \$5 million in fiscal year (FY) 2009 for implementation of the 9/11 Act by hiring an additional 50 surface transportation security inspectors. This will increase the number of inspectors to 225. TSA is allocating \$5.450 million for vulnerability and threat assessments including risk assessments for transit, rail, pipelines, highways and motor carriers. This funding will encompass high-risk transit agencies, high threat urban area rail corridors, trucking security, and critical infrastructure that are used by these modes. Further, this allocation will also encompass bridge and tunnel studies relating to high risk transit, rail and highway sectors. TSA is allocating \$2.775 million for an expansion of its Intermodal Security Training and Exercise Program (I-STEP). This will allow for additional exercises to occur with key surface transportation providers during FY 2009 and FY 2010. TSA will use \$2.5 million of the FY 2009 funding to create a broad based, virtual, multi-modal Transportation Security Information Sharing and Analysis Center (ISAC) to allow TSA to better transmit intelligence products, including risk assessments, with the transportation security community, including surface transportation stakeholders, and to allow stakeholders to share their products as well with the wider community. TSA will also use \$0.6 million of the FY 2009 funds to reimburse the existing transit ISAC as provided for in the 9/11 Act.

For fiscal year (FY) 2008, the Transportation Security Administration (TSA) received \$30 million in additional funding for implementation of 9/11 Act requirements, as opposed to \$20 million in FY 2009. The FY 2008 funds were directed to somewhat different requirements of the 9/11 Act. During FY 2008, TSA allocated \$13.2 million to develop regulations, strategic planning, reports, and studies that the 9/11 Act required. Most, although not all, of these regulations, plans, reports, and studies related to surface transportation security. TSA devoted \$2.7 million to conduct exercises with surface transportation security stakeholders through the Intermodal Security Training and Exercise Program (I-STEP). TSA also allocated \$0.8 million for inspection and review of critical pipeline facilities. FY 2008 funding of \$11.9 million was devoted to improving the backbone infrastructure of TSA's vetting and credentialing capabilities so that additional populations can be vetted. This includes transit and rail employees as required by the 9/11 Act. TSA also allocated FY 2008 funding of \$1.4 million to security reviews of foreign repair stations, a function that was also required by the 9/11 Act.

Question: The 2009 expenditure plan to implement recommendations of the 9/11 Act includes funding for intermodal security training and exercises. Explain to the Committee how these exercises differ from those provided with grant funds.

ANSWER: The Intermodal Security Training and Exercise Program applies a comprehensive regional approach to develop, prepare for, execute, and apply lessons learned from focused workshops and exercise scenarios tailored to the operating circumstances and needs of the participating mass transit and passenger rail agencies. Specific emphasis is placed on enhancing and testing prevention capabilities. For the most part, grant funds are awarded to address critical infrastructure vulnerabilities and security gaps.

Question: Similarly, the expenditure plan to implement recommendations of the 9/11 Act includes funding for an information sharing and analysis center (ISAC). Explain to the Committee how this ISAC's work will differ than the ISAC's already in existence. For example, the Association of American Railroads has had an ISAC since 9/11 and I believe the transit industry has had one as well. In total, how many transportation ISACs do we have?

ANSWER: This Transportation Security Information Security Analysis Center (TS-ISAC) will differ from the existing ISACs because it will provide a collaborative interface between Transportation Security Administration (TSA) analysts and State, Local, and transportation industry security representatives. Additionally, the TS-ISAC will house all TSA intelligence products and provide a repository for transportation security intelligence and information, and enable the TSA Office of Intelligence workforce to share insights, best practices, and improve the quality of their intelligence products.

The TS-ISAC will be supported by information from the Transportation Security Operations Center (TSA Freedom Center) and TSA's Office of Intelligence Watch Center. This will result in security awareness materials continuously being provided during routine operations, as well as alerts and time-sensitive information during periods of heightened threat.

Currently, there are three functioning transportation Information Sharing and Analysis Centers (ISACs) – the Highway ISAC, the Surface Transportation ISAC, and the Public Transit ISAC. The latter two operate in an effort coordinated by the Association of American Railroads and the American Public Transportation Association.

Question: Is this the first year that funding has been provided for this ISAC? If not, how much has been provided previously and for what purposes?

ANSWER: 2009 is the first year funding has been provided for the Transportation Security Information Sharing and Analysis Center.

Question: Please detail what contract support will be provided for the transportation ISAC in 2009.

ANSWER: The contract support planned for the Transportation Security Information Sharing and Analysis Center will include the development of a Knowledge Management System to support information sharing and collaboration. The system will include: requirements documentation, system development, implementation, field roll-out, access controls, and end-user account management.

Canine Teams

Question: What is the status of the National Explosives Detection Canine Teams used in mass transit? How many teams do you currently have? Where are they operating? Are they at full capacity?

ANSWER: Currently there are 83 explosives detection canine teams operating in 15 Transit Systems in 13 cities. In the remainder of calendar year 2009, the program projects to add an additional 34 teams. Three of these teams are currently in training and will operate in the Delaware River and Bay Authority Maritime Ferry System. In addition, AMTRAK (22 teams in Mass Transit) and the Washington State Patrol (9 teams in the Washington State Maritime Ferry System) have demonstrated their interest in participating in the National Explosives Detection Canine Teams Program.

Mass Transit Teams are currently operating at the following locations:

Portland, Oregon
San Francisco, California
Los Angeles, California
San Diego, California
Dallas, Texas
Chicago, Illinois
Atlanta, Georgia
Washington, DC
Baltimore, Maryland
Boston, Massachusetts
Philadelphia, Pennsylvania
Jersey City, New Jersey
New York, New York

Participating agencies determine their individual capacity based on the number of officers they can afford to dedicate to the canine program. The National Explosives Detection Canine Teams Program makes every effort to provide state and local mass transit systems with the resources they request.

Question: The 9/11 Commission Act encourages TSA to develop a certification program for non-TSA explosive dogs that are used by transit agencies. Did this occur?

ANSWER: Although the Transportation Security Administration (TSA) has not developed a formal certification training program, each team does receive TSA-approved standardized National Explosives Detection Canine Teams Program training on a recurring basis. TSA plans to pursue the development of a certification program in the near future.

Toxic Inhalation Hazard

Question: Toxic inhalation hazard materials have been identified as high risk because, in contrast to normal hazmat, an accident of intentional airborne release has the potential to harm widespread populations. In November 2006, the Secretary set a goal to reduce the risk posed by transporting TIH by rail in high threat urban areas by 50 percent in 2008. Was this goal met?

ANSWER: Yes. For the calendar year 2008, the cumulative national risk score for freight railroad carriers transporting Toxic Inhalation Hazard (TIH) revealed that the risk associated with the transportation by rail of large amounts of TIH for the year had been reduced by 59 percent.

Question: Has the TIH regulation been finalized? If so, please summarize for the Committee what measures railroads will take to enhance the control and chain of custody for TIH products as well as impose fines for noncompliance.

ANSWER: Yes, 49 CFR Part 1580, entitled "Rail Transportation Security," was published in the Federal Register on November 26, 2008, and, with the exception of one provision, became effective December 26, 2008. See 73 FR 72130. The effective date of 49 CFR 1580.107, which requires a secure chain of physical custody for rail cars containing one or more security-sensitive materials, was extended until April 1, 2009. This extension was to allow additional time for affected freight railroad carriers, rail hazardous materials

shippers, and rail hazardous materials receivers to conduct training and to implement Chain of Custody and Control (COCC) procedures. Those COCC procedures will enhance Toxic Inhalation Hazard (TIH) security by requiring that the shipper keep the loaded TIH rail cars in a rail secure area from the time of inspection until the rail cars are transferred to the freight railroad carrier. In addition, TIH rail cars must be attended when they are transferred from one carrier to another carrier if the rail cars are in or may subsequently enter a high threat urban area (HTUA), and attended when the rail cars are delivered to a receiver located in a HTUA. The freight railroad carrier must perform a security inspection of the rail car when it receives the car from the shipper or in interchange from another carrier, and must document each transfer of physical custody. 49 CFR 1580.103, entitled "Location and Shipping Information for Certain Railcars," requires freight railroad carriers to be able to determine the location and shipping information of each TIH rail car, as well as rail cars containing other rail security-sensitive materials, and report the information to the Transportation Security Administration (TSA) upon request. TSA will utilize Surface Transportation Inspectors to conduct compliance inspections across the freight rail network to determine compliance with all Part 1580 requirements. The Department of Homeland Security/TSA may impose a civil penalty of not more than \$10,000 on any covered person who violates any regulation prescribed in 49 C.F.R. part 1580.

Research Programs Related to Surface Transportation Security

Question: Please highlight for the Committee what research and development activities TSA is doing in coordination with the Science and Technology Directorate that may have an impact on security in the passenger rail and mass transit environment. For example, do you have any ongoing projects that look at random security screening of passengers in rail and mass transit systems? If so, what are they? Similarly, do you have any projects that look at how to better read tickets for explosives?

ANSWER: The Transportation Security Administration (TSA) has several applicable ongoing projects in conjunction with the Department of Homeland Security Science and Technology Directorate (DHS/S&T). In addition to DHS/S&T, TSA has interagency agreements with the Federal Railroad Administration (FRA), Technical Support Working Group, and Volpe Transportation Center for ongoing projects. These activities include:

Railcar Vulnerability Testing – to evaluate and test rail car vulnerabilities to potential terrorist attacks. TSA is working with FRA and the Transportation Technology Center, Inc. on this effort. The project involves modeling the potential results and confirming those results through full-scale testing.

Resilient Tunnel – to research possible technologies for use in reducing the potential vulnerability of transportation tunnels to catastrophic flooding as a result of a terrorist attack. In addition to this effort, TSA, DHS/S&T, and Lawrence Livermore National Laboratory are currently partnering with a major transit agency to model a mitigation solution to protect a vulnerable ventilation structure from terrorist attack.

Robot/Robocart Testing -- to investigate the feasibility and suitability for using robots and robocart to assist first responders in the event of an incident in rail and transit tunnels. Robocart is a small, portable, easily assembled, remotely-controlled, proof-of-concept vehicle that is designed to ride the rails to quickly deliver robots to the scene of an incident in a railway tunnel. Efforts are currently underway to make improvements to Robocart and it will be tested as part of a full-scale exercise in fiscal year (FY) 2009.

Video Indexing and Extraction -- to examine the integration of existing closed circuit television cameras and feeds with video storage, software for analysis, searchable databases, and wireless video transport to Personal Digital Assistant (PDAs).

Low Cost, Blast Resistant Cameras -- to develop and field test low-cost, blast resistant closed circuit television cameras for use in mass transit and passenger rail. DHS/S&T has conducted a blast analysis of these cameras and determined they are suitable for a full operational test. TSA is assisting S&T in the execution of the field tests.

Secure Bus -- to demonstrate the suitability of systems to provide driver authentication and safe and predictable remote disabling of transit buses. TSA, through an interagency agreement with the Department of Transportation's Volpe Transportation Center, recently completed a successful field test of this system conducted with San Diego Metropolitan Transit System (SDMTS). The final report on this project is being reviewed by TSA before publication. This technology will be included on the Authorized Equipment List for the Transit Security Grant Program in future grant cycles, and future iterations of this project may include evaluation of this and other security technologies for transit buses to be integrated with original equipment manufacturers.

Human Activity Monitoring for Mass Transit and Passenger Rail -- to develop an advance video content analysis program for use in high volume transit and passenger rail stations. This is an ongoing project, in conjunction with the Technical Support Working Group. The goal of the system is to permit a greater number of algorithms to run concurrently and reduce the impact of common causes of false positives. The small scale testing of this system has occurred on Minneapolis' Metro Transit Light Rail. The large scale testing will be at Amtrak's 30th Street Station in Philadelphia.

Anomaly Detection for Mass Transit -- to evaluate the suitability of the system for sustained use in the mass transit environment and determine the most effective operational use for screening passengers for anomalous objects carried on the body. TSA will begin a field test of a portable anomaly detector in a variety of transit systems throughout the country.

The Transportation Security Administration (TSA) and the Department of Homeland Security Science and Technology Directorate have both evaluated and field tested technologies to detect explosives traces on passenger tickets using document scanners and in-ticket dispensing machines. TSA does not have any ongoing projects in this area.

Management

Question: Please list all TSA political employees who received bonuses in 2008. Include the position, office, and bonus amount.

ANSWER: None of the Transportation Security Administration's political employees received a bonus in 2008.

Question: Please list all TSA SES bonuses provided in 2008 by position, office, and bonus amount.

ANSWER: Please see the chart below.

Office	Position Title	2008 Performance Bonus (\$)
ACQ	Executive Director, Prog Analysis, Office of Acquisitions	\$ 15,210
ACQ	Asst. Administrator for Acquisitions/CAO	\$ 20,097
ACQ	Deputy Assistant Administrator for Acquisitions	\$ 15,255
FAMS	FAMS - Special Agent-in-Charge, Miami Field Office	\$ 15,702

FAMS	FAMS - Asst. Administrator for Law Enforcement/FAMS	\$ 25,650
FAMS	FAMS - Deputy Assistant Administrator for Law Enforcement	\$ 20,160
FAMS	Assistant Director, Office of Admin. & Technical Services	\$ 9,547
FAMS	FAMS - Dep Asst Dir for Workforce Planning & Mgmt.	\$ 9,120
FAMS	FAMS - Special Agent-in-Charge, Atlanta Field Office	\$ 15,400
FAMS	FAMS - Deputy Assistant Director, Office of Field Operations (Reston, VA)	\$ 9,240
FAMS	FAMS - Special Agent-in-Charge, Washington Field Office	\$ 15,100
FAMS	FAMS - Special Agent-in-Charge, Chicago Field Office	\$ 9,064
FAMS	FAMS - Special Agent-in-Charge, Los Angeles Field Office	\$ 9,000
FAMS	FAMS - Special Agent-in-Charge, Newark Field Office	\$ 9,043
FAMS	FAMS - Plans Officer	\$ 9,416
FAMS	Assistant Director, Office of Flight Operations (Reston VA)	\$ 19,800
FAMS	Assistant Director, Office of Personnel & Training	\$ 9,795
FAMS	FAMS - Special Agent-in-Charge, Houston Field Office	\$ 9,077
FAMS	FAMS - Special Agent-in-Charge, Dallas Field Office	\$ 15,400
FAMS	FAMS - Special Agent-in-Charge, Orlando Field Office	\$ 14,941
FAMS	FAMS - Dep Assistant Dir, Office of Sec Svcs and Assessment	\$ 8,820
FAMS	FAMS - Asst. Director, Office of Flight Operations	\$ 16,000
FIN	Director, Financial Management Fin and Administration	\$ 15,210
FIN	Director, Budget & Performance	\$ 16,035
FIN	Assistant Administrator for Finance and Administration	\$ 30,240
FIN	Chief, Administrative Officer, Office of Finance & Admin	\$ 16,500
GS	Assistant Administrator for Global Strategies	\$ 13,440
HC	Deputy Asst. Administrator for Human Capital	\$ 16,200
INSP	Assistant Administrator for Inspections	\$ 16,800
INSP	Deputy Assistant Administrator Inspections	\$ 7,624
INTEL	Deputy Assistant Administrator for Intelligence and Analysis	\$ 25,200
INTEL	Deputy Asst. Administrator for Intelligence	\$ 16,800
OCC	Deputy Chief Counsel	\$ 21,000
OCC	Deputy Chief Counsel	\$ 10,000
OCC	Supervising Attorney Advisor	\$ 18,000
OCC	Chief Counsel	\$ 23,000
OCC	Deputy Chief Counsel	\$ 16,000
OCC	Deputy Chief Counsel	\$ 19,000
OCC	Deputy Chief Counsel	\$ 16,000
OSC	Special Counselor	\$ 14,787
OSO	DFSD, Cat X (Los Angeles International Airport)	\$ 9,126
OSO	Federal Security Director (FSD) Cat 1 (San Diego International Airport)	\$ 15,366
OSO	SFE, Western Region	\$ 7,757
OSO	FSD Cat X (Dallas Ft Worth International Airport) (EOD: 09/02/07)	\$ 14,250
OSO	FSD Cat X (Detroit Metro Wayne County Airport)	\$ 18,860
OSO	FSD Cat X (Luis Munoz Marin International Airport, PR)	\$ 14,086
OSO	FSD Cat X (Denver International Airport)	\$ 15,210
OSO	SFE, Central Area	\$ 16,085
OSO	FSD - Cat X (Charlotte/Douglas Airport)	\$ 11,424
OSO	FSD Cat X (Reagan National Airport Arlington VA)	\$ 15,765
OSO	FSD Cat 1 (Anchorage, AK)	\$ 9,420
OSO	GM, Field Operations, Off of Sec Ops	\$ 9,491
OSO	DFSD Cat X (Detroit Metro Wayne County Airport)	\$ 7,573

OSO	FSD - Cat X (Los Angeles International Airport)	\$ 19,680
-----	---	-----------

Office	Position Title	2008 Performance Bonus (\$)
OSO	DFSD- Cat X (O'Hare International Airport)	\$ 10,647
OSO	SFE (JFK, NY NY)	\$ 11,200
OSO	FSD - Cat X (Seattle-Tacoma Internat'l Airport)	\$ 7,300
OSO	FSD - Cat X (Miami International Airport NJ)	\$ 9,300
OSO	Area Director, Eastern Area, Off of Sec Ops	\$ 7,900
OSO	General Manager, Airports	\$ 14,476
OSO	Deputy Asst. Administrator for Office of Security Operations	\$ 16,200
OSO	FSD - Cat 1 (Portland International Airport, OR)	\$ 9,526
OSO	DFSD - Cat X (Washington-Dulles International Airport)	\$ 8,688
OSO	FSD - Cat X (Orlando International Airport FL)	\$ 25,116
OSO	FSD - Cat X (Honolulu International Airport) (EOD: 08/19/07)	\$ 10,382
OSO	FSD - Cat X (Minneapolis/St Paul, MN)	\$ 15,876
OSO	FSD - Cat X (Washington-Dulles International Airport, VA)	\$ 9,042
OSO	FSD - Cat X (George Bush International Airport TX)	\$ 8,945
OSO	FSD - Cat X (Tampa International Airport)	\$ 9,092
OSO	Assistant General Manager, Screening, Off of Sec Ops	\$ 8,208
OSO	FSD - Cat 1 (Salt Lake City International Airport)	\$ 15,635
OSO	FSD - Cat X (JFK International Airport)	\$ 7,605
OSO	FSD - Cat X (Logan International Airport)	\$ 9,526
OSO	FSD - Cat X (O'Hare International Airport, Chicago IL)	\$ 7,485
OSO	FSD - Cat X (Newark International Airport)	\$ 9,000
OSO	FSD - Cat X (McCarran International Airport)	\$ 18,976
OSO	Senior International Advisor (London, England)	\$ 16,085
OSO	DFSD - Cat X (Orlando International Airport)	\$ 8,839
OSO	FSD - Cat X (Baltimore-Washington International Airport)	\$ 15,808
OSO	FSD - Cat 1 (Austin - Bergstrom International Airport)	\$ 10,084
OSO	SFE, Eastern Area (Tampa, FL)	\$ 11,185
OSO	FSD - Cat X (Lambert St. Louis International Airport)	\$ 9,212
OSO	DFSD - Cat X (Regan National Airport)	\$ 9,126
OSO	FSD - Cat 1 (San Antonio International Airport)	\$ 9,373
OSO	SFE, Office of Security Oerations	\$ 16,605
OSO	SFE - Western Area (John Wayne Airport)	\$ 15,798
OSO	FSD - Cat X (Cincinnati/Northern Kentucky International Airport)	\$ 10,450
OSO	DFSD - Cat X (Miami International Airport)	\$ 7,311
TSNM	General Manager, Highway & Motor Carrier	\$ 7,623
TSNM	General Manager (GM), Pipeline	\$ 8,672
TSNM	GM, Rail	\$ 8,504
TSNM	GM, Mass Transit	\$ 7,375
TSNM	GM, General Aviation	\$ 14,180
TSNM	GM, Transportation Sector Network Integration	\$ 8,460
TSNM	Assistant Administrator	\$ 18,810
TSNM	GM International	\$ 8,970
TTAC	Assistant Administrator for Transportation Threat Assessment and Credentialing	\$ 16,764
	Executive Advisor (Transition)	\$ 17,100

	Deputy Administrator, TSA	\$	34,440
--	---------------------------	----	--------

Question: Please list by office and pay grade level the number of non-SES employees who received a bonus in 2008, the total bonus for the particular office and pay grade, and the total number of employees in the office and pay grade.

ANSWER: Please see the two charts that follow.

Calendar Year 2008 Non-TSES Awards

Key Org	Payband	B	C	D	E	F	G	H	I	J	K	L	TOTALS
Acquisition	Number of Employees	1	2	2	4	6	24	27	17	26	14		123
	Value of Cash Awards		\$1,900	\$2,036	\$3,075	\$6,625	\$10,281	\$69,465	\$63,475	\$52,372	\$68,000		\$2,772,249
Administrator's Office	Number of Cash Awards				1	3	1	1	3	1	1		7
	Value of Cash Awards			\$1,500			\$4,000	\$1,500	\$7,250		\$3,500		\$17,750
Business Transformation & Culture	Number of Cash Awards					1		1	1	3	12	1	19
	Value of Cash Awards					\$2,500		\$750	\$3,000	\$7,500	\$34,949	\$8,000	\$56,699
Chief Counsel	Number of Cash Awards			3		6	9	6	13	31	108	44	220
	Value of Cash Awards			\$2,000		\$3,700	\$4,350	\$4,800	\$7,900	\$24,250	\$103,300	\$63,850	\$214,150
Finance & Administration	Number of Cash Awards					16	29	38	53	113	47	3	299
	Value of Cash Awards					\$5,512	\$18,180	\$25,565	\$43,154	\$97,368	\$69,789	\$4,600	\$264,168
Global Strategies	Number of Cash Awards					3	2	6	44	50	72		177
	Value of Cash Awards					\$4,750	\$2,850	\$8,750	\$60,450	\$70,750	\$116,750		\$364,300
Human Capital	Number of Cash Awards					6	9	18	41	82	64	9	229
	Value of Cash Awards					\$3,356	\$6,648	\$12,533	\$35,394	\$95,579	\$113,560	\$40,176	\$307,246
Inspections	Number of Cash Awards					3	9	5	7	97	45	1	160
	Value of Cash Awards					\$3,400	\$3,150	\$3,150	\$5,200	\$102,615	\$91,350	\$3,500	\$209,215
Intelligence	Number of Cash Awards						8	20	15	36	17	2	78
	Value of Cash Awards						\$8,913	\$20,714	\$20,714	\$65,740	\$42,648	\$8,000	\$146,015
Law Enforcement	Number of Cash Awards					1	4	25	51	139	167	30	2,995
	Value of Cash Awards					\$250	\$1,765	\$13,306	\$35,697	\$106,754	\$321,783	\$79,913	\$2,832,431

Calendar Year 2005 Non-TSES Awards

Key Org	Payband	B	C	D	E	F	G	H	I	J	K	L	TOTALS
Legislative Affairs	Number of Cash Awards						1	3	6	6	2		18
	Number of Employees						1	1	4	1	1		7
	Value of Cash Awards						\$2,500	\$6,000	\$16,000	\$24,000	\$6,000		\$54,500
Operational Process & Technology	Number of Cash Awards				3	2	4	15	17	124	107	18	290
	Number of Employees				1	3	1	13	7	78	52	7	161
	Value of Cash Awards				\$1,821	\$2,500	\$5,800	\$14,983	\$16,483	\$157,823	\$209,860	\$43,000	\$452,270
Security Operations	Number of Cash Awards		14	19,180	78,800	34,517	24,878	4,249	3,668	1,124	569	7	167,015
	Number of Employees		16	18,414	19,266	7,535	5,624	1,674	1,501	623	317	5	54,997
	Value of Cash Awards		\$1,039	\$11,772,270	\$60,704,215	\$28,745,648	\$20,312,048	\$4,277,563	\$4,508,963	\$1,766,890	\$1,280,611	\$19,100	\$134,388,347
Security Technology	Number of Cash Awards									0	3		12
	Number of Employees									4	27		77
	Value of Cash Awards									\$12,300	\$4,750		\$17,050
Special Counselor	Number of Cash Awards			1	3	7	12	24	33	53	24	1	158
	Number of Employees			1	4	5	9	10	23	23	20	2	97
	Value of Cash Awards			\$500	\$1,250	\$4,350	\$7,341	\$12,432	\$21,140	\$47,640	\$16,449	\$4,000	\$135,103
Strategic Communications & Public Affairs	Number of Cash Awards						3	2	8	18	8		42
	Number of Employees						2	2	4	14	3		31
	Value of Cash Awards						\$7,000	\$6,383	\$3,500	\$12,483	\$40,649	\$22,250	\$93,265
Transportation Sector Network Management	Number of Cash Awards				2	7	29	33	54	138	135	4	408
	Number of Employees				2	8	11	17	25	75	61	2	204
	Value of Cash Awards				\$4,133	\$4,883	\$10,460	\$30,216	\$57,863	\$159,638	\$250,269	\$10,000	\$548,191
Threat Assessment & Credentialing	Number of Cash Awards						4	25	24	59	55	10	211
	Number of Employees						4	21	24	40	38	5	139
	Value of Cash Awards						\$6,600	\$9,150	\$38,208	\$38,604	\$151,879	\$43,600	\$396,335
Number of Cash Awards		3	17	19,190	78,851	34,707	24,065	4,600	6,066	2,382	1,450	130	172,461
	Number of Employees	3	24	18,438	19,307	7,714	6,130	2,176	5,118	1,705	956	92	61,655
	Value of Cash Awards	\$ 600	\$ 3,189	\$ 12,778,391	\$ 60,729,300	\$ 28,892,097	\$ 20,459,087	\$ 4,615,191	\$ 6,631,635	\$ 3,309,157	\$ 2,927,697	\$ 327,739	\$ 140,674,283

Amounts highlighted under Security Operations include Performance Accountability Standards System (PASS) Bonuses

Question: Please provide for the record a table that shows all funds expended by TSA political employees for travel in 2008. Include name of individual traveling, purpose of travel, location(s) visited, and total cost.

ANSWER: Please see the charts that follow.

Traveler Name	Purpose of Travel	Location visited	Trip Cost
Edmund Hawley	CONFERENCE ATTENDANCE	MONTERREY, CA	1,621.76
	CONFERENCE ATTENDANCE	BRUSSELS, BEL	3,178.61
	SITE VISIT	HOUSTON, TX	990.01
	CONFERENCE ATTENDANCE	SALT LAKE CITY, UT; DENVER, CO	1,803.39
	CONFERENCE ATTENDANCE	NEW YORK, NY	466.63
	CONFERENCE ATTENDANCE	OTTAWA, CAN	1,214.79
	CONFERENCE ATTENDANCE	ST LOUIS, MO	717.88
	CONFERENCE ATTENDANCE	BRUSSELS, BEL; PARIS, FRA	3,040.02
	CONFERENCE ATTENDANCE	DALLAX, TX; SAN ANTONIO, NM	971.17
	CONFERENCE ATTENDANCE	LONDON, ENG; GLASGOW, SCO	3,693.76
	CONFERENCE ATTENDANCE	ATLANTA, GA	600.38
	CONFERENCE ATTENDANCE	AMMAN, JOR; BERLIN, FRG; ROME, ITA; TEL AVIV, ISR; VIENNA, AUT; WARSAW, POL	9,110.89
	CONFERENCE ATTENDANCE	BOSTON, MA; DENVER, CO; SEATTLE, WA	2,344.75
	CONFERENCE ATTENDANCE	ST. LOUIS, MO	976.88
	CONFERENCE ATTENDANCE	OTTAWA, CAN; NEW YORK, NY; PITTSBURGH, PA	3,054.20
	CONFERENCE ATTENDANCE	BALTIMORE, MD; PHILADELPHIA, PA	703.13
	CONFERENCE ATTENDANCE	LOS ANGELES, CA; SAN FRANCISCO, CA	1,942.75
	OFF-SITE	CAMBRIDGE, MD	567.09
	CONFERENCE ATTENDANCE	ORLANDO, FL	389.00
	CONFERENCE ATTENDANCE	SAN FRANCISCO, CA; NEW YORK, NY	2,345.86
	TOTAL	39,732.95	

Traveler Name	Purpose of Travel	Location visited	Trip Cost
Ellen Howe	SITE VISIT	DALLAS, TX	3,196.78
	SITE VISIT	SAN ANTONIO, TX	1,598.39
	SITE VISIT	SAN FRANCISCO, CA	1,507.43
	INFORMATION MEETING	MANHATTAN, NY	1,300.13
	TRAINING	MANHATTAN, NY	760.00
	SPEECH OR PRESENTATION	MANHATTAN, NY	694.99
	SITE VISIT	BOSTON, MA	653.63
	CONFERENCE ATTENDANCE	OTTAWA, CAN	1,799.97
	INTERNATIONAL TRAVEL	LONDON,GBR	3,931.39
	SITE VISIT	MANHATTAN, NY	390.63
	SPEECH OR PRESENTATION	NEW ORLEANS, LA	1,143.70
	SPEECH OR PRESENTATION	MANHATTAN, NY	701.68
	SPECIAL MISSION TRAVEL	CHICAGO, IL; DENVER, CO; SEATTLE, WA	2,039.65
	SPEECH OR PRESENTATION	MANHATTAN, NY	539.91
		TOTAL	20,258.28
Rebekah Williams	CONFERENCE ATTENDANCE	LONDON, ENG; GLASGOW, SCO	5,188.11
	CONFERENCE ATTENDANCE	PHOENIX, AZ	761.50
	CONFERENCE ATTENDANCE	BIRMINGHAM, AL	770.54
	CONFERENCE ATTENDANCE	BRUSSELS, BEL	3,333.26
	CONFERENCE ATTENDANCE	BRUSSELS, BEL; PARIS, FRA	2,876.24
	CONFERENCE ATTENDANCE	CHARLSTON, SC	1,174.03
	CONFERENCE ATTENDANCE	AMMAN, JOR; BERLIN, FRG; ROME, ITA; TEL AVIV, ISR; VIENNA, AUT; WARSAW, POL	8,825.97
	CONFERENCE ATTENDANCE	LONDON, ENG; GLASGOW, SCO	5,174.11
	OFF-SITE	CAMBRIDGE, MD	436.54
	CONFERENCE ATTENDANCE	OTTAWA, CAN	1,199.29
	CONFERENCE ATTENDANCE	SAN FRANCISCO, CA	2,578.87
	CONFERENCE ATTENDANCE	SALT LAKE CITY, UT; DENVER, CO	2,199.44
	CONFERENCE ATTENDANCE	TEL AVIV, ISR	3,574.90
	CONFERENCE ATTENDANCE	MANHATTAN, NY	1,379.30
	CONFERENCE ATTENDANCE	MEMPHIS, TN	296.55
	CONFERENCE ATTENDANCE	DALLAS, TX	987.58
		TOTAL	40,756.23

Question: Please list the number, by office and pay grade level, of all TSA employees hired non-competitively in fiscal year 2008.

ANSWER: Please see the chart below.

Fiscal Year 2008 Non-Competitive Appointments

Key Org	B	C	D	E	F	G	H	I	J	K	L	TSES	TOTALS
Acquisition	2	2	1	1	3		1	1	4				15
Administrator's Office		1			2				1				4
Business Transformation & Culture					1		1			1			3
Chief Counsel	1		6		1	1							9
Finance & Administration					3	1	1						5
Global Strategies												1	1
Human Capital				1	2	1		1	1				6
Inspections			1					1	1				3
Intelligence						6	2	2	5	1		1	17
Law Enforcement	2	9	1		3	5	1		1				22
Operational Process & Technology	2	1			1				2			1	7
Security Operations			1	1		1	2	8	6	2		1	22
Special Counselor			1	1	1	1		1	1				6
Strategic Communications & Public Affairs								1	2		1		4
Transportation Sector Network Management	5	2			1	2				5		1	16
Transportation Threat Assessment & Credentialing					2	1	1	1	4	1			10
TOTALS	12	15	11	4	20	19	9	16	28	10	1	5	150

These numbers are drawn from personnel transactions recorded against the nature of action code 171. Transactions against this code are for excepted appointment not-to-exceed positions. These positions are term-limited appointments and generally cover non-competitive appointments within TSA.

Contracts

Question: Update and submit, through the most recent month available, the list provided in last year's hearing record (2009, Part 2, pages 469-507) regarding Sole Source Contracts. Organize by contractor, purpose, appropriation account, dollar award, full performance value, contract start date, contract end date, and reason for sole-source.

ANSWER: The chart that follows provides information regarding Sole Source Contracts as of March 24, 2009.

Vendor Name	Description of Requirement	Action Obligation	Base and All Options Value	Date Signed	Completion Date	Reason Not Completed
SCIENCE APPLICATIONS INTERNATIONAL CORPORATION	FAMS OPERATIONS SUPPORT	\$4,053,877.00	\$4,053,877.00	12/26/06	3/31/07	URGENCY
SCIENCE APPLICATIONS INTERNATIONAL CORPORATION	FAMS OPERATIONS SUPPORT	\$1,400,000.00	\$1,400,000.00	3/28/07	6/30/07	URGENCY
SCIENCE APPLICATIONS INTERNATIONAL CORPORATION	FAMS OPERATIONS SUPPORT	\$1,350,000.00	\$1,350,000.00	4/6/07	6/30/07	URGENCY
SCIENCE APPLICATIONS INTERNATIONAL CORPORATION	FAMS OPERATIONS SUPPORT	\$2,239,217.00	\$2,239,217.00	6/15/07	12/31/07	URGENCY

SCIENCE APPLICATIONS INTERNATIONAL CORPORATION	FAMS OPERATIONS SUPPORT	\$945,529.00	\$945,529.00	8/1/07	12/31/07	URGENCY
Broward County	NEDCTP Activities for the 4th Qtr of FY07 to include requirements as outlined within the existing CA and all previously signed modification.	\$135,838.81	\$135,838.81	4/23/07	1/0/00	ONLY ONE SOURCE - OTHER
CrossMatch Technologies	One year enhanced warranty for ID 1000 system and 24X7 helpdesk as well as SW Engineering hours and funds for travel	\$266,000.00	\$266,000.00	3/7/07	4/13/08	UNIQUE SOURCE
Computer Sciences Corporation	Bridge contract to continue the Financial Systems Support Services (FSSS) pending award of a new contract.	\$423,269.00	\$423,269.00	12/21/07	2/29/08	ONLY ONE SOURCE - OTHER
SABRE INCORPORATED	SABRE AIRCREWS/ QIK APPLICATIONS & ILOG CPLEX LICENSES AND MAINTENANCE FOR MISSION SCHEDULER, MANUAL PR 05-FAM-0036 MOD 1,	\$133,540.00	\$133,540.00	12/27/06	12/31/07	ONLY ONE SOURCE - OTHER
DATAMAXX APPLIED TECHNOLOGIES INCORPORATED	LABOR AND TRAVEL	\$554,751.78	\$554,751.78	5/10/07	9/30/07	ONLY ONE SOURCE - OTHER
DATAMAXX GROUP INCORPORATED	DATAMAXX, INC. DELIVERY ORDER 8	\$2,191,604.40	\$2,191,604.40	1/3/07	9/30/07	ONLY ONE SOURCE - OTHER
MISCELLANEOUS FOREIGN CONTRACTORS	THIS PR WAS ESTABLISHED FOR THE FAMS TO TSA UDO CONVERSION FOR AWARD NUMBER: HSCEAM06P0065 FPD DOCUMENT: 2406HSAMP0065	\$4,800.00	\$4,800.00	11/18/06	12/31/06	ONLY ONE SOURCE - OTHER
COVENANT AVIATION SECURITY LIMITED LIABILITY COMPANY	A.P. SECURITY SCREENING SERVICES	\$7,220,984.00	\$167,587,320.00	11/20/06	10/31/06	ONLY ONE SOURCE - OTHER
PERFORMANCE ASSESSMENT NETWORK INCORPORATED	FFDO TRAINING PROGRAM	\$1,172,877.00	\$1,172,877.00	5/24/07	5/31/07	ONLY ONE SOURCE - OTHER
Dun and Bradstreet, Inc.	PR provides funding to support Dun & Bradstreet services for Air Cargo's Indirect Air Carrier Management System, Known Shipper Management System and the Freight Assessment Systems.	\$4,500,000.00	\$27,631,944.31	5/15/07	5/15/12	ONLY ONE SOURCE - OTHER
AMERICAN ASSOCIATION OF COMMUNITY COLLEGES	CREW MEMBER SELF-DEFENSE TRAINING PROGRAM	\$2,620,000.00	\$2,620,000.00	9/10/07	11/30/07	AUTHORIZED BY STATUTE
SABRE INCORPORATED (9502)	PMO SERVICE	\$372,000.00	\$372,000.00	5/11/07	5/10/08	FOLLOW-ON CONTRACT
SABRE INCORPORATED (9502)	PMO SERVICE	\$344,000.00	\$344,000.00	6/12/07	5/10/08	FOLLOW-ON CONTRACT
SABRE INCORPORATED (9502)	PMO SERVICE	\$283,400.00	\$283,400.00	8/16/07	5/10/08	FOLLOW-ON CONTRACT
SABRE INCORPORATED (9502)	PMO SERVICE	\$168,216.00	\$168,216.00	8/31/07	5/10/08	FOLLOW-ON CONTRACT

AOC SOLUTIONS INCORPORATED	NON-COMPETITIVE PROCUREMENT OF ACCOUNTING, STANDARD GENERAL LEDGER, BUDGETARY, AND FINANCIAL SYSTEMS SUPPORT SERVICES.	\$165,000.00	\$165,000.00	11/22/06		ONLY ONE SOURCE - OTHER
AOC SOLUTIONS INCORPORATED	NON-COMPETITIVE PROCUREMENT OF ACCOUNTING, STANDARD GENERAL LEDGER, BUDGETARY, AND FINANCIAL SYSTEMS SUPPORT SERVICES. PR IS BASED ON GOVERNMENT COST ESTIMATE	\$ 65,000.00	\$ 65,000.00	1/3/07		ONLY ONE SOURCE - OTHER
AOC SOLUTIONS INCORPORATED	NON-COMPETITIVE PROCUREMENT OF ACCOUNTING, STANDARD GENERAL LEDGER, BUDGETARY, AND FINANCIAL SYSTEMS SUPPORT SERVICES. PR IS BASED ON GOVERNMENT COST ESTIMATE.	\$ 71,200.00	\$ 71,200.00	2/13/07		ONLY ONE SOURCE - OTHER
AMERICAN ASSOCIATION OF AIRPORT EXECUTIVES	FINGERPRINTING SUPPORT - FUNDS FOR CONTRACTOR TO PROVIDE A CLEARINGHOUSE FOR FINGERPRINT AND DIGITAL PHOTO FILES FOR PROSPECTIVE TRANSPORTATION SECURITY OFFICER (TSO) CANDIDATES.	\$ 56,650.00	\$ 86,647.00	5/22/07	9/10/10	AUTHORIZED BY STATUTE
AMERICAN ASSOCIATION OF AIRPORT EXECUTIVES	FINGERPRINTING SUPPORT - FUNDS FOR CONTRACTOR TO PROVIDE A CLEARINGHOUSE FOR FINGERPRINT AND DIGITAL PHOTO FILES FOR PROSPECTIVE TRANSPORTATION SECURITY OFFICER (TSO) CANDIDATES.	\$677,350.00	\$677,350.00	7/3/07	9/10/10	AUTHORIZED BY STATUTE
THE CORPORATE EXECUTIVE BOARD COMPANY	MEMBERSHIP FEE	\$ 57,500.00	\$ 57,500.00	6/25/07	6/29/08	UNIQUE SOURCE
ONYX OF ALEXANDRIA INCORPORATED	SAFETY INFORMATION SYSTEM (SIS) MODIFICATION TO DESIGN, DEVELOP, IMPLEMENT AN INTEGRATED CASE MANAGEMENT MODULE TO THE EXISTING SIS PLATFORM.	\$1,211,537.22	\$1,211,537.22	9/21/07	9/23/08	ONLY ONE SOURCE - OTHER
Desyne Web Services	New contract for one year and a possible six month extension while new system is built. New contract will combine this PR for Application Maintenance at \$148,750 as well as Application Hosting under PR 2107207CMO006 for \$96,000.	\$244,750.00	\$244,750.00	9/28/07	1/0/00	UNIQUE SOURCE

GRA, Inc.	This procurement request is to increase the quantity of hours/funding against CLIN 0007 - Training; include an addendum to the SOW; establish and fund (\$100,000) a new CLIN 0009 - Other Direct Costs; incorporate three clauses (Limitation of Cost, Allowable Cost and Payment, and Limitation of Funds); Change the COTR from Julie Perry to Valarie Ramos; Change the CO from Charles Eppright to Brenda Samuels; and include an updated copy of Schedule B to reflect these changes.	\$172,136.00	\$-	3/7/07	9/7/07	ONLY ONE SOURCE - OTHER
THE EKMAN GROUP TRAINING DIVISION	THE PURPOSE OF THIS PROCUREMENT IS TO OBTAIN SERVICES TO PROVIDE A TWO DAY TRAINING COURSE ENTITLED "EVALUATING TRUTHFULNESS AND DETECTING DECEPTION". IT CONSISTS OF VERBAL, NON-VERBAL, FACIAL EXPRESSIONS, VOICE PITCH, CRITERIA-BASED CONTENT ANALYSIS (CBCA), STATEMENT ANALYSIS AND MEMORY RECALL AS IT RELATES TO DECEPTION OR TRUTHFULNESS.	\$990,900.00	\$990,900.00	7/13/07	8/18/07	UNIQUE SOURCE
THE EKMAN GROUP TRAINING DIVISION	THE PURPOSE OF THIS PROCUREMENT IS TO OBTAIN SERVICES TO PROVIDE A TWO DAY TRAINING COURSE ENTITLED "EVALUATING TRUTHFULNESS AND DETECTING DECEPTION". IT CONSISTS OF VERBAL, NON-VERBAL, FACIAL EXPRESSIONS, VOICE PITCH, CRITERIA-BASED CONTENT ANALYSIS (CBCA), STATEMENT ANALYSIS AND MEMORY RECALL AS IT RELATES TO DECEPTION OR TRUTHFULNESS.	\$ 54,000.00	\$ 54,000.00	7/24/07	8/18/07	UNIQUE SOURCE
CORT BUSINESS SERVICES CORPORATION	FUNDING FOR FY07 CORT RENTAL FURNITURE AT VARIOUS AIRPORT LOCATIONS.	\$2,563,168.81	\$2,563,168.81	12/29/06	1/28/07	FOLLOW-ON CONTRACT
CORT BUSINESS SERVICES CORPORATION	FUNDING FOR FY07 CORT RENTAL FURNITURE AT VARIOUS AIRPORT LOCATIONS.	\$ 71,000.00	\$ 71,000.00	8/16/07	6/27/08	FOLLOW-ON CONTRACT
TOXCO INCORPORATED	PURCHASE OF BATTERY RECYCLING MAIL BACK CONTAINERS FOR MULTIPLE DELIVERY ADDRESSES.	\$5,696.00	\$-	3/14/07	6/14/10	SIMPLIFIED ACQUISITION PROCEDURE - NON-COMPETITIVE
JFK INTERNATIONAL AIR TERMINAL LIMITED LIABILITY COMPANY	LEASE OF SPACE FOR TSA USE IN TERMINAL 4, JOHN F KENNEDY INTERNATIONAL AIRPORT	\$ 64,484.00	\$ 64,484.00	9/26/07	9/26/07	AUTHORIZED BY STATUTE
JFK INTERNATIONAL AIR TERMINAL LIMITED LIABILITY COMPANY	LEASE OF SPACE FOR TSA USE IN TERMINAL 4, JOHN F KENNEDY INTERNATIONAL AIRPORT	\$2,268.90	\$2,268.90	9/27/07	9/30/12	AUTHORIZED BY STATUTE

BRITISH AIRWAYS PLC	LEASE AGREEMENT, INCLUDING CONSTRUCTION FUNDING, FOR TSA OCCUPIED SPACE AT BRITISH AIRWAYS TERMINAL 7, JFK INTERNATIONAL AIRPORT	\$190,178.14	\$190,178.14	9/21/07	9/21/07	ONLY ONE SOURCE - OTHER
FLORIDA INSTITUTE OF TECHNOLOGY	DHS PROGRAM MANAGEMENT TOOLS (DHS PMT 250), OCTOBER 2006. 40-HOUR COURSE COVERS SEVEN BASIC TOOLS INCLUDED IN THE DAU VERSION OF PMT250. TOPICS TO BE PRESENTED ARE: 1. SYSTEM MANGEMENT CONTEXT; 2. INTEGRATED PRODUCT AND PROCESS DEVELOPMENT (IPPD); 3. INTEGRATED PRODUCT (PROGRAM) TEAM (IPT) MANAGEMENT; 4. SYSTEM ENGINEERING; 5. WORK BREAKDOWN STRUCTURE (WBS); 6. CONTRACT MANAGEMENT; 7. EARNED VALUE (EV) MEASUREMENT; 8. PROGRAM SCHEDULING; 9. RISK MANAGEMENT. TEAM PROBLEM AND REVIEW.	\$ 18,000.00	\$ 18,000.00	1/18/07	1/18/07	SIMPLIFIED ACQUISITION PROCEDURE 5-NON-COMPETITIVE
P3 SOLUTIONS LIMITED LIABILITY COMPANY	ON-SITE TRAINING COURSE ENTITLED: FROM RFP RELEASE TO PROPOSAL SUBMISSION: AN INDUSTRY PERSPECTIVE. JANUARY 16, 2007, AND JANUARY 23, 2007. 3.5 HOUR COURSE PROVIDES AN OVERVIEW OF HOW INDUSTRY RESPONDS TO GOVERNMENT RFPS. COURSE PARTICIPANTS WILL LEARN, STEP-BY-STEP, HOW A TYPICAL CONTRACTOR (SMALL AND LARGE BUSINESSES) WOULD GO ABOUT PREPARING PROPOSALS THAT ENABLE THE GOVERNMENT TO MAKE A BEST-VALUE DETERMINATION. COST: \$2,499 FOR EACH OF THE TWO COURSES = \$4,998.	\$4,998.00	\$4,998.00	1/23/07	1/23/07	SIMPLIFIED ACQUISITION PROCEDURE 5-NON-COMPETITIVE
FLORIDA INSTITUTE OF TECHNOLOGY	NONE.	\$ 36,000.00	\$ 36,000.00	2/26/07	9/30/07	ONLY ONE SOURCE - OTHER

<p>FEDERAL PUBLICATIONS SEMINARS LIMITED LIABILITY COMPANY</p>	<p>ON-SITE COST AND PRICE ANALYSIS IN GOVERNMENT CONTRACTS COURSE. THE COURSE WILL COVER:</p> <ol style="list-style-type: none"> 1. THE CONTRACT PRICING ENVIRONMENT; 2. THE FOUNDATIONS OF PRICE ANALYSIS; 3. PRICE-RELATED DATA AND FACTORS FOR AWARD; 4. QUANTITATIVE TECHNIQUES FOR PRICE ANALYSIS; 5. PRICE ANALYSIS RELATED DECISIONS; 6. DOCUMENTING PRICE ANALYSIS; 7. OVERVIEW OF COST ANALYSIS; 8. QUANTITATIVE TECHNIQUES FOR COST ANALYSIS; 9. DIRECT MATERIAL, DIRECT LABOR, OTHER DIRECT AND INDIRECT COST ANALYSIS; 10. FACILITIES CAPITAL COST OF MONEY; 11. PROFIT/FEE ANALYSIS; AND 12. PREPARING FOR NEGOTIATION. <p>TWO, TWO-DAY SESSIONS; FEBRUARY 27, 2007 AND FEBRUARY 28, 2007, FOR THE OFFICE OF ACQUISITION (OOA) FELLOWS, AND MARCH 21, 2007 AND MARCH 22, 2007, FOR OOA STAFF. COST: \$9,500 FOR EACH TWO-DAY COST.</p>	<p>\$ 19,000.00</p>	<p>\$ 19,000.00</p>	<p>2/16/07</p>	<p>3/22/07</p>	<p>SIMPLIFIED ACQUISITION PROCEDURE S-NON-COMPETITIVE</p>
<p>P3 SOLUTIONS LIMITED LIABILITY COMPANY</p>	<p>ON-SITE TRAINING COURSE ENTITLED: FROM RFP RELEASE TO PROPOSAL SUBMISSION: AN INDUSTRY PERSPECTIVE. 3.5 HOUR COURSE PROVIDES AN OVERVIEW OF HOW INDUSTRY RESPONDS TO GOVERNMENT RFPs. COURSE PARTICIPANTS WILL LEARN, STEP-BY-STEP, HOW A TYPICAL CONTRACTOR (SMALL AND LARGE BUSINESSES) WOULD GO ABOUT PREPARING PROPOSALS THAT ENABLE THE GOVERNMENT TO MAKE A BEST-VALUE DETERMINATION.</p> <p>MARCH 6, 2007, FROM 8:30 A.M. TO 11:30 A.M.; AND MARCH 8, 2007, FROM 12:30 P.M. TO 3:30 P.M.</p> <p>COST: \$2,499 FOR EACH COURSE = \$4,998.</p>	<p>\$4,998.00</p>	<p>\$4,998.00</p>	<p>2/8/07</p>	<p>3/8/07</p>	<p>SIMPLIFIED ACQUISITION PROCEDURE S-NON-COMPETITIVE</p>

MAIC (Minority Advancement in Corporations Inc.)	Program Analyst Support for Cost Analysis & Research Branch	\$270,336.00	\$-	1/19/07	1/18/08	ONLY ONE SOURCE - OTHER
Oracle Solution & Services Limited Liability Comp.	Non-Competitive Procurement of Budgetary Support Services to correct a material weakness identified during the FY 2006 Financial Statement Audit. PR is based on a government cost estimate. Documentation will be provided to the Office of Acquisition. PR FIN018 was under funded therefore PR FIN022 was created to cover the cost of the award.	\$1,378,960.00	\$-	1/25/07	1/31/08	UNIQUE SOURCE
THE DASTON CORPORATION	RATIFICATION FOR PROPERTY DOCUMENTATION SERVICES PROVIDED FROM 8/2/2007 THROUGH 9/19/2007.	\$ 93,423.65	\$ 93,423.65	9/21/07	9/21/07	ONLY ONE SOURCE - OTHER
TALX CORPORATION	TALX RATIFICATION - FUNDS TO COVER RATIFICATION OF INVOICES DATED FROM MAY 1, 2005 THROUGH NOVEMBER 30, 2006. TALX CONTRACT HSTS01-05-P-HRA017 PROVIDES SOCIAL SECURITY SERVICES TO TSA EMPLOYEES.	\$ 14,895.25	\$ 14,895.25	12/21/06	12/21/06	ONLY ONE SOURCE - OTHER
ARAMARK SERVICES INCORPORATED (1630)	FOUNDATIONS OF LEADERSHIP TRAINING - 5 CLASSES TO BE CONDUCTED FOR SUPERVISORY TRANSPORTATION SECURITY OFFICERS (STSO). STUDENTS AND INSTRUCTORS WILL ARRIVE ON MAY 6 2007 AND THE CLASSES WILL BE CONDUCTED MAY 7-17 2007.	\$250,000.00	\$250,000.00	1/23/07	5/18/07	ONLY ONE SOURCE - OTHER
ARAMARK SERVICES INCORPORATED (1630)	FOUNDATIONS OF LEADERSHIP TRAINING - 5 CLASSES TO BE CONDUCTED FOR SUPERVISORY TRANSPORTATION SECURITY OFFICERS (STSO). STUDENTS AND INSTRUCTORS WILL ARRIVE ON MAY 6 2007 AND THE CLASSES WILL BE CONDUCTED MAY 7-17 2007.	\$ 18,785.00	\$ 18,785.00	2/1/07	5/18/07	ONLY ONE SOURCE - OTHER
VISIONARY LEADERSHIP LIMITED	SENIOR LEADERSHIP DEVELOPMENT PROGRAM (SLDP) - REQUEST FOR A GUEST SPEAKER IN SUPPORT OF THE SENIOR LEADERSHIP PROGRAM. THIS SPEAKER WILL BE ADDRESSING 85 SLDP SELECTEES IN THE KINK-OFF MEETING OF THEIR ORIENTATION.	\$5,000.00	\$5,000.00	1/30/07	2/12/07	UNIQUE SOURCE
OCEAN VIEW HOTEL CORPORATION	FOUNDATIONS VENUE JUNE 07 WAIKIKI BEACH - REQUEST \$110,000 TO SECURE 428 ROOM NIGHTS TO DELIVER TWO CONSECUTIVE OFFERINGS OF THE FOUNDATIONS OF LEADERSHIP AND TO HOUSE THE INSTRUCTORS FOR THE ENTIRE PERIOD OF TIME.	\$ 55,000.00	\$ 55,000.00	3/26/07	6/28/07	UNIQUE SOURCE

BIGSPEAK INCORPORATED	SPEAKER SERIES *STACY ALLISON - REQUEST \$19,000 TO SECURE A SPEAKER FOR TSA LEADERSHIP SPEAKER SERIES. PERIOD OF PERFORMANCE: 26 APR 2007	\$ 19,000.00	\$ 19,000.00	4/4/07	4/26/07	UNIQUE SOURCE
FREEMOUNT CORPORATION INCORPORATED	SPEAKER SERIES *CLIFTON L. TAUBERT - REQUEST \$12,750 TO SECURE A SPEAKER FOR TSA LEADERSHIP SPEAKER SERIES. PRESENTATION DATE: 28 JUN 2007	\$ 12,750.00	\$ 12,750.00	4/5/07	6/28/07	UNIQUE SOURCE
VISIONARY LEADERSHIP LIMITED	LEADERSHIP SPEAKER SERIES MAJOR GENERAL PERRY M. SMITH - REQUEST \$5,000 TO SECURE A SPEAKER FOR TSA LEADERSHIP SPEAKER SERIES. SPEAKING DATE: 27 SEP 2007 TOPIC: ETHICS AND LEADERSHIP: A PRACTICAL GUIDE LOCATION: HQ, TSA	\$5,000.00	\$5,000.00	5/1/07	9/27/07	UNIQUE SOURCE
ECKERD COLLEGE INCORPORATED	LEADERSHIP PROGRAM, ECKERD - REQUEST \$68,000 TO FUND TEN (10) SLOTS FOR TEN TSA SXCUTIVES OR SENIORS MANAGERS TO ATTEND THE ECKERD COLLEGE LEADERHSIP DEVELOPMENT PROGRAM, A NETWORK ASSOCIATE OF THE CENTER FOR CREATIVE LEADERSHIP (CCL).	\$ 68,000.00	\$ 68,000.00	5/22/07	10/19/07	FOLLOW-ON CONTRACT
UNIVERSITY OF VIRGINIA DARDEN SCHOOL FOUNDATION INCORPORATED	DARDEN EXECUTIVE EDUCATION - REQUEST \$17,000 TO FUND TWO (2) SLOTS FOR TWO TSA EXECUTIVES TO ATTEND THE DARDEN SCHOOL OF BUSINESS ADMINISTRATION, CREATING THE FUTURE, THE CHALLENGE OF TRANSFORMATIONAL LEADERSHIP. SCHEDULE:	\$ 17,000.00	\$ 17,000.00	7/6/07	10/19/07	UNIQUE SOURCE
ROCKHURST UNIVERSITY CONTINUING EDUCATION CENTER INCORPORATED	FEE FOR TRAINING CLASS	\$5,200.00	\$5,200.00	9/21/07	10/21/07	ONLY ONE SOURCE - OTHER
WASHINGTON SPEAKERS BUREAU	THIS PR IS FOR THE PURCHASE OF THE SERVICES FOR A GUEST SPEAKER AT THE OTT TRAINING COORDINATOR CONFERENCE FROM 10/31/2006 THROUGH 11/1/2006.	\$ 10,000.00	\$ 10,000.00	10/30/06	11/1/06	SIMPLIFIED ACQUISITION PROCEDURE S-NON-COMPETITIVE
NINTH HOUSE INCORPORATED	PROFESSIONAL MANAGEMENT SERVICES	\$7,890.00	\$7,890.00	6/29/07	8/15/07	UNIQUE SOURCE
CORT BUSINESS SERVICES CORPORATION	CORT RENTAL FURNITURE BUYOUT PROPOSAL FOR FIELD LOCATIONS	\$1,304,319.57	\$1,304,319.57	12/22/06	12/31/07	ONLY ONE SOURCE - OTHER
CORT BUSINESS SERVICES CORPORATION	CORT RENTAL FURNITURE BUYOUT PROPOSAL FOR FIELD LOCATIONS	\$ 75,000.00	\$ 75,000.00	2/9/07	12/31/07	ONLY ONE SOURCE - OTHER
CORT BUSINESS SERVICES CORPORATION	CORT RENTAL FURNITURE BUYOUT PROPOSAL FOR FIELD LOCATIONS	\$100,000.00	\$100,000.00	5/22/07	12/31/07	ONLY ONE SOURCE - OTHER

CORT BUSINESS SERVICES CORPORATION	CORT RENTAL FURNITURE BUYOUT PROPOSAL FOR FIELD LOCATIONS	\$108,791.61	\$108,791.61	8/16/07	12/31/07	ONLY ONE SOURCE - OTHER
F&A CARPET	PO - THIS IS TO REPLACE CARPET FOR NEWLY ACQUIRED SPACE (1800 SF) AT THE MIAMI INTERNATIONAL AIRPORT (MIA). REQUESTED PERIOD OF PERFORMANCE WILL LAST 30 DAYS AFTER AWARD DATE.	\$5,660.00	\$5,660.00	3/8/07	3/9/07	SIMPLIFIED ACQUISITION PROCEDURE - NON-COMPETITIVE
FORSMAN INCORPORATED	PO- PROVIDE FUNDING TO COBALT CONTRACTOR TO CONSTRUCT AND RENOVATE 13 TSA LOCATIONS AT MCCARRAN INTERNATIONAL AIRPORT (LAS) LAS VEGAS, NEVADA. REQUESTED PERIOD OF PERFORMANCE IS 8 MONTHS.	\$1,160,148.00	\$1,160,148.00	7/18/07	11/30/07	FOLLOW-ON CONTRACT
PLATA CORPORATION	PO - FUNDING FOR DESIGN AND CONSTRUCTION OF THE T2 & T3 ON-SITE SPACE AT CHICAGO O'HARE AIRPORT (ORD).	\$ 88,724.46	\$ 88,724.46	9/19/07	3/31/08	AUTHORIZED BY STATUTE
BARKLEY REGIONAL AIRPORT AUTHORITY	PO- FUNDING NEEDED FOR YEARLY JANITORIAL SERVICES FOR PAH (BARKLEY REGIONAL AIRPORT, PADUCAH, KY). TSA CURRENTLY HAS A MOU WITH FAA AND TSA NEEDS TO PROCURE JANITORIAL SERVICES DIRECTLY. SERVICES ARE TO INCLUDE DAILY CLEANING AND SUPPLIES, WITH SNOW REMOVAL AND LANDSCAPING.	\$ 15,360.00	\$ 15,360.00	9/19/07	9/18/08	ONLY ONE SOURCE - OTHER
The Onyx Group	To design, and implement an integrated worker's compensation case management module into the existing safety information systems. Associated with PR 2107FAMMED005.	\$1,211,537.22	\$1,795,017.14	9/21/07	9/23/08	ONLY ONE SOURCE - OTHER
WHITE OAK TECHNOLOGIES INCORPORATED	DATA HARVESTING	\$875,590.00	\$875,590.00	6/4/07	9/21/08	UNIQUE SOURCE
IntelliTrans, Inc.	Sole-Source to IntelliTrans, Inc., for electronic monitoring and reporting services of Toxic Inhalation Hazard (TIH) and Highway Non-Transportable radioactive substances via Rail	\$455,625.00	\$455,625.00	3/1/07	3/1/08	UNIQUE SOURCE
General Dynamics	Mod to Truck Tracking Security Pilot Contract with General Dynamics - HSTS02-05-C-HMC163 Mod will extend PoP from 05/31/2007 until 12/31/2007 and IGCE to add funds of \$1.3M. SSJ required (see milestones).	\$1,350,000.00	\$5,066,350.00	6/29/07	1/0/00	ONLY ONE SOURCE - OTHER
General Dynamics	General Dynamics Single Source Mod - HSTS02-05-C-HMC163 - Additional required funds beyond IGCE amount.	\$ 58,606.00	\$5,066,350.00	6/29/07	1/31/08	ONLY ONE SOURCE - OTHER

SAIC	SAIC Mod to change task descriptions - Ssj required - HSTS02-05-C-STZ004 See milestones	\$225,000.00	\$2,261,963.00	6/29/07	4/30/08	ONLY ONE SOURCE - OTHER
SAIC	Extra funding required for SAIC sole source mod.	\$975.00	\$2,261,963.00	6/29/07	4/30/08	ONLY ONE SOURCE - OTHER
NATIONAL LAW ENFORCEMENT TELECOMMUNICATION SYSTEM	SUBSCRIPTION TO THE NATIONAL LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEM	\$ 48,000.00	\$ 48,000.00	11/3/06	12/31/07	UNIQUE SOURCE
TRANSPORTATION TECHNOLOGY CENTER INCORPORATED	SECURITY TRAINING	\$200,000.00	\$200,000.00	2/16/07	11/30/07	UNIQUE SOURCE
TRANSPORTATION TECHNOLOGY CENTER INCORPORATED	SECURITY TRAINING	\$200,000.00	\$200,000.00	6/26/07	11/30/07	UNIQUE SOURCE
CLASSIFIED DOMESTIC CONTRACTOR	MANAGEMENT SUPPORT SERVICES	\$968,042.00	\$968,042.00	8/2/07	10/30/08	ONLY ONE SOURCE - OTHER
INFOGLIDE SOFTWARE CORPORATION	SF SYSEM DESIGN/TEST	\$1,299,995.39	\$1,299,995.39	10/3/06	9/30/07	ONLY ONE SOURCE - OTHER
INFOGLIDE SOFTWARE CORPORATION	SF SYSEM DESIGN/TEST	\$182,280.00	\$182,280.00	10/11/06	9/30/07	ONLY ONE SOURCE - OTHER
INFOGLIDE SOFTWARE CORPORATION	SF SYSEM DESIGN/TEST	\$1,970,058.00	\$1,970,058.00	3/30/07	9/30/07	ONLY ONE SOURCE - OTHER
AMERICAN ASSOCIATION OF AIRPORT EXECUTIVES	COLLECT AND PROCESS FINGERPRINTS FOR AFSP	\$2,850.00	\$2,850.00	11/28/06	2/28/10	ONLY ONE SOURCE - OTHER
AMERICAN ASSOCIATION OF AIRPORT EXECUTIVES	COLLECT AND PROCESS FINGERPRINTS FOR AFSP	\$ 51,000.00	\$ 51,000.00	12/19/06	2/28/10	ONLY ONE SOURCE - OTHER
AMERICAN ASSOCIATION OF AIRPORT EXECUTIVES	COLLECT AND PROCESS FINGERPRINTS FOR AFSP	\$3,840.00	\$3,840.00	1/24/07	2/28/10	ONLY ONE SOURCE - OTHER
AMERICAN ASSOCIATION OF AIRPORT EXECUTIVES	COLLECT AND PROCESS FINGERPRINTS FOR AFSP	\$ 90,000.00	\$ 90,000.00	2/28/07	2/28/10	ONLY ONE SOURCE - OTHER
AMERICAN ASSOCIATION OF AIRPORT EXECUTIVES	COLLECT AND PROCESS FINGERPRINTS FOR AFSP	\$1,320.00	\$1,320.00	5/21/07	2/28/10	ONLY ONE SOURCE - OTHER
AMERICAN ASSOCIATION OF AIRPORT EXECUTIVES	COLLECT AND PROCESS FINGERPRINTS FOR AFSP	\$ 60,000.00	\$ 60,000.00	8/20/07	2/29/08	ONLY ONE SOURCE - OTHER
ONEIL MOVING SYSTEMS INCORPORATED	STORAGE OF HOUSEHOLD GOODS BELONGING TO TSA EMPLOYEES WHILE ON OVERSEAS ASSIGNMENT	\$ 11,136.00	\$ 11,136.00	1/8/07	12/31/07	ONLY ONE SOURCE - OTHER
AMERICAN INTERNATIONAL FORWARDING INCORPORATED	STORAGE OF HOUSEHOLD GOODS BELONGING TO TSA EMPLOYEES WHILE ON OVERSEAS ASSIGNMENT	\$8,866.32	\$8,866.32	1/11/07	12/31/07	ONLY ONE SOURCE - OTHER
AMERICAN INTERNATIONAL FORWARDING INCORPORATED	STORAGE OF HOUSEHOLD GOODS BELONGING TO TSA EMPLOYEES WHILE ON OVERSEAS ASSIGNMENT	\$ 13,342.08	\$ 13,342.08	2/23/07	12/31/07	ONLY ONE SOURCE - OTHER
ALASKA SEAVAN INCORPORATED	STORAGE OF HOUSEHOLD GOODS BELONGING TO TSA EMPLOYEES, WHILE ON OVERSEAS ASSIGNMENT	\$ 15,828.60	\$ 15,828.60	2/23/07	12/31/07	ONLY ONE SOURCE - OTHER

GRAEBEL/MID ATLANTIC MOVERS INCORPORATED	STORGE OF HOUSEHOLD GOODS BELONGING TO TSA EMPLOYEES WHILE ON OVERSEAS ASSIGNMENT	\$2,772.00	\$2,772.00	2/23/07	12/31/07	ONLY ONE SOURCE - OTHER
XSPEDIUS COMMUNICATIONS LIMITED LIABILITY COMPANY	2 CIRCUITS AND MAINTENANCE FOR TELECOMMUNICATION SERVICE	\$388,200.00	\$388,200.00	8/17/07	9/30/10	URGENCY
INFOGLIDE SOFTWARE CORPORATION	INFOGLIDE SOFTWARE LICENSES AND MAINTENANCE	\$1,470,000.00	\$1,470,000.00	12/6/06	12/31/07	UNIQUE SOURCE
MISCELLANEOUS FOREIGN CONTRACTORS	SOLE SOURCE JUSTIFICATION FOR MICHAEL STAPLETON ASSOCIATES AND THE STATEN ISLAND FERRY TO CONTRACT OFF-DUTY LAW ENFORCEMENT OFFICERS WHO WILL STAND WATCH DURING SEACAP SCREENING PERIODS. THESE LAW ENFORCEMENT PERSONNEL WILL ASSIST WITH RESOLUTION OF ALARMS DURING SECONDARY SCREENING AND TAKE CHARGE SHOULD SCREENING UNCOVER ANY CONTRABAND, PROHIBITED ITEMS, OR WEAPONS. THE PERIOD OF PERFORMANCE WILL OCCUR BETWEEN APRIL 2 -20, 2007.	\$ 20,000.00	\$ 20,000.00	4/9/07	5/9/07	UNIQUE SOURCE
AOPA AIR SAFETY FOUNDATION	ONLINE TRAINING COURSE NTE \$150,000 AND ADDITIONAL PROMOTIONAL MATERIAL DEVELOPMENT AND DISTRIBUTION NTE \$70,000 FOR AIRPORT WATCH	\$220,000.00	\$220,000.00	7/5/07	6/14/07	ONLY ONE SOURCE - OTHER
AOPA AIR SAFETY FOUNDATION	ONLINE TRAINING COURSE NTE \$150,000 AND ADDITIONAL PROMOTIONAL MATERIAL DEVELOPMENT AND DISTRIBUTION NTE \$70,000 FOR AIRPORT WATCH	\$ 55,000.00	\$ 55,000.00	9/12/07	6/14/07	ONLY ONE SOURCE - OTHER
NATA COMPLIANCE SERVICES LIMITED LIABILITY COMPANY	WORK IN CONJUNCTION WITH THE NATIONAL AIR TRANSPORTATION ASSOCIATION (NATA) TO ACQUIRE AVIATION CARD READERS AND EMPLOY THESE CARD READERS AT FIXED BASED OPERATOR (FBO) LOCATIONS AT THE NATION'S BUSIEST AND LARGEST GA AIRPORTS OR DESIGNATED GA FACILITIES AT PUBLIC USE AIRPORTS. CO: GUY GALLOWAY TSNM: GA POC: ERIK JENSEN	\$8,098.00	\$8,098.00	8/23/07	9/22/07	UNIQUE SOURCE

DUN AND BRADSTREET INCORPORATED (2360)	THIS PR PROVIDES FUNDING TO RENEW DUN & BRADSTREET SERVICES FOR AIR CARGO'S INDIRECT AIR CARRIER MANAGEMENT SYSTEM, KNOWN SHIPPER MANAGEMENT SYSTEM, AND THE FREIGHT ASSESSMENT SYSTEMS. NOTE: CONTRACT NUMBER IS HSTS01-05-F-AOP196	\$6,509,949.82	\$6,509,949.82	5/22/07	5/22/08	ONLY ONE SOURCE - OTHER
INTELLITRANS LIMITED LIABILITY COMPANY	TOXIC INHALATION HAZARD (TIH) TANK CAR MOVEMENT IN HIGH THREAT URBAN AREAS (HTUA)	\$981,500.00	\$981,500.00	3/1/07	12/31/08	ONLY ONE SOURCE - OTHER
INTELLITRANS LIMITED LIABILITY COMPANY	TOXIC INHALATION HAZARD (TIH) TANK CAR MOVEMENT IN HIGH THREAT URBAN AREAS (HTUA)	\$114,755.00	\$114,755.00	9/6/07	12/31/08	ONLY ONE SOURCE - OTHER
Oracle Solution & Services LLC/Miracle Systems LLC	Provides financial database, analysis, and administrative Support for the Office of Security and Assessment from July 1, 2007 to June 30, 2008. Vendor will perform the following duties: Processes, Analysis and Audit Database Management, Reports Creation, Ad Hoc Querying Data Entry, Financial Documentation, Files Maintenance, etc.	\$945,552.00	\$3,464,512.00	8/31/07	8/30/08	ONLY ONE SOURCE - OTHER
ADVANCED MEASUREMENT TECHNOLOGY INCORPORATED	PROCUREMENT OF RADIATION DETECTION EQUIPMENT: THREE MECHANICALLY COOLED, HIGH PURITY GERMANIUM (HPGE) RADIOISOTOPE IDENTIFICATION DEVICES (RIDS) (HPGE RIDS) TO SUPPORT THE SOUTHERN REGIONAL RADIOLOGICAL PILOT PROGRAM (SRRPP). THE REQUIRED RID (2019 MODEL) IS ONLY AVAILABLE FROM THE MANUFACTURER, ORTEC. (ADVANCED MEASUREMENT TECHNOLOGY, INC.). JUSTIFICATION FOR SINGLE SOURCE AWARD NO. 07-2-10 APPROVED BY TSA OFFICE OF CHIEF COUNSEL ON 8/17/07.	\$225,358.07	\$225,358.07	8/29/07	8/29/09	UNIQUE SOURCE
SKY GROUP ASSOCIATES INCORPORATED	THIS PR REPLACES PR 21-07-207MLSS02 THIS REQUEST WILL PROVIDE ADDITIONAL FUNDING TO SUPPORT THE ONGOING LARGE AIRCRAFT STANDARD SECURITY PROGRAM (LASSP) CONTRACT FOR 4 ADDITIONAL MONTHS AT THE CURRENT RATE.	\$267,728.09	\$267,728.09	8/30/07	6/30/08	UNIQUE SOURCE
DYNO NOBEL INCORPORATED	DYNO NOBEL - IDIQ	\$8,954.40	\$8,954.40	8/29/07	12/31/07	ONLY ONE SOURCE - OTHER

DYNO NOBEL INCORPORATED	DYNO NOBEL - IDIQ	\$1,876.80	\$1,876.80	9/4/07	12/31/07	ONLY ONE SOURCE - OTHER
MITRE Corporation	MITRE IDIQ	\$2,461,841.00	\$3,301,917.00	1/29/07	1/0/00	ONLY ONE SOURCE - OTHER
The MITRE Corporation	PR to provide additional funding to PR TTC301 for the MITRE Corp.	\$500,000.00	\$500,000.00	2/22/07	1/0/00	ONLY ONE SOURCE - OTHER
ILM	Task Order off of HSTS02-07-D-TTC339 for Indirect Air Carriers (IAC)	\$298,864.24	\$298,864.24	4/19/07	4/23/07	ONLY ONE SOURCE - OTHER
ENTERPRISE SOLUTIONS REALIZED INCORPORATED	ESR TO #1 - PROVIDE SYSTEM ARCHITECTURE AND DESIGN, ENGINEERING PLANNING AND INTEGRATION OF THE RATIONAL UNIFIED PROCESS (RUP). PROVIDE EXPERTISE IN COMPUTER HARDWARE, SOFTWARE AND APPLICATION DEVELOPMENT.	\$465,561.00	\$465,561.00	1/25/07	1/27/10	AUTHORIZED BY STATUTE
THE MITRE CORPORATION	THE MITRE CORP - SYSTEMS ENGINEERING AND ASSESSMENT SERVICES (SEAS). THE ADDITIONAL FUNDING WILL EXTEND THE FUNDED PERIOD OF PERFORMANCE TO SEPTEMBER 30, 2007	\$3,301,917.00	\$3,301,917.00	1/29/07	10/1/07	ONLY ONE SOURCE - OTHER
THE MITRE CORPORATION	THE MITRE CORP - PROVIDING SYSTEMS ENGINEERING AND ASSESSMENT SERVICES (SEAS)	\$833,650.00	\$833,650.00	1/29/07	10/1/07	ONLY ONE SOURCE - OTHER
THE MITRE CORPORATION	THE MITRE CORP - PROVIDING SYSTEMS ENGINEERING AND ASSESSMENT SERVICES (SEAS)	\$500,000.00	\$500,000.00	2/22/07	10/1/07	ONLY ONE SOURCE - OTHER
THE MITRE CORPORATION	THE MITRE CORP - PROVIDING SYSTEMS ENGINEERING AND ASSESSMENT SERVICES (SEAS)	\$167,864.00	\$167,864.00	4/3/07	10/1/07	ONLY ONE SOURCE - OTHER
THE MITRE CORPORATION	THE MITRE CORP - PROVIDING SYSTEMS ENGINEERING AND ASSESSMENT SERVICES (SEAS)	\$604,792.00	\$604,792.00	5/11/07	10/1/07	ONLY ONE SOURCE - OTHER
THE MITRE CORPORATION	THE MITRE CORP - PROVIDING SYSTEMS ENGINEERING AND ASSESSMENT SERVICES (SEAS)	\$356,000.00	\$356,000.00	7/31/07	10/1/07	ONLY ONE SOURCE - OTHER
DYNO NOBEL INCORPORATED	FY 07 DYNO NOBEL - EXPLOSIVES	\$3,600.90	\$3,600.90	2/23/07	4/6/07	ONLY ONE SOURCE - OTHER
ENSGN BICKFORD AEROSPACE AND DEFENSE COMPANY	ENSGN-BICKFORD - EXPLOSIVES	\$ 93,690.40	\$ 93,690.40	3/9/07	6/1/07	UNIQUE SOURCE
HODGDON POWDER COMPANY	HODGDON POWDER - EXPLOSIVES	\$ 16,158.00	\$ 16,158.00	3/9/07	5/21/07	UNIQUE SOURCE
TieBridge, Inc	HAZMAT Truck Security Pilot Surface Transportation and Tracking of High-Hazard Materials International Security Practices Study	\$ 49,600.00	\$ 49,600.00	8/29/07	2/28/08	UNIQUE SOURCE
APPLIED COMMUNICATIONS GROUP	5 PROFESSIONAL DEVELOPMENT TRAINING COURSES FOR TSA-OI STAFF MEMBERS	\$ 27,000.00	\$ 27,000.00	5/8/07	9/28/07	UNIQUE SOURCE

ID Solutions, Inc.	Procurement of additional ID Solutions - Automated Fingerprint Identification System (AFIS) software licenses for TWIC Phase IV	\$ 32,500.00	\$ 32,500.00	1/22/07	1/21/08	UNIQUE SOURCE
Gemalto	Card Stock for ID cards, to support the TWIC deployment. Note: this PR is for the cards only; the laminate is being procured under another PR	\$ 97,400.00	\$ 97,400.00	2/15/07	6/20/07	UNIQUE SOURCE
AWARE INCORPORATED (1026)	PROCUREMENT OF NISTPACK SERVER SOFTWARE LICENSES AND MAINTENANCE FOR THE TWIC SYSTEM.	\$ 42,627.50	\$ 42,627.50	9/6/07	9/5/08	ONLY ONE SOURCE - OTHER
U.S. Army	For purchase of explosive propellants from the U.S. Army Rock Island Arsenal	\$ 22,782.00	\$ 22,782.00	7/1/07	1/0/00	UNIQUE SOURCE
U.S. Army	Purchase of explosive propellants for NEDCTP from the U.S. Army's Rock Island Arsenal	\$ 35,202.00	\$ 35,202.00	7/1/07	1/0/00	UNIQUE SOURCE
U.S. Army Rock Island Arsenal	Purchase of explosive training propellants for the national Explosives Detection Canine Team Program (NEDCTP) from the U.S. Army	\$ 21,354.00	\$ 21,354.00	7/1/07	1/0/00	UNIQUE SOURCE
RENO TAHOE AIRPORT AUTHORITY	LEASE ON AIRPORT OPERATIONS PREMISES - EFFECTIVE 10/1/02	\$154,462.68	\$914,951.41	7/18/07	6/30/08	UNIQUE SOURCE
KENT COUNTY DEPARTMENT OF AERONAUTICS	SPACE RENTAL	\$187,375.92	\$187,375.92	8/16/07	7/17/08	UNIQUE SOURCE
NEC UNIFIED SOLUTIONS INCORPORATED	TELECOMM FOR DFW	\$4,151.78	\$4,151.78	2/15/07	5/17/07	ONLY ONE SOURCE - OTHER
NEC UNIFIED SOLUTIONS INCORPORATED	TELECOMM FOR DFW	\$ 10,000.00	\$ 10,000.00	5/17/07	12/15/07	ONLY ONE SOURCE - OTHER
SIGNAL SOLUTIONS INCORPORATED	SOFTWARE SERVICES	\$279,285.00	\$279,285.00	11/6/06	11/9/10	ONLY ONE SOURCE - OTHER
OBBERON ASSOCIATES INCORPORATED	DATA MANAGEMENT	\$1,561,330.56	\$1,561,330.56	4/3/07	5/17/08	ONLY ONE SOURCE - OTHER
Teracore, Inc.	Request to add additional funds to the Teracore contract. Additional work was added which was not envisioned in the original scope, therefore, additional funds are needed to cover the work. The contract number is: HSTS03-06-C-SMA014. The accounting string is: TS078A000 2007 HQA0100 GE0000 7700 5000 500ADM	\$ 54,363.00	\$403,351.00	2/14/07	3/31/07	ONLY ONE SOURCE - OTHER
Teracore, Inc.	Funding Option Period of 45 days on HSTS03-06-C-SMA014	\$ 54,363.00	\$403,351.00	3/30/07	5/15/07	ONLY ONE SOURCE - OTHER
Unisys Corporation	Funds to extend services for circuits under HSTS03-07-J-CIO082.	\$486,493.22	\$486,493.22	3/16/07	6/30/07	ONLY ONE SOURCE - OTHER
Unisys Corporation	Funs for HSTS03-07-J-CIO113 for O&M services on contract services	\$399,232.84	\$399,232.84	3/23/07	3/19/08	ONLY ONE SOURCE - OTHER

Unisys Corporation	Additional funds for RTOP CIO044 Microsoft upgrade, related to PR CIO044	\$1,695,680.00	\$2,195,680.00	5/11/07	5/8/08	ONLY ONE SOURCE - OTHER
Unisys Corporation	Funds for TO under the Bridge to support the KSD residing in Malvern, PA.	\$630,000.00	\$2,841,294.27	5/17/07	11/30/07	ONLY ONE SOURCE - OTHER
Unisys Corporation	Tibco Middleware support under eTAS program	\$517,669.60	\$2,647,977.42	9/12/07	9/11/08	ONLY ONE SOURCE - OTHER
Nsync Services Inc.	Funds to support a PLC pilot at three airports, PR replaces PR# 2107207CIO095	\$287,000.00	\$-	3/20/07	3/19/08	ONLY ONE SOURCE - OTHER
Nsync Services Inc.	Hi Soc Deployment completion utilizing Power Line Communications Technology.	\$221,747.40	\$-	4/6/07	4/6/07	ONLY ONE SOURCE - OTHER
STATE OF ALASKA	FERRY PASSES	\$ 12,780.00	\$ 12,780.00	5/9/07	12/31/07	ONLY ONE SOURCE - OTHER
STATE OF ALASKA	FERRY PASSES	\$ 30,000.00	\$ 30,000.00	8/24/07	12/31/07	ONLY ONE SOURCE - OTHER
UNISYS CORPORATION	IT BRIDGE	\$9,408.47	\$9,408.47	6/18/07	12/31/07	FOLLOW-ON CONTRACT
UNISYS CORPORATION	IT BRIDGE	\$ 11,130.44	\$ 11,130.44	2/1/07	6/30/07	FOLLOW-ON CONTRACT
UNISYS CORPORATION	IT BRIDGE	\$ 47,771.88	\$ 47,771.88	6/4/07	12/31/07	FOLLOW-ON CONTRACT
UNISYS CORPORATION	IT BRIDGE	\$324,595.58	\$324,595.58	4/19/07	12/31/07	FOLLOW-ON CONTRACT
UNISYS CORPORATION	IT BRIDGE	\$381,319.41	\$381,319.41	4/26/07	12/31/07	FOLLOW-ON CONTRACT
UNISYS CORPORATION	LAND MOBILE RADIO MANAGED SERVICES	\$2,907,407.00	\$2,907,407.00	1/9/07	12/31/07	FOLLOW-ON CONTRACT
UNISYS CORPORATION	IT BRIDGE	\$ 48,144.93	\$ 48,144.93	3/6/07	12/31/07	FOLLOW-ON CONTRACT
UNISYS CORPORATION	SUPPORT FOR THE FINGERPRINT SYSTEMS	\$866,114.48	\$866,114.48	12/14/06	12/31/07	FOLLOW-ON CONTRACT
UNISYS CORPORATION	IT BRIDGE	\$562,496.85	\$562,496.85	6/20/07	6/20/07	FOLLOW-ON CONTRACT
NSYNC SERVICES INCORPORATED	ISSUE: FUNDING OF 8A CONTRACTOR TO PROVIDE DSL AND / OR WIRELESS CONNECTIVITY FOR AIRPORTS THAT HAVE PCS THAT WILL NOT BE CONNECTED TO TSA NETWORK BY 30 SEPTEMBER 06. THIS PR IS FOR NEW WORK WHICH INCLUDES PLANNING, SITE PREPARATION, INSTALLATION AND COST FOR THE DEPLOYMENT OF THE SMALL SITE DSL SOLUTION AND / OR COMMERCIAL WIRELESS CONNECTIVITY.	\$288,683.79	\$288,683.79	1/26/07	8/31/07	AUTHORIZED BY STATUTE

NSYNC SERVICES INCORPORATED	ISSUE: FUNDING OF 8A CONTRACTOR TO PROVIDE DSL AND / OR WIRELESS CONNECTIVITY FOR AIRPORTS THAT HAVE PCS THAT WILL NOT BE CONNECTED TO TSA NETWORK BY 30 SEPTEMBER 06. THIS PR IS FOR NEW WORK WHICH INCLUDES PLANNING, SITE PREPARATION, INSTALLATION AND COST FOR THE DEPLOYMENT OF THE SMALL SITE DSL SOLUTION AND / OR COMMERCIAL	\$284,329.94	\$284,329.94	7/17/07	3/31/08	AUTHORIZED BY STATUTE
UNISYS CORPORATION	SYSTEMS MANAGEMENT SUPPORT FOR THE TSA CONTACT CENTER OF THE OFFICE OF SPECIAL COUNSELOR. PURPOSE OF THIS PR IS TO TRANSITION SR-40066 FROM THE TSA ITMS CONTRACT TO THE NEW BRIDGE CONTRACT. FUNDING SHOULD COVER SERVICES DELIVERED BY UNISYS FOR ONE FISCAL QUARTER.	\$267,765.66	\$267,765.66	12/11/06	12/31/07	FOLLOW-ON CONTRACT
UNISYS CORPORATION	SYSTEMS MANAGEMENT SUPPORT FOR THE TSA CONTACT CENTER OF THE OFFICE OF SPECIAL COUNSELOR. PURPOSE OF THIS PR IS TO TRANSITION SR-40066 FROM THE TSA ITMS CONTRACT TO THE NEW BRIDGE CONTRACT. FUNDING SHOULD COVER SERVICES DELIVERED BY UNISYS FOR ONE FISCAL QUARTER.	\$3,602.00	\$3,602.00	2/27/07	4/30/07	FOLLOW-ON CONTRACT
UNISYS CORPORATION	SYSTEMS MANAGEMENT SUPPORT FOR THE TSA CONTACT CENTER OF THE OFFICE OF SPECIAL COUNSELOR. PURPOSE OF THIS PR IS TO TRANSITION SR-40066 FROM THE TSA ITMS CONTRACT TO THE NEW BRIDGE CONTRACT. FUNDING SHOULD COVER SERVICES DELIVERED BY UNISYS FOR ONE FISCAL QUARTER.	\$ 25,740.52	\$ 25,740.52	8/6/07	8/31/07	FOLLOW-ON CONTRACT
MASSACHUSETTS PORT AUTHORITY	LEASE SPACE	\$ 78,994.55	\$ 78,994.55	1/22/07	2/28/07	UNIQUE SOURCE
MASSACHUSETTS PORT AUTHORITY	LEASE SPACE	\$572,917.24	\$572,917.24	2/27/07	9/30/07	UNIQUE SOURCE
MASSACHUSETTS PORT AUTHORITY	LEASE SPACE	\$568,857.90	\$568,857.90	8/29/07	2/28/08	UNIQUE SOURCE
MASSACHUSETTS PORT AUTHORITY	LEASE SPACE	\$ 10,431.53	\$ 10,431.53	8/29/07	2/29/08	UNIQUE SOURCE
MASSACHUSETTS PORT AUTHORITY	LEASE SPACE	\$5,313.56	\$5,313.56	6/15/07	9/30/07	UNIQUE SOURCE
MASSACHUSETTS PORT AUTHORITY	LEASE SPACE	\$6,642.15	\$6,642.15	8/27/07	2/28/08	UNIQUE SOURCE
ORANGE COUNTY OF (0928) 184716	LEASED SPACE	\$268,438.44	\$268,438.44	8/2/07	8/31/08	UNIQUE SOURCE
MASSACHUSETTS PORT AUTHORITY	LEASED SPACE	\$ 23,930.06	\$ 64,953.02	5/21/07	10/17/08	UNIQUE SOURCE

MINNEAPOLIS ST PAUL METROPOLITAN AIRPORTS COMMISSION	FIBER CABLE	\$4,224.00	\$4,224.00	2/7/07	2/28/09	UNIQUE SOURCE
METROPOLITAN WASHINGTON AIRPORTS AUTHORITY	FIBER LEASE	\$6,948.00	\$ 30,708.00	2/27/07	6/18/09	UNIQUE SOURCE
METROPOLITAN WASHINGTON AIRPORTS AUTHORITY	FIBER LEASE	\$ 40,920.00	\$ 40,920.00	6/12/07	6/18/09	UNIQUE SOURCE
METROPOLITAN WASHINGTON AIRPORTS AUTHORITY	TO MEET THE OCIO HIGH SPEED OPERATIONAL CONNECTIVITY (HI-SOC) REQUIREMENTS AT DULLES (IAD) INTERNATIONAL AIRPORT, THE US GOVT [TSA] DESIRES TO LEASE 22,300 FEET (\$0.23 PER FOOT) OF SINGLE MODE (SM) DARK FIBER FROM METRO WASHINGTON [MWAA] AIRPORT AUTHORITY.	\$6,584.40	\$6,584.40	2/13/07	7/31/07	ONLY ONE SOURCE - OTHER
METROPOLITAN WASHINGTON AIRPORTS AUTHORITY	TO MEET THE OCIO HIGH SPEED OPERATIONAL CONNECTIVITY (HI-SOC) REQUIREMENTS AT DULLES (IAD) INTERNATIONAL AIRPORT, THE US GOVT [TSA] DESIRES TO LEASE 22,300 FEET (\$0.23 PER FOOT) OF SINGLE MODE (SM) DARK FIBER FROM METRO WASHINGTON [MWAA] AIRPORT AUTHORITY.	\$252.00	\$1,116.00	4/5/07	7/31/07	ONLY ONE SOURCE - OTHER
METROPOLITAN WASHINGTON AIRPORTS AUTHORITY	TO MEET THE OCIO HIGH SPEED OPERATIONAL CONNECTIVITY (HI-SOC) REQUIREMENTS AT DULLES (IAD) INTERNATIONAL AIRPORT, THE US GOVT [TSA] DESIRES TO LEASE 22,300 FEET (\$0.23 PER FOOT) OF SINGLE MODE (SM) DARK FIBER FROM METRO WASHINGTON [MWAA] AIRPORT AUTHORITY.	\$ 73,032.00	\$-	7/17/07	7/31/08	ONLY ONE SOURCE - OTHER
CITY OF DAYTON	FIBER LEASE	\$576.00	\$576.00	6/4/07	6/30/08	ONLY ONE SOURCE - OTHER
SABRE INCORPORATED (9502)	TO FUND THE SINGLE SOURCE CONTRACT WITH SABRE, INC., OF SOUTHLAKE, TX, FOR PROFESSIONAL SERVICES TO DEVELOP AND DEPLOY THE TSA%U2019S IMPLEMENTATION OF SABRE STAFFPLAN AND STAFFADMIN, COMMONLY KNOWN AS THE SCREENER SCHEDULING SYSTEM (S3).	\$1,583,476.00	\$1,583,476.00	12/28/06		STANDARDIZATION

CITY OF ALBUQUERQUE	TO MEET THE OCIO HIGH SPEED OPERATIONAL CONNECTIVITY (HI-SOC) REQUIREMENTS AT ALBUQUERQUE INTERNATIONAL SUNPORT, THE US GOVT [TSA] DESIRES TO LEASE [4] STRANDS OF MULTI MODE (MMF) DARK FIBER FROM CITY OF ALBUQUERQUE, ALBUQUERQUE INTERNATIONAL SUNPORT (ABQ). HI-SOC IS FUNDED BY CONGRESS.	\$3,600.00	\$3,600.00	8/2/07	9/30/08	UNIQUE SOURCE
GREATER ORLANDO AVIATION AUTHORITY	THIS PURPOSE OF THIS PR IS TO PROVIDE FUNDING FOR FIBER INSTALLATION AT MCO (ORLANDO INTERNATIONAL AIRPORT).	\$4,615.00	\$4,615.00	12/13/06	3/13/06	UNIQUE SOURCE
CONGRESSIONAL QUARTERLY INCORPORATED	SUBSCRIPTION	\$1,750.00	\$1,750.00	12/19/06	8/2/07	ONLY ONE SOURCE - OTHER
FEDERAL EXPRESS CORPORATION	SHIPPING	\$ 12,000.00	\$ 12,000.00	2/8/07	3/16/08	UNIQUE SOURCE
CONGRESSIONAL QUARTERLY INCORPORATED	CONGRESSIONAL ELECTRONIC AND HOMELAND SECURITY SUBSCRIPTION	\$1,334.00	\$1,334.00	4/23/07	9/12/07	ONLY ONE SOURCE - OTHER
DESYNE WEB SERVICES INCORPORATED	DATABASE DEVELOPMENT, HOSTING AND MAINTENANCE	\$163,200.00	\$163,200.00	11/22/06	4/20/08	ONLY ONE SOURCE - OTHER
DESYNE WEB SERVICES INCORPORATED	DATABASE DEVELOPMENT, HOSTING AND MAINTENANCE	\$ 22,057.00	\$ 23,300.00	2/23/07	4/20/08	ONLY ONE SOURCE - OTHER
B&B ARMR CORPORATION	PR PROVIDES FUNDING FOR ANNUAL MAINTENANCE FOR FOUR (4) NASATKA SURFACE MOUNT BARRIERS IN SUPPORT OF ACCESS CONTROL AT TSA HQ GATED ENTRANCES. PHYSICAL SECURITY POC IS MARTY HOROWITZ AT 571-227-1191.	\$5,315.00	\$5,315.00	6/22/07	9/22/07	ONLY ONE SOURCE - OTHER
B&B ARMR CORPORATION	PR PROVIDES FUNDING FOR ANNUAL MAINTENANCE FOR FOUR (4) NASATKA SURFACE MOUNT BARRIERS IN SUPPORT OF ACCESS CONTROL AT TSA HQ GATED ENTRANCES. PHYSICAL SECURITY POC IS MARTY HOROWITZ AT 571-227-1191.	\$3,544.00	\$3,544.00	9/24/07	11/24/07	ONLY ONE SOURCE - OTHER
ABM LIMITED LIABILITY COMPANY (2203)	ABM, LLC - EXECUTIVE CONSULTATION GUIDANCE CONCERNING AVIATION SECURITY AND OTHER TOPICS IN SUPPORT OF THE WAR ROOM EFFORT AND AT THE DIRECTION OF THE ASSISTANT SECRETARY'S OFFICE. HSTS03-07-R-ADM900 PERIOD OF PERFORMANCE IS NOV 15, 2006 %U2013 NOV 14, 2007 W/ 1 YR. OPTION PERIOD	\$476,600.00	\$476,600.00	11/15/06	11/26/07	UNIQUE SOURCE

ABM LIMITED LIABILITY COMPANY (2203)	ABM, LLC - EXECUTIVE CONSULTATION GUIDANCE CONCERNING AVIATION SECURITY AND OTHER TOPICS IN SUPPORT OF THE WAR ROOM EFFORT AND AT THE DIRECTION OF THE ASSISTANT SECRETARY'S OFFICE. HSTS03-07-R-ADM900 PERIOD OF PERFORMANCE IS NOV 15, 2006 %U2013 NOV 14, 2007 W/ 1 YR. OPTION PERIOD	\$ 25,000.00	\$ 25,000.00	7/10/07	11/26/07	UNIQUE SOURCE
HOU LIHAN ASSOCIATES LIMITED LIABILITY COMPANY	CONTRACTING GUIDANCE ON SECURITY INITIATIVES, ORGANIZATIONAL POLICIES & PROCEDURES AND CRITICAL INCIDENT MANAGEMENT.	\$210,000.00	\$420,000.00	1/8/07	1/7/08	ONLY ONE SOURCE - OTHER
INVERTIX CORPORATION	PR IS FOR TSOC ANS SYSTEM MODIFICATIONS	\$489,999.00	\$1,630,821.00	2/2/07	2/4/09	ONLY ONE SOURCE - OTHER
INVERTIX CORPORATION	PR IS FOR TSOC ANS SYSTEM MODIFICATIONS	\$ 46,151.00	\$ 46,151.00	3/7/07	2/4/09	ONLY ONE SOURCE - OTHER
Invertix Corporation	ANS Support specialist to provide database management, Solaris OS support	\$220,000.00	\$220,000.00	2/2/07	2/4/08	ONLY ONE SOURCE - OTHER
BOOZ ALLEN HAMILTON INCORPORATED (3626)	CONTRACTOR SUPPORT TO INCREASE THE EFFECTIVENESS OF THE ORGANIZATION BY IMPLEMENTING IMPROVEMENT INITIATIVES THAT WILL RATIONALIZE ROLES AND RESPONSIBILITIES, STREAMLINE PROCESSES, AND IMPROVE THE EXECUTION OF DAY-TO-DAY OPERATIONS.	\$1,014,936.96	\$7,993,322.58	12/4/06	5/31/07	FOLLOW-ON CONTRACT
BOOZ ALLEN HAMILTON INCORPORATED (3626)	CONTRACTOR SUPPORT TO INCREASE THE EFFECTIVENESS OF THE ORGANIZATION BY IMPLEMENTING IMPROVEMENT INITIATIVES THAT WILL RATIONALIZE ROLES AND RESPONSIBILITIES, STREAMLINE PROCESSES, AND IMPROVE THE EXECUTION OF DAY-TO-DAY OPERATIONS.	\$476,314.46	\$476,314.46	12/5/06	5/31/07	FOLLOW-ON CONTRACT
BOOZ ALLEN HAMILTON INCORPORATED (3626)	CONTRACTOR SUPPORT TO INCREASE THE EFFECTIVENESS OF THE ORGANIZATION BY IMPLEMENTING IMPROVEMENT INITIATIVES THAT WILL RATIONALIZE ROLES AND RESPONSIBILITIES, STREAMLINE PROCESSES, AND IMPROVE THE EXECUTION OF DAY-TO-DAY OPERATIONS.	\$593,446.99	\$593,446.99	12/7/06	5/31/07	FOLLOW-ON CONTRACT

BOOZ ALLEN HAMILTON INCORPORATED (3626)	CONTRACTOR SUPPORT TO INCREASE THE EFFECTIVENESS OF THE ORGANIZATION BY IMPLEMENTING IMPROVEMENT INITIATIVES THAT WILL RATIONALIZE ROLES AND RESPONSIBILITIES, STREAMLINE PROCESSES, AND IMPROVE THE EXECUTION OF DAY-TO-DAY OPERATIONS.	\$150,000.00	\$150,000.00	12/21/06	5/31/07	FOLLOW-ON CONTRACT
BOOZ ALLEN HAMILTON INCORPORATED (3626)	CONTRACTOR SUPPORT TO INCREASE THE EFFECTIVENESS OF THE ORGANIZATION BY IMPLEMENTING IMPROVEMENT INITIATIVES THAT WILL RATIONALIZE ROLES AND RESPONSIBILITIES, STREAMLINE PROCESSES, AND IMPROVE THE EXECUTION OF DAY-TO-DAY OPERATIONS.	\$1,111,339.36	\$1,111,339.36	1/4/07	5/31/07	FOLLOW-ON CONTRACT
BOOZ ALLEN HAMILTON INCORPORATED (3626)	CONTRACTOR SUPPORT TO INCREASE THE EFFECTIVENESS OF THE ORGANIZATION BY IMPLEMENTING IMPROVEMENT INITIATIVES THAT WILL RATIONALIZE ROLES AND RESPONSIBILITIES, STREAMLINE PROCESSES, AND IMPROVE THE EXECUTION OF DAY-TO-DAY OPERATIONS.	\$600,000.00	\$600,000.00	1/26/07	5/31/07	FOLLOW-ON CONTRACT
BOOZ ALLEN HAMILTON INCORPORATED (3626)	CONTRACTOR SUPPORT TO INCREASE THE EFFECTIVENESS OF THE ORGANIZATION BY IMPLEMENTING IMPROVEMENT INITIATIVES THAT WILL RATIONALIZE ROLES AND RESPONSIBILITIES, STREAMLINE PROCESSES, AND IMPROVE THE EXECUTION OF DAY-TO-DAY OPERATIONS.	\$165,453.92	\$165,453.92	2/5/07	5/31/07	FOLLOW-ON CONTRACT
BOOZ ALLEN HAMILTON INCORPORATED (3626)	CONTRACTOR SUPPORT TO INCREASE THE EFFECTIVENESS OF THE ORGANIZATION BY IMPLEMENTING IMPROVEMENT INITIATIVES THAT WILL RATIONALIZE ROLES AND RESPONSIBILITIES, STREAMLINE PROCESSES, AND IMPROVE THE EXECUTION OF DAY-TO-DAY OPERATIONS.	\$ 75,000.00	\$ 75,000.00	2/23/07	5/31/07	FOLLOW-ON CONTRACT
BOOZ ALLEN HAMILTON INCORPORATED (3626)	CONTRACTOR SUPPORT TO INCREASE THE EFFECTIVENESS OF THE ORGANIZATION BY IMPLEMENTING IMPROVEMENT INITIATIVES THAT WILL RATIONALIZE ROLES AND RESPONSIBILITIES, STREAMLINE PROCESSES, AND IMPROVE THE EXECUTION OF DAY-TO-DAY OPERATIONS.	\$ 99,535.94	\$ 99,535.94	3/1/07	5/31/07	FOLLOW-ON CONTRACT

BOOZ ALLEN HAMILTON INCORPORATED (3626)	CONTRACTOR SUPPORT TO INCREASE THE EFFECTIVENESS OF THE ORGANIZATION BY IMPLEMENTING IMPROVEMENT INITIATIVES THAT WILL RATIONALIZE ROLES AND RESPONSIBILITIES, STREAMLINE PROCESSES, AND IMPROVE THE EXECUTION OF DAY-TO-DAY OPERATIONS.	\$125,000.00	\$125,000.00	3/21/07	5/31/07	FOLLOW-ON CONTRACT
BOOZ ALLEN HAMILTON INCORPORATED (3626)	CONTRACTOR SUPPORT TO INCREASE THE EFFECTIVENESS OF THE ORGANIZATION BY IMPLEMENTING IMPROVEMENT INITIATIVES THAT WILL RATIONALIZE ROLES AND RESPONSIBILITIES, STREAMLINE PROCESSES, AND IMPROVE THE EXECUTION OF DAY-TO-DAY OPERATIONS.	\$175,000.00	\$175,000.00	3/28/07	5/31/07	FOLLOW-ON CONTRACT
BOOZ ALLEN HAMILTON INCORPORATED (3626)	CONTRACTOR SUPPORT TO INCREASE THE EFFECTIVENESS OF THE ORGANIZATION BY IMPLEMENTING IMPROVEMENT INITIATIVES THAT WILL RATIONALIZE ROLES AND RESPONSIBILITIES, STREAMLINE PROCESSES, AND IMPROVE THE EXECUTION OF DAY-TO-DAY OPERATIONS.	\$532,513.00	\$532,513.00	5/16/07	8/31/07	FOLLOW-ON CONTRACT
BOOZ ALLEN HAMILTON INCORPORATED (3626)	CONTRACTOR SUPPORT TO INCREASE THE EFFECTIVENESS OF THE ORGANIZATION BY IMPLEMENTING IMPROVEMENT INITIATIVES THAT WILL RATIONALIZE ROLES AND RESPONSIBILITIES, STREAMLINE PROCESSES, AND IMPROVE THE EXECUTION OF DAY-TO-DAY OPERATIONS.	\$170,000.00	\$(532,513.00)	8/21/07	9/30/07	FOLLOW-ON CONTRACT
BOOZ ALLEN HAMILTON INCORPORATED (3626)	CONTRACTOR SUPPORT TO INCREASE THE EFFECTIVENESS OF THE ORGANIZATION BY IMPLEMENTING IMPROVEMENT INITIATIVES THAT WILL RATIONALIZE ROLES AND RESPONSIBILITIES, STREAMLINE PROCESSES, AND IMPROVE THE EXECUTION OF DAY-TO-DAY OPERATIONS.	\$122,427.54	\$122,427.54	8/21/07	9/30/07	FOLLOW-ON CONTRACT

CARNEGIE MELLON UNIVERSITY	<p>IA WITH THE NAVY. NAVY WILL DEFINE AND DOCUMENT THE DETAILED FUNCTIONAL REQUIREMENTS OF THE APPLICATION. DEVELOPA PILOT OF THE WEB-BASED APPLICATION FOR POTENTIAL USERS TO TEST USABILITY. INITIATE A PLAN TO GATHER USER REQUIREMENTS FROM THE FIELD AND TSA HQ THROUGH INTERVIEWS OF PERSONNEL AND THROUGH PERFORMANCE TESTING OF THE PILOT WITH PERSONNEL. GATHER REQUIREMENTS THROUGH INTERVIEWS. COMPILE USER REQUIREMENTS INTO USE-CASE DOCUMENTS FOR FURTHER DEVELOPMENT OR CUSTOMIZATION AS NECESSARY.</p> <p>POC: ANDREW COX</p>	\$300,000.00	\$300,000.00	9/28/07	3/28/08	PATENT/DATA RIGHTS
MDI SECURITY SYSTEMS (6358)	MDI/HSPD-12 SYSTEM HEALTH CHECKS.	\$ 74,760.00	\$ 74,760.00	7/3/07	6/30/08	ONLY ONE SOURCE - OTHER
KNOWLEDGE CONSULTING GROUP	<p>ISSO PR - FUNDING TO ASSIGN AN INFORMATION SYSTEM SECURITY OFFICER (ISSO) FROM BPA #HSTS-03-04-A-CIO-038 TO THE INTEGRATED HIRING OPERATIONS & PERSONNEL (IHOP) PROGRAM. THE ISSO WILL BE RESPONSIBLE FOR MAINTAINING THE SECURITY POSTURE OF THE SYSTEM THROUGHOUT ITS LIFECYCLE. DUTIES INCLUDE OVERSIGHT AND IMPLEMENTATION OF IT SECURITY CONTROLS, AND VERIFICATION OF CONTROLS AND COMPLIANCE WITH TSA AND DHS SECURITY REQUIREMENTS. ISSO WILL ALSO BE RESPONSIBLE FOR PRODUCTION OF CERTIFICATION AND ACCREDITATION (C&A) DOCUMENTATION</p> <p>PERIOD OF PERFORMANCE: 1 YEAR (12 MONTHS FROM DATE OF AWARD)</p>	\$176,582.40	\$176,582.40	9/13/07	6/22/11	FOLLOW-ON CONTRACT

UNISYS CORPORATION	<p>THIS PR PROVIDES FUNDING IN SUPPORT OF THE AIR CARGO FREIGHT ASSESSMENT SYSTEM HOSTING REQUIREMENTS FOR A PERIOD OF (8) MONTHS AFTER CONTRACT AWARD. NOTE: SOW AND IGCE IS BEING PROVIDED IN SEPERATE CORRESPONDENCE.</p> <p>PROGRAM POC IS ROBERT E. MOORE, 571-227-3505.</p> <p>CONTRACTING OFFICER IS SUE MESSINA, 571-227-4055. CONTRS ARE BORIS DESOUZA, 571-227-3003 AND KEN CARTER 571-227-1009.</p> <p>CRM AND TECHNICAL POC IS HOLLY BOLGER 571-227-3036.</p>	\$237,422.77	\$237,422.77	8/13/07	8/12/08	ONLY ONE SOURCE - OTHER
UNISYS CORPORATION	<p>THE PURPOSE OF THIS TASK ORDER, HSTS03-07-J-CG0046 TO CONTRACT HSTS03-06-D-CIOS00 IS TO ORDER PREVIOUSLY ACCEPTED CLINS ON THE BRIDGE CONTRACT TO PROVIDE MANAGED SERVICES FOR (31) KSMS SERVERS.</p>	\$587,382.45	\$587,382.45	3/29/07	9/30/07	ONLY ONE SOURCE - OTHER
UNISYS CORPORATION	<p>THIS PR IS FOR UNISYS TO PROVIDE 24X7X365 SECURE VOICE OPERATIONS AND MAINTENACE FOR THE RED SWITCH SERVICE FROM JAN 01, 2007 TO DEC 31, 2007 FOR THE AMOUNT OF \$595,832.4 FOR 12 MONTHS</p>	\$595,832.40	\$595,832.40	12/29/06	12/31/07	ONLY ONE SOURCE - OTHER
UNISYS CORPORATION	O&M FUNDING FOR BRIDGE SERVERS	\$1,052,468.80	\$1,052,468.80	3/23/07	12/31/07	ONLY ONE SOURCE - OTHER
UNISYS CORPORATION	O&M FUNDING FOR BRIDGE SERVERS	\$ 28,081.62	\$ 28,081.62	8/24/07	12/31/07	ONLY ONE SOURCE - OTHER
UNISYS CORPORATION	<p>REQUEST TO ACQUIRE ADDITIONAL ENGINEERING SUPPORT TO ALIEVIATE THE BACKLOG OF OPERATIONS AND MAINTENANCE PROJECTS THAT ARE ON HOLD DUE TO RESOURCE CONSTRAINTS.</p>	\$2,381,624.35	\$2,381,624.35	8/20/07	12/31/07	FOLLOW-ON CONTRACT
UNISYS CORPORATION	<p>THE PURPOSE OF THIS TASK ORDER, HSTS03-07-J-CIO220, TO CONTRACT HSTS03-06-D-CIOS00 IS TO EXPAND VOIP DEPLOYMENT BY QUANTITY AS WELL AS LOCATION, THROUGH ORDERING PREVIOUSLY ACCEPTED CLINS.</p>	\$1,756,240.00	\$1,756,240.00	3/29/07	12/31/07	FOLLOW-ON CONTRACT
UNISYS CORPORATION	TOP UPGRADE	\$ 27,311.90	\$ 27,311.90	8/20/07	12/31/07	ONLY ONE SOURCE - OTHER

UNISYS CORPORATION	INFRASTRUCTURE UPGRADE SUPPORT	\$129,514.00	\$129,514.00	8/20/07	12/31/07	ONLY ONE SOURCE - OTHER
UNISYS CORPORATION	SUPPORT FOR LEGACY CIRCUIT MIGRATION PROJECT (VOICE AND DATA SERVICES)	\$1,294,541.32	\$1,294,541.32	8/23/07	8/15/08	ONLY ONE SOURCE - OTHER
UNISYS CORPORATION	RESEARCH IN MOTION (RIM) TIER 2 T-SUPPORT	\$9,019.59	\$9,019.59	8/15/07	12/31/07	ONLY ONE SOURCE - OTHER
UNISYS CORPORATION	LAX HISOC DEPLOYMENT THE PR IS FOR NEW WORK WHICH INCLUDES PLANNING, SITE PREPARATION, AND INSTALLATION COST FOR THE DEPLOYMENT OF THE TSA APPROVED HI-SOC SOLUTION TO LAX AIRPORT.	\$128,951.84	\$128,951.84	6/14/07	12/31/07	ONLY ONE SOURCE - OTHER
UNISYS CORPORATION	SUN SERVER MAINTENANCE	\$4,332.68	\$4,332.68	8/24/07	12/31/07	ONLY ONE SOURCE - OTHER
UNISYS CORPORATION	UNISYS- STIP PHASE 1	\$446,670.00	\$446,670.00	2/12/07	12/31/07	ONLY ONE SOURCE - OTHER
BOOZ ALLEN HAMILTON INCORPORATED (3626)	FUND PURCHASE ORDER FOR WORK PERFORMED ON 12/1 AND 12/4 RE BAH CONTRACTORS. PLEASE CHARGE TO ACCOUNTING STREAM: TS078A000D 2007 HQA010 GE0000 7700 5100 510 BTC	\$5,957.00	\$5,957.00	12/19/06	12/19/06	FOLLOW-ON CONTRACT
GENERAL DYNAMICS C4 SYSTEMS INCORPORATED	PR IS FOR TACLANE ENCRYPTORS FOR TSOC AND AOF.	\$ 65,850.00	\$ 65,850.00	8/9/07	8/8/08	ONLY ONE SOURCE - OTHER
MULTIMODE SERVICES INCORPORATED	MULTIMODE SERVICES, INC. INSTALLATION, OPERATIONS AND MAINTENANCE OF TSA ALERT. SEE SOW	\$925,000.00	\$2,043,074.00	12/21/06	12/20/07	ONLY ONE SOURCE - OTHER
MIAMI DADE COUNTY	SYSTEMS INNOVATION GROUP THIS PR IS FOR OPTION YEAR 1 (DECEMBER 1, 2006 - NOVEMBER 30, 2007). 90 STRANDS OF SINGLE MODE FIBER OPTIC CABLE LEASED FROM MIAMI-DADE AVIATION TO PROVIDE INTERCONNECTIVITY BETWEEN TSA LAN INFRASTRUCTURES INSTALLED IN THE MIAMI INTERNATIONAL AIRPORT.	\$ 23,663.76	\$ 70,993.68	11/30/06	11/30/09	ONLY ONE SOURCE - OTHER

<p>MIAMI DADE COUNTY</p>	<p>(RATIFICATION) THIS PR COVERS THE USE OF THE AIRPORT'S SINGLE MODE FIBER OPTIC CABLE INFRASTRUCTURE TO INTERCONNECT THE TSA NETWORK BETWEEN ALL OF THE FSD OPERATIONAL AND ADMINISTRATIVE SPACE, WHICH INCLUDES BUT IS NOT LIMITED TO; THE AIRPORT'S FIFTEEN (15) SECURITY CHECKPOINTS, TWO (2) NETWORK TRAINING ROOMS, A NUMBER OF SCREENING BREAK ROOMS, FORTY-EIGHT (48) SEPARATE BAGGAGE SCREENING AREAS, AND TWO INLINE BAGGAGE SCREENING SYSTEMS, NORTH AND SOUTH TERMINAL TO MAKE UP THE MIA LAN FOR HISOC CONNECTIVITY TO THE TSA'S NETWORK CORE CABINET. PERIOD OF PERFORMANCE MAY 2006-NOVEMBER 2006.</p>	<p>\$ 13,804.56</p>	<p>\$ 13,804.56</p>	<p>1/30/07</p>	<p>1/30/07</p>	<p>ONLY ONE SOURCE - OTHER</p>
--------------------------	--	---------------------	---------------------	----------------	----------------	--------------------------------

<p>ALLEGHENY COUNTY AIRPORT AUTHORITY</p>	<p>[PIT] FIBER LEASE WITH ALLEGHENY COUNTY AIRPORT AUTHORITY , PENNSYLVANIA</p> <p>PURPOSE OF THIS STATEMENT OF WORK (SOW) IS TO SET FORTH TSA%U2019S REQUIREMENTS FOR SERVICES FROM THE (ACAA) IN SUPPORT OF TSA%U2019S HIGH SPEED OPERATIONAL CONNECTIVITY (HI-SOC) PROGRAM AT [PIT] INTERNATIONAL AIRPORT.</p> <p>LEASE OF AIRPORTS SINGLE MODE FIBER OPTIC CABLE IS NEEDED TO ENSURE CONTINUOUS NETWORK CONNECTIVITY TO ALL FSD ADMINISTRATIVE AND OPERATIONAL SPACE WITHIN THE PIT AIRPORT. THE PIT TSA NETWORK INFRASTRUCTURE IS INTERCONNECTED BY THE AIRPORT FIBER WHICH PROVIDES HISOC NETWORK CONNECTIVITY BETWEEN THE TSA NETWORK CORE CABINET AND THE AIRPORT'S CHECKPOINTS, TRAINING ROOMS, BREAK ROOM AND OPERATIONAL ADMINISTRATIVE SPACE.</p> <p>7,226 SINGLEMODE FIBER OPTIC AT \$0.21 A FOOT ON ANNUAL BASIS WITH MAINT INCLUDED</p> <p>\$70 INSTALLATION FEE</p>	<p>\$1,517.52</p>	<p>\$1,517.52</p>	<p>1/1/07</p>	<p>12/31/07</p>	<p>ONLY ONE SOURCE - OTHER</p>
---	---	-------------------	-------------------	---------------	-----------------	--------------------------------

<p>GREATER ORLANDO AVIATION AUTHORITY</p>	<p>THIS PR COVERS THE EXISTING LEASE OF TWELVE (12) STRANDS OF FIBER OPTIC CABLE. THIS FIBER LEASE SUPPORTS THE INTERCONNECTIVITY OF THE TSA NETWORK BETWEEN THE AIRPORTS CHECKPOINTS, TRAINING ROOMS, BREAK ROOM AND TSA NETWORK CORE CABINET FOR THE HI-SOC CONNECTIVITY. MONTHLY REOCCURRING CHARGE OF \$552.00.</p> <p>THE ADDITIONAL WORK EXPANDS THE CURRENT LEASE AGREEMENT AND PROVIDES TSA SINGLE MODE FIBER LEASE CAMPUS WIDE, SEVEN CHANNELS DELIVERED TO COMMUNICATION ROOMS SUPPORTING A LAST MILE CONNECTION TO CUSTOMER EQUIPMENT BASED LAN/WAN. THE MONTHLY REOCCURRING CHARGE FOR THE NEW FIBER IS \$805.</p> <p>TOTAL MONTHLY REOCCURRING CHARGE IS \$1357.00.</p> <p>POC: GREATER AVIATION AUTHORITY ATTN: AL ROBINSON 407-825-3500</p> <p>CODE: 001323344 CONTRACT: HSTS03-06-P-C10025</p> <p>THE PERIOD OF PERFORMANCE FOR NEW LEASE COVERS OPTION YEAR 1 - JANUARY 1, 2007 - DECEMBER 31, 2007.</p>	<p>\$ 16,284.00</p>	<p>\$ 54,840.00</p>	<p>12/28/06</p>	<p>12/31/09</p>	<p>ONLY ONE SOURCE - OTHER</p>
---	---	---------------------	---------------------	-----------------	-----------------	--------------------------------

<p>GREATER ORLANDO AVIATION AUTHORITY</p>	<p>THIS PR COVERS THE EXISTING LEASE OF TWELVE (12) STRANDS OF FIBER OPTIC CABLE. THIS FIBER LEASE SUPPORTS THE INTERCONNECTIVITY OF THE TSA NETWORK BETWEEN THE AIRPORTS CHECKPOINTS, TRAINING ROOMS, BREAK ROOM AND TSA NETWORK CORE CABINET FOR THE HI-SOC CONNECTIVITY. MONTHLY REOCCURRING CHARGE OF \$552.00.</p> <p>THE ADDITIONAL WORK EXPANDS THE CURRENT LEASE AGREEMENT AND PROVIDES TSA SINGLE MODE FIBER LEASE CAMPUS WIDE, SEVEN CHANNELS DELIVERED TO COMMUNICATION ROOMS SUPPORTING A LAST MILE CONNECTION TO CUSTOMER EQUIPMENT BASED LAN/WAN. THE MONTHLY REOCCURRING CHARGE FOR THE NEW FIBER IS \$805.</p> <p>TOTAL MONTHLY REOCCURRING CHARGE IS \$1357.00.</p> <p>POC: GREATER AVIATION AUTHORITY ATTN: AL ROBINSON 407-825-3500</p> <p>CODE: 001323344 CONTRACT: HST503-06-P-CIO025</p> <p>THE PERIOD OF PERFORMANCE FOR NEW LEASE COVERS OPTION YEAR 1 - JANUARY 1, 2007 - DECEMBER 31, 2007.</p>	<p>\$1,317.00</p>	<p>\$4,485.00</p>	<p>7/16/07</p>	<p>12/31/09</p>	<p>ONLY ONE SOURCE - OTHER</p>
---	---	-------------------	-------------------	----------------	-----------------	--------------------------------

<p>HILLSBOROUGH COUNTY AVIATION AUTHORITY</p>	<p>PR FOR ONE YEAR OF LEASED SINGLE MODE FIBER OPTIC FROM THE HILLSBOROUGH COUNTY AVIATION AUTHORITY IN SUPPORT OF THE HIGH SPEED OPERATIONAL CONNECTIVITY (HI-SOC) PROGRAM AT THE TAMPA INTERNATIONAL AIRPORT (TPA).</p> <p>VENDOR: HILLSBOROUGH COUNTY AVIATION AUTHORITY.</p> <p>HI-SOC SPEND PLAN HI-SOC O & M FIBER LEASE</p> <p>PL: BARBARA SHOWELL 571-227-2442 ACQUISITION: BRANDON PRINDLE - 571-227-3002 COTR - NYAL PIPER - 571-227-3711</p>	<p>\$ 12,000.00</p>	<p>\$ 39,720.00</p>	<p>5/15/07</p>	<p>5/31/10</p>	<p>ONLY ONE SOURCE - OTHER</p>
---	---	---------------------	---------------------	----------------	----------------	--------------------------------

<p>SANFORD AIRPORT AUTHORITY</p>	<p>HISOC SPEND PLAN; HISOC O & M; HISOC FIBER LEASES</p> <p>THIS PR COVERS FIBER LEASE FROM SANFORD AIRPORT AUTHORITY FOR THE USE OF HISOC.</p> <p>TSA REQUESTS SANFORD AIRPORT AUTHORITY PROVIDE TSA A TOTAL OF SIX (6) STRANDS OF SINGLE-MODE (SM) FIBER OPTIC CABLE, WITH ASSOCIATED FIBER CROSS CONNECTIONS, AND USE OF ONE SANFORD AIRPORT AUTHORITY CONDUIT TO SUPPORT TSA COMMUNICATIONS CONNECTIVITY REQUIREMENTS AT SFB. SPECIFICALLY:</p> <p>A. TWO (2) STRANDS OF SM FIBER SHALL BE EXTENDED FROM THE SAA COMMUNICATION CLOSET TO TERMINAL B BAGGAGE BETWEEN IT EQUIPMENT IN DOMESTIC BAGGAGE. DISTANCE OF EACH STRAND SHALL BE DETERMINED BY SAA.</p> <p>B. TWO (2) STRANDS OF SM FIBER SHALL BE EXTENDED FROM THE SAA COMMUNICATION CLOSET TO TERMINAL B CHECKPOINT IT CABINET IN THE SECURITY OFFICE. DISTANCE OF EACH STRAND SHALL BE DETERMINED BY SAA.</p> <p>C. TWO (2) STRANDS OF SM FIBER SHALL BE EXTENDED FROM SAA COMMUNICATION CLOSET TO TERMINAL A CHECKPOINT IT CABINET IN THE PASSENGER SCREENING SUPERVISOR OFFICE. THE DISTANCE OF EACH STRAND SHALL BE DETERMINED BY SAA.</p> <p>D. THE LEASE COST OF EACH FIBER RUN/CONNECTION OF THE SIX (6) STRANDS OF SM FIBER OPTIC CABLE REQUIRED IS @ \$30.00 PER CONNECTION X 3 = \$90.00 PER MONTH. TOTAL ANNUAL COST IS \$1,080.00 PER YEAR.</p> <p>THE SANFORD AIRPORT AUTHORITY AGREES TO BE RESPONSIBLE FOR MAINTENANCE AND REPAIR OF THE SIX (6) STRANDS OF SM FIBER OPTIC CABLE AND ASSOCIATED FACILITIES.</p> <p>VENDOR POC:</p>	<p>\$2,580.00</p>	<p>\$4,920.00</p>	<p>5/11/07</p>	<p>5/31/10</p>	<p>ONLY ONE SOURCE - OTHER</p>
--------------------------------------	--	-------------------	-------------------	----------------	----------------	--------------------------------

<p>MIAMI DADE COUNTY</p>	<p>THIS PR IS REQUIRED TO COVER THE COST TO PROVIDE AND INSTALL ADDITIONAL FIBER FOR THE HI-SPEED CONNECTIVITY PROJECT. PROVIDE, INSTALL, TERMINATE AND TEST TWO (2) STRANDS OF SINGLE MODE FIBER FROM THE TSA ROOM E3688 TO TWELVE LOCATIONS. CURRENT LEASE EXISTS UNDER CONTRACT HSTS03-07-P-CIO020.</p> <p>MIAMI DADE COUNTY ATTN: JOAN NUNEZ 4200 N.W. 36TH ST MIAMI, FL 3315-92616 3 0 5 - 8 7 6 - 8 4 9 3</p> <p>PROJECT LEAD: BARBARA SHOWELL 571-227-2442 CONTRACT SPECIALIST: BRANDON PRINDLE 571-227-3002</p>	<p>\$117,164.79</p>	<p>\$167,158.23</p>	<p>6/11/07</p>	<p>9/30/10</p>	<p>ONLY ONE SOURCE - OTHER</p>
<p>COMPUTER SCIENCES CORPORATION (3126)</p>	<p>ATTN: SUE MESSINA (CO)</p> <p>[SOW NOT REQUIRED FOR THIS COMSEC RELATED HARDWARE REQUEST]. OTHER SUPPORT DOCUMENTATION TO BE PROVIDED TO TSA BUY TEAM.</p> <p>THIS REQUEST IS TO OBTAIN HARDWARE DESCRIBED AS THREE (3) LOCAL MANAGEMENT DEVICES (LMD) WORK STATIONS IN THE AMOUNT OF \$16,300 EACH. SUBTOTAL AMOUNTS TO \$49,900. S&H IS \$1,200 PER SITE BRINGING THE TOTAL TO \$52,500.</p> <p>THIS IS A ONE TIME PURCHASE TO SUPPORT TSA%U2019S REQUIREMENT TO ESTABLISH LMD ONLY ACCOUNTS AT THE THREE REGIONAL COMSEC LOCATIONS PHILADELPHIA, PA; SAN ANTONIO, TX; AND LOS ANGELES, CA.</p> <p>PORTFOLIO COST CODE: IT SECURITY COMPLIANCE, AUDIT TEAM</p> <p>CONTACT JILL VAUGHAN ON 571-227-2034 FOR QUESTIONS ON THIS ORDER.</p>	<p>\$ 44,100.00</p>	<p>\$ 44,100.00</p>	<p>8/27/07</p>	<p>8/26/08</p>	<p>ONLY ONE SOURCE - OTHER</p>

<p>HOUSTON CITY OF (1164)</p>	<p>FIBER LEASE FOR IAH/HOU</p> <p>THE PR IS FOR NEW WORK WHICH INCLUDES PLANNING, SITE PREPARATION, INSTALLATION AND INITIAL O&M COST FOR THE DEPLOYMENT OF THE TSA APPROVED HI-SOC SOLUTION TO GEORGE BUSH INTERCONTINENTAL AIRPORT (IAH) HOUSTON, TX.</p> <p>POC EVERETT KENNEDY 571-227-1043</p> <p>HISOC SPEND PLAN HISOC O & M FIBER LEASES</p>	<p>\$ 15,840.00</p>	<p>\$ 47,520.00</p>	<p>8/17/07</p>	<p>7/31/10</p>	<p>ONLY ONE SOURCE - OTHER</p>
-------------------------------	--	---------------------	---------------------	----------------	----------------	--------------------------------

<p>RHODE ISLAND AIRPORT CORPORATION (1772)</p>	<p>HI-SOC SPEND PLAN HI-SOC O&M FIBER LEASES</p> <p>SERVICE PROCURED IS FOR LEASED USE OF SINGLE MODE FIBER OPTIC FROM RIAC TO PROVIDE INTERCONNECTIVITY BETWEEN TSA LAN INFRASTRUCTURES INSTALLED IN THE PVD INTERNATIONAL AIRPORT.</p> <p>THE FIBER IN QUESTION HAS END POINTS AT THE RIAC COMMUNICATIONS ROOM BENEATH THE CHECKPOINT AND THE ELECTRICAL CLOSET ACROSS FROM THE TSA LOCKER SPACE. THE DISTANCE IS APPROXIMATELY 800 FEET TIMES TWO (2) STRANDS FOR A GRAND TOTAL OF 1600. THE ENDPOINTS ARE BOTH IN LIMITED ACCESS, LOCKED ROOMS, AND THE FIBER IS NOT VISIBLE ALONG THE PATH; THEREFORE, SECURITY IS NOT AN ISSUE. TSA WILL NEED ACCESS TO THE RIAC SECURE SPACE FROM TIME TO TIME FOR MAINTENANCE ISSUES.</p> <p>TSA SHALL LEASE THE FOLLOWING LENGTHS OF SINGLE MODE FIBER FROM RIAC:</p> <p>APPROX 800' X 2 STRANDS FOR A TOTAL OF 1,600' U2019</p> <p>PM & TECHNICAL BARBARA SHOWELL & DANIN JOHNSON PRIMARY POINT OF CONTACT 601 SOUTH 12TH STREET ARLINGTON, VA 22202 PHONE: (571) 227-2442 & (202) 320 1255</p> <p>MEGAN DAKE CONTRACTING OFFICER%U2019S TECHNICAL REPRESENTATIVE (COTR) 601 SOUTH 12TH STREET ARLINGTON, VA 22202 PHONE: (202) 997-4374 / FAX (304) 594-1722</p> <p>ACQUISITION BRANDON PRINDLE CONTRACT SPECIALIST 601 SOUTH 12TH STREET ARLINGTON, VA 22202 PHONE: (571) 227-3002 FAX: (571) 227-2913 BRANDON.PRINDLE@DHS.GOV</p>	<p>\$1,200.00</p>	<p>\$3,600.00</p>	<p>6/22/07</p>	<p>6/30/08</p>	<p>ONLY ONE SOURCE - OTHER</p>
--	--	-------------------	-------------------	----------------	----------------	--------------------------------

Congressional Quarterly	RENEWAL OF CQ.COM ON CONGRESS & CQ WEEKLY	\$ 23,151.00	\$ 23,151.00	2/13/07	2/12/08	ONLY ONE SOURCE - OTHER
0	Purchase of legal reference books from publisher, Dewey Publications, per list provided to CO	\$ 12,099.90	\$ 12,099.90	9/20/07	1/0/00	ONLY ONE SOURCE - OTHER
WEST PUBLISHING CORPORATION	WEST SUBSCRIPTION SERVICE	\$ 52,549.09	\$ 52,549.09	6/21/07	9/30/07	UNIQUE SOURCE
GPS INTERNATIONAL TECHNOLOGIES INCORPORATED	5 FS1 PACKAGE 2; FS1 TRACKER WITH 3.6 AH BATTERY; BATTERY CHARGER AND SLAP N STICK DEPLOYMENT CASE 1 LE15.000 SHARED PLAN: 15,000 LOCATES PER MONTH SHARED BETWEEN 5 DEVICES ONLY FOR 1 YR. OVERAGE LOCATES BILLED AT .15 PER 5 ONE-TIME NETWORK ACTIVATION FEE 1 FEDEX 2ND DAY SHIPPING	\$8,052.24	\$8,052.24	4/25/07	6/27/07	ONLY ONE SOURCE - OTHER
ICS CONTRACT SERVICES LIMITED LIABILITY COMPANY	PR - THIS IS A SHORT TERM EXTENSION TO CONTRACT HSTS03-06-P-RES282 FOR FOUR MONTHS OF JANITORIAL SERVICE AT ATLANTA, GA (ATL) AIRPORT LOCATION UNTIL THE SPACE CAN BE ADDED TO THE GSA LEASE. POP FROM 11/1/06 TO 03/01/07	\$ 16,046.52	\$ 16,046.52	11/2/06	1/31/07	ONLY ONE SOURCE - OTHER
B AND B ARMR CORPORATION	PR PROVIDES FUNDING FOR ANNUAL MAINTENANCE FOR FOUR (4) NASATKA SURFACE MOUNT BARRIERS IN SUPPORT OF ACCESS CONTROL AT TSA HQ GATED ENTRANCES. PHYSICAL SECURITY IS MARTY HOROWITZ AT 571-227-1191.	\$8,840.00	\$8,840.00	9/20/07	9/23/08	AUTHORIZED BY STATUTE
MEDECO SECURITY LOCKS INCORPORATED	PR PROVIDE FUNDS TO PURCHASE MEDECO LOCKSETS, REMOVABLE CORES, CUT KEYS AND STAMPING KEYS FOR INSTALLATION AT TSA HQ AND FREEDOM CENTER. PHYSICAL SECURITY POC IS MARTY HOROWITZ AT 571-227-1191.	\$ 30,914.67	\$ 30,914.67	8/24/07	11/5/07	ONLY ONE SOURCE - OTHER
OAG WORLDWIDE	OAG DATABASE SUBSCRIPTION	\$ 43,826.00	\$ 43,826.00	6/25/07	8/31/07	ONLY ONE SOURCE - OTHER
OAG WORLDWIDE	OAG DATABASE SUBSCRIPTION	\$ 45,140.00	\$ 45,140.00	7/31/07	8/31/08	ONLY ONE SOURCE - OTHER
Duluth Airport Authority	INSTALLATION OF BAGGAGE SCREENING EQUIPMENT FOR TWO REVEAL CT80 EQUIPMENT AT DULUTH INTERNATIONAL AIRPORT. Adding \$50,000 to the OTA>	\$ 50,000.00	\$ 50,000.00	2/26/07	12/31/07	ONLY ONE SOURCE - OTHER

City of Duluth	INSTALLATION OF BAGGAGE SCREENING EQUIPMENT FOR TWO REVEAL CT-80 EQUIPMENT. MODIFICATIONS TO BHS SECURITY SYSTEMS TO MEET TSA REQUIREMENTS Modification to existing OTA	\$153,000.00	\$853,000.00	6/25/07	12/31/07	ONLY ONE SOURCE - OTHER
Duluth Airport Authority	Funding modification to existing OTA with Duluth Airport Authority for inline baggage screening system.	\$177,000.00	\$1,030,000.00	9/14/07	1/0/00	ONLY ONE SOURCE - OTHER
INVISION TECHNOLOGIES INCORPORATED	SERVICES ASSOCIATED WITH ATL NORTH AND SOUTH TERMINALS WITH MULTIPLEXING CAPABILITY	\$ 78,190.00	\$ 78,190.00	2/22/07	2/22/07	UNIQUE SOURCE
L-3 COMMUNICATIONS SECURITY AN	PROVIDE FOR NEDS INTEGRATION OF 14 EXAMINER EDS AT LAS MODES 3 & 4	\$361,402.81	\$361,402.81	6/27/07	6/30/08	ONLY ONE SOURCE - OTHER
L-3 COMMUNICATIONS SECURITY AN	INTEGRATE 4 EDS EXAMINER EDS AT OKC	\$ 66,061.65	\$ 66,061.65	9/5/07	2/28/08	ONLY ONE SOURCE - OTHER
L-3 COMMUNICATIONS SECURITY AN	INTEGRATES 3 EXAMINER EDS AT KEAHOLE INTL AIRPORT	\$ 98,541.56	\$ 98,541.56	8/3/07	9/30/07	ONLY ONE SOURCE - OTHER
L-3 COMMUNICATIONS SECURITY AN	NEDS INTEGRATION OF 31 UNITS AT PHX, OSR ROOM FURNITURE, RIGGING FOR RECEIPT DELIVERY, SHORT TERM STORAGE AND PLACEMENT IN BAG ROOM AT PHX	\$ 54,520.00	\$ 54,520.00	7/17/07	8/28/07	NATIONAL SECURITY
A B Won PAT Guam International Airport Authority	ADD FUNDING TO GUM OTA TO PROVIDE ADDITIONAL IN-LINE SCREENING CAPABILITY FOR ORIGINATING CHECKED BAGGAGE	\$407,500.00	\$2,329,000.00	8/17/07	11/30/08	ONLY ONE SOURCE - OTHER
RENO TAHOE AIRPORT AUTHORITY	RENO-TAHOE AIRPORT AUTHORITY AGREEMENT HSTS0406ADEP393; ADD FUNDING TO EXISTING RNO OTA FOR ENHANCEMENTS TO MEET BSIS REQUIREMENTS RELATING TO BHS DESIGN AND CONSTRUCTION	\$5,000,000.00	\$12,000,000.00	8/24/07	5/31/09	ONLY ONE SOURCE - OTHER
Kenton County Airport Board	Funding modification to existing OTA for CVG, HSTS04-06-A-DEP405	\$6,078,000.00	\$9,128,000.00	9/12/07	10/31/09	ONLY ONE SOURCE - OTHER
Capital Region Airport Commission	Funding Modification to HSTS04-06-A-DEP480	\$300,000.00	\$300,000.00	3/19/07	12/31/07	ONLY ONE SOURCE - OTHER
L-3 COMMUNICATIONS SECURITY AN	MODIFICATION OF 4 EDS UNITS	\$161,444.47	\$161,444.47	9/13/07	3/31/08	NATIONAL SECURITY
L-3 COMMUNICATIONS CORPORATION (4475)	PREVENTIVE AND CORRECTIVE MAINTENANCE FOR EDS AND LINESCAN EQUIPMENT	\$ 85,716.00	\$ 85,716.00	1/17/07	3/10/07	ONLY ONE SOURCE - OTHER
L-3 COMMUNICATIONS SECURITY AN	INTEGRATES 45 EXPLOSIVE DETECTION SYSTEMS AT ATL	\$900,075.69	\$900,075.69	8/17/07	2/28/08	ONLY ONE SOURCE - OTHER
L-3 COMMUNICATIONS SECURITY AN	INTEGRATES 45 EXPLOSIVE DETECTION SYSTEMS AT ATL	\$ 48,445.58	\$ 48,445.58	8/3/07	9/30/07	NATIONAL SECURITY
L-3 COMMUNICATIONS SECURITY AN	FUNDING FOR DECOMMISSION AND REMOVAL OF EDS UNITS	\$430,562.15	\$430,562.15	9/20/07	6/30/08	NATIONAL SECURITY
L-3 COMMUNICATIONS SECURITY AN	UPGRADE AND NEDS OF 8 EDS UNITS	\$ 44,240.84	\$ 44,240.84	8/24/07	12/31/07	NATIONAL SECURITY

INVISION TECHNOLOGIES INCORPORATED	EDS EQUIPMENT AND SERVICES	\$ 46,800.00	\$ 46,800.00	8/28/07	8/28/07	UNIQUE SOURCE
SMITHS DETECTION TORONTO LIMITED	PROVIDE CONSUMABLES FOR 25 UNITS	\$5,415.85	\$5,415.85	1/10/07	2/28/07	ONLY ONE SOURCE - OTHER
SMITHS DETECTION TORONTO LIMITED	PROVIDE CONSUMABLES FOR 25 UNITS	\$ 12,976.67	\$ 12,976.67	3/7/07	6/29/07	ONLY ONE SOURCE - OTHER
DENVER INTERNATIONAL AIRPORT (DIA)	REQUEST TO PROCESS OTA FOR DENVER INTERNATIONAL AIRPORT (DIA) TO PURCHASE AND INSTALL CLOSED CIRCUIT TV SYSTEM	\$1,691,064.60	\$41,691,064.60	6/26/07	6/30/08	ONLY ONE SOURCE - OTHER
City of Chicago	REQUEST TO PROCESS OTA FOR CHICAGO INTERNATIONAL AIRPORT (ORD) TO PURCHASE AND INSTALL CLOSED CIRCUIT TV (CCTV) SYSTEM	\$1,400,000.00	\$1,400,000.00	5/24/07	5/31/08	ONLY ONE SOURCE - OTHER
Port of Seattle	REQUEST TO PROCESS OTA FOR SEATTLE TACOMA INTERNATIONAL AIRPORT (SEA) TO PURCHASE AND INSTALL CLOSED CIRCUIT TV (CCTV) SYSTEM	\$2,000,000.00	\$2,000,000.00	2/6/07	2/6/08	ONLY ONE SOURCE - OTHER
Niagra Frontier Transportation Authority	REQUEST TO PROCESS OTA FOR BUFFALO NIAGARA INTERNATIONAL AIRPORT TO PURCHASE AND INSTALL CCTV SYSTEM FOR BUF.	\$680,693.00	\$680,693.00	2/20/07	2/20/08	ONLY ONE SOURCE - OTHER
Memphis-Shelby County Airport Authority	REQUEST TO PROCESS OTA FOR MEMPHIS-SHELBY COUNTY AIRPORT AUTHORITY (MSCAA) TO PURCHASE AND INSTALL CLOSED CIRCUIT TV (CCTV) SYSTEM FOR MEM.	\$657,250.00	\$657,250.00	1/30/07	1/30/08	ONLY ONE SOURCE - OTHER
City of Atlanta	HARTSFIELD-JACKSON ATLANTA INTERNATIONAL AIRPORT TO PURCHASE AND INSTALL CLOSED CIRCUIT TV SYSTEM. ENVIRONMENTAL AND TECHNICAL SERVICES	\$1,987,682.00	\$1,987,682.00	6/11/07	6/30/08	ONLY ONE SOURCE - OTHER
San Diego County Regional Airport	REQUEST TO PROCESS OTA FOR SAN DIEGO INTERNATIONAL AIRPORT TO PURCHASE AND INSTALL CLOSED CIRCUIT TV	\$713,497.00	\$713,497.00	5/29/07	5/31/08	ONLY ONE SOURCE - OTHER
A. B. Won Pat Guam International Airport Authority	REQUEST TO PROCESS OTA FOR GUAM INTERNATIONAL AIRPORT AUTHORITY FOR INCREMENTAL FUNDS TO COMPLETE ACQUISITION FOR CLOSED CIRCUIT TV (CCTV) SYSTEM. Funding will be added via a modification to existing OTA.	\$243,000.00	\$618,838.00	5/31/07	4/30/08	ONLY ONE SOURCE - OTHER
Ted Stevens Anchorage International Airport	OTA for Ted Stevens Anchorage International Airport (ANC) to purchase and install Closed Circuit TV (CCTV) system.	\$220,000.00	\$220,000.00	3/13/07	3/31/08	ONLY ONE SOURCE - OTHER
COMMONWEALTH PORTS AUTHORITY	REQUEST TO PROCESS OTA FOR SAIPAN INTERNATIONAL AIRPORT (GSN) TO PURCHASE AND INSTALL CLOSED CIRCUIT TV SYSTEM	\$300,000.00	\$300,000.00	4/16/07	5/30/07	ONLY ONE SOURCE - OTHER

The Port Authority of New York and New Jersey	PROVIDE FUNDING FOR THE DESIGN AND DEPLOYMENT OF CLOSED CIRCUIT TELEVISION (CCTV) CAMERAS AND A DIGITAL VIDEO RECORDING SYSTEM FOR THE PASSENGER SCREENING CHECKPOINTS AT LGA, JFK, AND EWR AIRPORTS	\$5,000,000.00	\$5,000,000.00	8/9/07	8/31/09	ONLY ONE SOURCE - OTHER
County of Sacramento	PROVIDE FUNDING FOR A CLOSED CIRCUIT TELEVISION (CCTV) SYSTEM AT SMF	\$567,989.00	\$567,989.00	9/19/07	9/30/12	ONLY ONE SOURCE - OTHER
City of Austin	PROVIDE FUNDING FOR A CLOSED CIRCUIT TELEVISION (CCTV) SYSTEM AT AUSTIN-BERGSTROM INTERNATIONAL AIRPORT (AUS)	\$973,632.00	\$973,632.00	5/29/07	5/31/08	ONLY ONE SOURCE - OTHER
Puerto Rico Ports Authority	PUERTO RICO PORTS AUTHORITY INSTALLATION OF CCTV SURVEILLANCE SYSTEMS AT THE LUIS MUNOZ MARIN INTERNATIONAL AIRPORT (SIU) IN SAN JUAN, PUERTO RICO.	\$842,876.00	\$842,876.00	6/11/07	6/30/08	ONLY ONE SOURCE - OTHER
LOUISVILLE REGIONAL AIRPORT AUTHORITY	REQUEST TO PROCESS OTA FOR LOUISVILLE REGIONAL AIRPORT AUTHORITY (SDFA) TO PURCHASE AND INSTALL CLOSED CIRCUIT TV (CCTV) SYSTEM	\$259,000.00	\$259,000.00	8/17/07	8/31/08	ONLY ONE SOURCE - OTHER
Dallas Fort Worth International Airport Board	PROVIDE FUNDING FOR IDENTIFICATION OF STRATEGIC CAMERA LOCATIONS, DETERMINING REQUIREMENTS FOR EACH LOCATION AND IDENTIFY CAMERAS THAT MEET EACH LOCATION REQUIREMENT. INSTALL SELECTED CAMERAS INTO THE EXISTING SURVEILLANCE SYSTEM AND INTEGRATE IN MRC CONTROL PROCESSES OF THE CURRENT ENVIRONMENT	\$2,000,000.00	\$2,000,000.00	8/13/07	8/31/08	ONLY ONE SOURCE - OTHER
Austin Straubel International Airport	PROVIDE AND INSTALL SPECTRA IV PAN-TILT-ZOOM CAMERAS AND DF5 DOME PACKS AT TWO CHECKPOINTS AND AIRLINE TICKET COUNTERS AT GRB	\$198,586.00	\$198,598.00	8/24/07	8/31/07	ONLY ONE SOURCE - OTHER
State of Alaska Dept of Tran & Public Facilities	Expansion of CCTV system at Fairbanks International Airport (FAI).	\$617,217.00	\$617,217.00	8/21/07	8/31/09	ONLY ONE SOURCE - OTHER
Airport Authority for MSY	ELECTRICAL WORK FOR SCREENING EQUIPMENT IN BAGGAGE CLAIM AREA OF NEW ORLEANS INTERNATIONAL AIRPORT (MSY)	\$ 20,000.00	\$ 20,000.00	4/26/07	4/30/08	ONLY ONE SOURCE - OTHER
Norfolk Airport Authority	PROVIDE ELECTRICAL POWER FOR THE INSTALLATION OF 5 REVEAL CT80 REDUCED SIZE EDS (RS-EDS) AT NORFOLK INTERNATIONAL AIRPORT, TERMINAL LOBBY AREA	\$ 55,000.00	\$ 55,000.00	4/6/07	9/30/07	ONLY ONE SOURCE - OTHER

Metropolitan Washington Airports Authority	METROPOLITAN WASHINGTON AIRPORTS AUTHORITY OTA IAD SOUTH BAGROOM OTA FOR CONSTRUCTION OF AN IN-LINE SYSTEM. CONSTRUCTION COSTS OF BHS & INFRASTRUCTURE IMPROVEMENTS	\$33,000,000.00	\$33,000,000.00	9/10/07	9/30/09	ONLY ONE SOURCE - OTHER
Broward County	Funding modification to existing OTA for FLL.	\$8,450,000.00	\$18,450,000.00	9/12/07	6/30/10	ONLY ONE SOURCE - OTHER
Broward County	BROWARD COUNTY AVIATION DEPARTMENT OTA FORT LAUDERDALE-HOLLYWOOD INTERNATIONAL AIRPORT FLL TERMINAL 1 OTA FOR CONSTRUCTION FOR AN IN-LINE SYSTEM. CONSTRUCTION COSTS OF BHS & INFRASTRUCTURE IMPROVEMENTS	\$10,000,000.00	\$10,000,000.00	9/5/07	12/31/09	ONLY ONE SOURCE - OTHER
City of Des Moines	PROVIDE FUNDING TO DES MOINES AIRPORT FOR PRODUCING A SCHEMATIC DESIGN FOR A 2 EDS IN-LINE SYSTEM FOR CHECKED BAGGAGE SCREENING	\$ 24,000.00	\$ 24,000.00	6/11/07	12/31/07	ONLY ONE SOURCE - OTHER
Dane County, Wisconsin	PROVIDE FUNDING TO DANE COUNTY REGIONAL AIRPORT TO PRODUCE CONCEPT LAYOUT AND COST ESTIMATE FOR 4 EDS SYSTEMS FOR SCREENING CHECKED BAGGAGE.	\$ 14,000.00	\$ 14,000.00	8/21/07	8/31/08	ONLY ONE SOURCE - OTHER
Raleigh Durham Airport Authority	RALEIGH DURHAM AIRPORT AUTHORITY OTA RDU OTA FOR CONSTRUCTION OF AN IN-LINE SYSTEM	\$7,000,000.00	\$7,000,000.00	7/19/07	3/31/11	ONLY ONE SOURCE - OTHER
Port of Portland	PDX (PORTLAND, OREGON) OTA FOR DESIGN AND CONSTRUCTION OF AN IN-LINE SYSTEM	\$5,000,000.00	\$5,000,000.00	9/10/07	12/31/10	ONLY ONE SOURCE - OTHER
City of Des Moines	PROVIDE FUNDING TO DES MOINES INTERNATIONAL AIRPORT TO COMPLETE IN-LINE SYSTEM DESIGN, PRODUCE BIDDING PACKAGE, AND CONSTRUCT AND COMMISSION AND IN-LINE SYSTEM SECURITY SYSTEM FOR CHECKED BAGGAGE SCREENING AT DES MOINES INTERNATIONAL AIRPORT	\$2,000,000.00	\$3,000,000.00	9/12/07	12/31/09	ONLY ONE SOURCE - OTHER
CITY OF DES MOINES	ADDITIONAL FUNDING PR FOR OTA WITH CITY OF DES MOINES. SEE ALSO PR 2107207DEP367	\$1,000,000.00	\$3,000,000.00	9/12/07	12/31/09	ONLY ONE SOURCE - OTHER
San Francisco	OTA for modifications/construction to Terminal 1 baggage screening system at SFO	\$2,600,000.00	\$2,600,000.00	9/12/07	12/31/08	ONLY ONE SOURCE - OTHER
Spectrum San Diego Inc.	To purchase up to 40 CPI units for deployment at federalized airports. (Replaces PR 2107207DEP431)	\$1,700,000.00	\$37,234,156.55	9/25/07	9/23/12	ONLY ONE SOURCE - OTHER

INVISION TECHNOLOGIES INCORPORATED	PURCHASE OF VARIOUS EQUIPMENT OF 20 FLAT POWERED CONVEYORS, 1 MUX NETWORK, 1 NETWORK PRINTER, 6 PTRI WORKSTATION, PTRI MOUNTING KITS & 6 BARCODE SCANNERS	\$983,500.00	\$983,500.00	3/12/07	9/30/07	UNIQUE SOURCE
INVISION TECHNOLOGIES INCORPORATED	PURCHASE OF VARIOUS EQUIPMENT OF 20 FLAT POWERED CONVEYORS, 1 MUX NETWORK, 1 NETWORK PRINTER, 6 PTRI WORKSTATION, PTRI MOUNTING KITS & 6 BARCODE SCANNERS	\$ 89,207.00	\$ 89,207.00	8/2/07	9/30/07	UNIQUE SOURCE
L-3 COMMUNICATIONS SECURITY AN	EQUIPMENT RELOCATION	\$170,317.10	\$170,317.10	8/8/07	9/30/07	ONLY ONE SOURCE - OTHER
L-3 COMMUNICATIONS SECURITY AN	EQUIPMENT RELOCATION	\$173,522.80	\$173,522.80	9/28/07	1/31/08	ONLY ONE SOURCE - OTHER
L-3 COMMUNICATIONS SECURITY AN	TO ORDER TO UPGRADE L-3 EDS MACHINES AT WASHINGTON DULLES INTERNATIONAL AIRPORT (IAD).	\$ 67,707.06	\$352,000,000.00	7/11/07	10/9/07	ONLY ONE SOURCE - OTHER
L-3 COMMUNICATIONS SECURITY AN	IN ORDER TO PROVIDE FUNDING FOR THE NEDS OF 3 UNITS AT WILLIAM P HOBBY INTERNATIONAL AIRPORT (HOU)	\$110,433.28	\$352,000,000.00	7/18/07	12/31/07	ONLY ONE SOURCE - OTHER
INVISION TECHNOLOGIES INCORPORATED	DECOMMISSION OF 1 CTX 5500	\$151,652.00	\$151,652.00	5/9/07	8/15/07	UNIQUE SOURCE
L 3 COMMUNICATIONS CORPORATION (4475)	L-3- EBSP EXCEPTED MAINTENANCE	\$ 12,543.69	\$ 12,543.69	6/1/07	6/30/07	ONLY ONE SOURCE - OTHER
L 3 COMMUNICATIONS CORPORATION (4475)	L-3- EBSP EXCEPTED MAINTENANCE	\$487,456.31	\$487,456.31	7/10/07	6/30/07	ONLY ONE SOURCE - OTHER
L-3 COMMUNICATIONS SECURITY AN	REMOVE (1) LOT 1 EDS AND REPLACE WITH EXISTING LOT 2 EDS AT BWI	\$123,017.47	\$123,017.47	8/14/07	10/31/07	FOLLOW-ON CONTRACT
L-3 COMMUNICATIONS SECURITY AN	REMOVE (1) LOT 1 EDS AND REPLACE WITH EXISTING LOT 2 EDS AT BWI	\$472,407.46	\$472,407.46	9/24/07	8/31/08	FOLLOW-ON CONTRACT
L-3 COMMUNICATIONS SECURITY AN	PHASE C OF THE NEDS PROJECT FOR THE CENTRAL WEST POD EDS INSTALLATION AT MCO.	\$1,638,209.43	\$1,638,209.43	8/27/07	6/30/08	ONLY ONE SOURCE - OTHER
L-3 COMMUNICATIONS SECURITY AN	REFURBISHMENT OF FIVE (5) LOT 2, L3 EDS UNITS.	\$3,569,948.39	\$3,569,948.39	9/17/07	7/31/08	ONLY ONE SOURCE - OTHER
L 3 COMMUNICATIONS CORPORATION (4475)	THE PURPOSE OF THIS DELIVERY ORDER 014 IS TO PURCHASE X-RAY TUBES FOR THE PREVENTIVE AND CORRECTIVE MAINTENANCE FOR EXAMINER 6000 EXPLOSIVE DETECTION SYSTEMS.	\$2,062,500.00	\$2,062,500.00	8/15/07	3/10/08	ONLY ONE SOURCE - OTHER
L-3 COMMUNICATIONS SECURITY AN	INSTALLATION OF (4) L3 6000 UNITS AT LIH.	\$948,861.80	\$948,861.80	9/5/07	6/30/08	ONLY ONE SOURCE - OTHER
L-3 COMMUNICATIONS SECURITY AN	TO INSTALL TWENTY-FOUR (24) METER WIDE TUNNELS AT TAMPA INTL AIRPORT (TPA).	\$638,986.86	\$352,000,000.00	7/13/07	6/30/08	ONLY ONE SOURCE - OTHER

L-3 COMMUNICATIONS SECURITY AN	TO INSTALL TWENTY-FOUR (24) METER WIDE TUNNELS AT TAMPA INTL AIRPORT (TPA).	\$ 75,245.01	\$ 75,245.01	7/13/07	9/11/07	ONLY ONE SOURCE - OTHER
L-3 COMMUNICATIONS SECURITY AN	TO ORDER TO INSTALL EIGHT (8) EDS UNITS AT GEORGE BUSH HOUSTON INTERCONTINENTAL AIRPORT (IAH).	\$1,485,408.86	\$352,000,000.00	7/12/07	5/31/08	ONLY ONE SOURCE - OTHER
L-3 COMMUNICATIONS SECURITY AN	NEDS OF (10) FFOV W/MWT FOR TERMINAL C AT IAH.	\$1,682,593.98	\$1,682,593.98	9/7/07	6/30/08	ONLY ONE SOURCE - OTHER
L-3 COMMUNICATIONS SECURITY AN	UPGRADE KITS (25)	\$1,775,000.00	\$1,775,000.00	9/17/07	6/30/08	ONLY ONE SOURCE - OTHER
L 3 COMMUNICATIONS CORPORATION (4475)	L-3- STT MAINTENANCE BAGGAGE HANDLING SYSTEM	\$ 90,853.72	\$ 90,853.72	9/21/07	3/31/08	ONLY ONE SOURCE - OTHER
L-3 COMMUNICATIONS SECURITY AN	REPLACEMENT AND REMOVAL OF EQUIPMENT	\$352,159.88	\$352,159.88	8/16/07	12/31/07	ONLY ONE SOURCE - OTHER
L 3 COMMUNICATIONS CORPORATION (4475)	CORRECTIVE MAINTENANCE FOR OCTOBER 2007	\$5,125,633.00	\$5,125,633.00	9/18/07	10/31/07	ONLY ONE SOURCE - OTHER
L 3 COMMUNICATIONS CORPORATION (4475)	CORRECTIVE MAINTENANCE FOR OCTOBER 2007	\$ 57,985.20	\$ 57,985.20	9/17/07	12/31/07	ONLY ONE SOURCE - OTHER
L 3 COMMUNICATIONS CORPORATION (4475)	CORRECTIVE MAINTENANCE FOR OCTOBER 2007	\$6,485,169.99	\$6,485,169.99	9/17/07	3/10/08	ONLY ONE SOURCE - OTHER
L-3 COMMUNICATIONS SECURITY AN	ENGINEERING SUPPORT SERVICES - STIP	\$1,411,380.00	\$1,411,380.00	9/28/07	9/30/08	ONLY ONE SOURCE - OTHER
L-3 COMMUNICATIONS SECURITY AN	DECOMMISSIONING OF TEN (10) L3 EXAMINER 6000 EDS AT ORD.	\$455,889.08	\$455,889.08	9/19/07	10/30/08	ONLY ONE SOURCE - OTHER
L-3 COMMUNICATIONS SECURITY AN	IN ORDER TO PROCURE STAND-ALONE SIMULATORS	\$291,200.00	\$352,000,000.00	6/28/07	9/30/07	ONLY ONE SOURCE - OTHER
SPECTRUM SAN DIEGO INCORPORATED	SUGGESTED VENDOR: SPECTRUM SAN DIEGO, INC.	\$ 60,000.00	\$ 60,000.00	4/26/07	4/26/07	ONLY ONE SOURCE - OTHER
NOMADICS INCORPORATED	SENSING ELEMENTS (EXTENDED LIFE SENSING CARTRIDGE: FP-01-E)	\$ 45,591.30	\$ 45,591.30	7/25/07	11/21/07	ONLY ONE SOURCE - OTHER
NOMADICS INCORPORATED	SENSING ELEMENTS (EXTENDED LIFE SENSING CARTRIDGE: FP-01-E)	\$3,287.27	\$3,287.27	8/8/07	11/21/07	ONLY ONE SOURCE - OTHER

EGS INCORPORATED (2250)	THIS PR PROVIDES FY078 APPROPRIATIONS TO FUND A BRIDGE FOR CONTRACT (HSTS03-06-A-ACC911) (REQUISITION #21-06-206AOP531) WITH EGS IN CONTINUING ADMINISTRATIVE SUPPORT AT BRADLEY, SEATTLE, DENVER, MIDLAND INTERNATIONAL, AMARILLO AND BURLINGTON AIRPORTS. THE CURRENT TASK ORDER WITH EGS INC. HAS BEEN FUNDED WITH FY067 APPROPRIATIONS WHICH ALL UNEXPENDED FUNDS MUST BE DE-OBLIGATED BY 30 SEPTEMBER 2007. THIS BRIDGE WILL CONTINUE SERVICES UNTIL THE FY08 NATIONAL ADMIN SERVICES CONTRACT IS PUT IN PLACE.	\$100,000.00	\$100,000.00	9/17/07	5/12/11	URGENCY
REGAL DECISION SYSTEMS INCORPORATED	THIS PR IS THE FORTH TASK ORDER 4 UNDER THE BPA ESTABLISHED THROUGH CONTRACT HSTS02-06-A-AOP270. THE PERIOD OF PERFORMANCE FOR THIS TASK ORDER WILL BE FROM THE DATE OF AWARD THROUGH JULY 31, 2008. THE WORK TO BE PERFORMED UNDER THIS TASK ORDER IS OUTLINED IN THE ATTACHED TASK 4 STATEMENT OF WORK (SOW) AND THE ASSOCIATED REQUIRMENTS IDENTIFIED IN APPENDIX A OF TEH SOW.	\$264,274.00	\$264,274.00	3/14/07	5/9/08	ONLY ONE SOURCE - OTHER
REGAL DECISION SYSTEMS INCORPORATED	THIS PR IS THE FIFTH TASK ORDER UNDER THE BPA ESTABLISHED UNDER CONTRACT HSTS02-06-A-AOP270. THE PERIOD OF PERFORMANCE OF THE WORK ORDERED UNDER THIS PR WILL BE 4 MONTHS FROM THE DATE OF AWARD. THE WORK TO BE PERFORMED UNDER THIS TASK ORDER IS OUTLINED IN THE ATTACHED TASK 5 STATEMENT OF WORK (SOW) AND THE ASSOCIATED REQUIREMENTS DOCUMENT.	\$185,095.54	\$185,095.54	7/30/07	5/9/08	PATENT/DAT A RIGHTS

REGAL DECISION SYSTEMS INCORPORATED	THIS PR IS THE FIFTH TASK ORDER UNDER THE BPA ESTABLISHED UNDER CONTRACT HSTS02-06-A-AOP270. THE PERIOD OF PERFORMANCE OF THE WORK ORDERED UNDER THIS PR WILL BE 4 MONTHS FROM THE DATE OF AWARD. THE WORK TO BE PERFORMED UNDER THIS TASK ORDER IS OUTLINED IN THE ATTACHED TASK 5 STATEMENT OF WORK (SOW) AND THE ASSOCIATED REQUIREMENTS DOCUMENT.	\$1,329.38	\$1,329.38	7/30/07	5/9/08	PATENT/DATA RIGHTS
OAG Worldwide	Software for access to OAG database to analyze and review flight data for staff planning.	\$4,920.00	\$4,920.00	3/8/07	1/0/00	ONLY ONE SOURCE - OTHER
Accelera Solutions Inc.	Replaces PR 2107207OSO057 and PR 2107207OSO152 accomadates and increase in price for this item associated with a small business. CITRIX	\$ 38,848.73	\$ 38,848.73	3/30/07	1/0/00	ONLY ONE SOURCE - OTHER
ALACHUA COUNTY OF (4843)	RATIFICATION ACTION FOR STORAGE FACILITIES FOR DISASTER PREPAREDNESS PLAN EQUIPMENT AND SUPPLIES GAINESVILLE REGIONAL AIRPORT POC: FRANK STAGL 3880 NE 39TH AVENUE, SUITE B GAINEVILLE, FLORIDA 32609 TSA HQ POC: JOHN DUPRAS, OSO MONTHLY PAYMENT OF \$3000.00 FOR APPROX 4000SQ. FT. FOR PERIOD OF AUGUST 2006-SEPTEMBER 2007. PR IS TO INCREASE FROM \$36,000.00 TO ADDITIONAL \$3,000.00. TO A TOTAL \$39,000.00 TO COVER A 13TH MONTH PERIOD.	\$ 39,000.00	\$ 39,000.00	9/24/07	9/30/07	UNIQUE SOURCE
Commercial Movers Inc.	RDU016 Storage and Distribution of Consumable Supplies 9 Storage bays.	\$9,315.00	\$9,315.00	8/23/07	1/0/00	ONLY ONE SOURCE - OTHER
CLASSIFIED DOMESTIC CONTRACTOR	MAY-SEPTEMBER 2007 FEES .	\$ 87,500.00	\$687,500.00	5/15/07	9/30/09	NATIONAL SECURITY
Grant Oliver	Parking decals for mission parking at Pittsburgh airport	\$ 44,280.00	\$235,086.00	10/1/07	9/30/07	ONLY ONE SOURCE - OTHER
Grant Oliver Corporation	Mission Parking Decals at Pittsburgh Airport. Option Year One - funded only under CR time frame.	\$6,497.75	\$ 50,777.55	10/16/07	11/16/07	ONLY ONE SOURCE - OTHER
Port of Seattle	Parking decals for mission parking at the Seattle / Tacoma airport	\$ 58,853.76	\$382,158.00	10/1/07	9/30/07	ONLY ONE SOURCE - OTHER

New South Parking	Parking decals for mission parking at airport	\$108,000.00	\$108,000.00	1/30/07	9/30/07	ONLY ONE SOURCE - OTHER
Metropolitan Airports Commission	parking decals for mission parking at airport	\$ 26,984.00	\$ 26,984.00	1/30/07	12/31/07	ONLY ONE SOURCE - OTHER
VP INTERNATIONAL SUPPLY INCORPORATED	LIFE FITNESS TREADMILL - 95TI FOR DETROIT.	\$4,331.00	\$4,331.00	5/9/07	6/27/07	ONLY ONE SOURCE - OTHER
VP INTERNATIONAL SUPPLY INCORPORATED	LIFE FITNESS TREADMILL - 95TI FOR DETROIT.	\$343.00	\$343.00	5/18/07	6/27/07	ONLY ONE SOURCE - OTHER
LEE TECHNOLOGIES SERVICES INCORPORATED	PRODUCT EXPANSION - UPS SYSTEM 10KVA EXPANDED TO 15KVA ON MODEL EPS3010, S/N: A03-11278 REFERENCE QUOTE: FWS-0715823A	\$2,317.02	\$2,317.02	5/18/07	6/22/07	ONLY ONE SOURCE - OTHER
PELICAN PRODUCTS INCORPORATED	60 EACH - MODEL 1500 PELICAN - BLACK WITH FOAM INSERT PRICE QUOTE PER TELECON NOEMEE GASBIAN - JULY 13, 2007 (PELICAN PRODUCTS) AND THE UNDERSIGNED.	\$4,716.00	\$4,716.00	7/16/07	8/15/07	SIMPLIFIED ACQUISITION PROCEDURE S-NON-COMPETITIVE
DATAMAXX APPLIED TECHNOLOGIES INCORPORATED	PR TO FUND TRIP LABOR AND TRAVEL FOR THE PERIOD OCTOBER 1, 2006-SEPTEMBER 30, 2007 \$1,083,749.85(HSTS07-07-F-DM11)- CARRYOVER AIR TO GROUND FUNDS	\$1,083,749.85	\$1,083,749.85	3/1/07	9/30/07	ONLY ONE SOURCE - OTHER
DATAMAXX GROUP INCORPORATED	PR TO FUND RECURRING COSTS IN SUPPORT OF PDAS FOR THE PERIOD OCTOBER 1, 2006-SEPTEMBER 30, 2007, \$7,078,125.28. (HSTS07-07-DM12)-FY07 BASE	\$7,078,125.28	\$7,078,125.28	10/16/06	9/30/07	ONLY ONE SOURCE - OTHER
DATAMAXX GROUP INCORPORATED	PR TO FUND RECURRING COSTS IN SUPPORT OF PDAS FOR THE PERIOD OCTOBER 1, 2006-SEPTEMBER 30, 2007, \$7,078,125.28. (HSTS07-07-DM12)-FY07 BASE	\$356,960.00	\$356,960.00	2/9/07	9/30/07	ONLY ONE SOURCE - OTHER
DATAMAXX GROUP INCORPORATED	PR TO FUND RECURRING COSTS IN SUPPORT OF PDAS FOR THE PERIOD OCTOBER 1, 2006-SEPTEMBER 30, 2007, \$7,078,125.28. (HSTS07-07-DM12)-FY07 BASE	\$200,000.00	\$200,000.00	7/13/07	9/30/07	ONLY ONE SOURCE - OTHER

DATAMAXX GROUP INCORPORATED	PR TO FUND PDA ACCESSORIES- CHARGERS, CABLES, PLUGS, BATTERIES, EARBUDS, \$15,407.15. NOTE: PR-2107FAMISD004 "PR TO FUND RECURRING COSTS IN SUPPORT OF PDAS" WAS AMENDED FROM \$7,078,125.28 TO \$7,036,071.28. THE AMENDMENT DEOBLIGATED \$42,054 TO BE USED ON ADDITIONAL PRS FOR PDA RELATED COST.	\$ 15,407.15	\$ 15,407.15	1/3/07	2/2/07	ONLY ONE SOURCE - OTHER
DATAMAXX GROUP INCORPORATED	PR TO FUND FAMS SIM MIGRATION EFFORT. TO BE FUNDED FROM FY04 AIR TO GROUND EARMARK	\$ 53,216.00	\$ 53,216.00	6/20/07	8/31/07	ONLY ONE SOURCE - OTHER
FEDERAL CARTRIDGE COMPANY	1000 ROUNDS OF FEDERAL GMM .223 REM GM223M3 77GR AMMO FOR MOBILE TRAINING TEAM. PRICE IS \$114.20 PER 200 ROUNDS. ORL WOULD NEED THIS AMMUNITION DROP SHIPPED TO THEM BY WEDNESDAY 11/8/2007.	\$571.00	\$571.00	11/7/06	12/7/06	ONLY ONE SOURCE - OTHER
MISCELLANEOUS FOREIGN CONTRACTORS	123 PARTICIPANTS AT 10.00 EACH FOR FY07 RANGE USAGE. PERIOD OF PERFORMANCE WILL END 9/30/2007	\$1,230.00	\$1,230.00	12/18/06	9/30/07	FOLLOW-ON CONTRACT
MISCELLANEOUS FOREIGN CONTRACTORS	BLUE RIDGE ARSENAL - HQ RANGE USAGE (JAN. 07 - DEC. 07)	\$9,600.00	\$9,600.00	12/28/06	12/31/07	AUTHORIZED BY STATUTE
STONEWALL LIMITED	RANGE CONTRACT FOR 2007 DATE OF AWARD THROUGH DECEMBER 31, 2007 INCLUDES: 24 TWO SESSIONS ON PRIVATE RANGE, 2 EIGHT HOUR SESSIONS ON PRIVATE RANGE AND UNLIMITED USE OF PUBLIC RANGE BY INDIVIDUAL AGENTS	\$2,500.00	\$2,500.00	2/1/07	3/3/07	ONLY ONE SOURCE - OTHER
CLASSIFIED DOMESTIC CONTRACTOR	FY2007 TRANSACTION FEES	\$ 20,000.00	\$ 60,000.00	2/16/07	9/30/09	NATIONAL SECURITY

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE	<p>INT'L ASSOCIATION OF CHIEF OF POLICE (IACP) P.O.BOX 90976 WASHINGTON DC 20090-0976 1-800-THE-IACP</p> <p>RENEWAL OF 2007 MEMBERSHIP (\$100 PER MEMBER)</p> <p>30 MEMBERS X \$100 = \$3,000</p> <p>NAMES PROVIDED IN LINE ITEM 1</p>	\$3,000.00	\$3,000.00	2/20/07	3/22/07	UNIQUE SOURCE
PRADO FAMILY SHOOTING RANGE	<p>PERIOD OF PERFORMANCE FOR THIS PURCHASE ORDER IS FROM DATE OF AWARD THROUGH DECEMBER 31, 2007</p> <p>PRICING IS AS FOLLOWS \$325.00 FOR 8 HOUR DAY, \$225.00 FOR HALF DAY AND ADDITIONAL SHOOTING BAY IS \$100.00.</p> <p>EMAIL INVOICES TO FIN-SMB- TSAINVOICES@USCG@MIL</p>	\$9,750.00	\$9,750.00	2/22/07	12/31/07	SIMPLIFIED ACQUISITION PROCEDURE - NON-COMPETITIVE
CHESAPEAKE LOCK AND SAFE SERVICE COMPANY	<p>PR PROVIDES FUNDING TO COMPLETE A WEAPONS STORAGE ROOM SECURITY CAGE AND PARTITION ENCLOSURE AT CEILING AT FAMS HQ RESTON VA. PHYSICAL SECURITY POC IS ANDY COBURN AT 703-487-3155.</p>	\$1,755.00	\$1,755.00	3/2/07	4/11/07	ONLY ONE SOURCE - OTHER
AMERICAN BANK NOTE HOLOGRAPHICS	<p>FFDO CREDENTIAL LAMINATES</p> <p>AMERICAN BANK NOTE HOLOGRAPHICS POC: MICHAEL BANAHAN 609-632-0842</p> <p>CO: MICHELLE BENVENUTO, FAMS CONTRACT AND PROCUREMENT BRANCH, 609-813-3338</p>	\$50,000.00	\$50,000.00	3/26/07	5/2/07	ONLY ONE SOURCE - OTHER
FEDERAL PRISON INDUSTRIES INCORPORATED (5705) 1515236	<p>42" ROUND TABLE, MAHOGONY FURNITURE LINE: SYMPHONY PRODUCT NUMBER WITH COLOR CODE: S42R(MH)</p> <p>UNICOR WEST COAST POC IS: JOSEPH ROTH (818) 246-8334 (OFFICE) (818) 749-4923 (CELL)</p>	\$665.00	\$665.00	4/10/07	5/10/07	UNICOR
MISCELLANEOUS FOREIGN CONTRACTORS	<p>INDOOR FIREARMS RANGE USE FOR 17 DAYS FROM 1/31/07 THROUGH MAY 15 OF 2007. THE MAP AUDIT REQUIRED ALL MAKE-UP TRAINING AND ADDITIONAL FIREARMS TRAINING.</p>	\$6,500.00	\$6,500.00	4/12/07	5/15/07	AUTHORIZED BY STATUTE

FEDERAL PRISON INDUSTRIES INCORPORATED (5705) 1531953	OFFICE FURNITURE FOR NEW ATSAC DESK, BOOKCASE, LATERAL FILE AND TWO CHAIRS	\$4,465.89	\$4,465.89	5/22/07	7/16/07	UNICOR
SIGARMS INCORPORATED	RECOMMENDED VENDOR: SIGARMS INERT, FULLY FUNCTIONAL TRAINING WEAPON THAT REPLICATES THE SIGARMS P 229-357 PISTOLS.	\$3,894.00	\$3,894.00	6/29/07	8/31/07	ONLY ONE SOURCE - OTHER
GRADUATE SCHOOL USDA	PROFESSIONAL DEVELOPMENT TRAINING. ATL SUBMITTING 182S TO OPT.	\$9,150.00	\$9,150.00	7/12/07	8/11/07	ONLY ONE SOURCE - OTHER
COMBINED SYSTEMS INCORPORATED	AMMO REQUEST FOR MITT - MULTIPLE VENDORS (FEDERAL, DEF-TEC, CTS - SEE LIST)	\$1,071.18	\$1,071.18	8/29/07	9/5/07	ONLY ONE SOURCE - OTHER
HECKLER AND KOCH DEFENSE INCORPORATED	SPARE PARTS KITS TO SUPPORT FUNCTION AND READINESS FOR FEMT RIFLES. POC JERALD BRANZ	\$3,520.00	\$3,520.00	9/7/07	2/8/08	ONLY ONE SOURCE - OTHER
UNITED STATES POSTAL SERVICE	PR IS FOR REIMBURSEMENT COSTS UNDER INTERAGENCY AGREEMENT BETWEEN FAMS AND US POSTAL INSPECTION SERVICE, CAREER DEVELOPMENT DIVISION, FIREARMS TRAINING FACILITY. NEW AGREEMENT NUMBER CONTRACTING OFFICER - STEVE DAVIS, FAMS CONTRACT & PROCUREMENT BRANCH. (609) 909-5712 POP - CURRENT DATE THROUGH MAY 8, 2008.	\$3,000.00	\$3,000.00	6/20/07	5/8/08	AUTHORIZED BY STATUTE
GOVERNMENT PRINTING OFFICE UNITED STATES	PRINTING	\$ 11,523.00	\$ 11,523.00	7/25/07	8/15/07	AUTHORIZED BY STATUTE
City of Phoenix	FY07 reimbursement allotment for Phoenix Sky Harbor International Airport (PHX).	\$26,166,666.67	\$91,500,000.00	9/24/07	12/31/09	ONLY ONE SOURCE - OTHER
SACRAMENTO	ADDITIONAL FUNDING FOR CCTV OTA WITH SACRAMENTO. SEE ALSO 2107207CTO213	\$567,989.00	\$567,989.00	9/19/07	9/30/12	ONLY ONE SOURCE - OTHER
VIRGIN ISLANDS PORT AUTHORITY	THE VIRIGIN ISLANDS PORT AUTHORITY STT OTA SUPPORTING CORRECTIVE REPAIS AND ENHANCMENTS TO ELECCTRICAL POWER INFRASTRUTURE SUPPORTING BAGGAGE SCREENING AT STT. MANGEMENT, LABOR AND MATERIAL COSTS OF INFRASTRUCTURE.	\$495,000.00	\$495,000.00	9/10/07	9/30/08	ONLY ONE SOURCE - OTHER
MITRE Corporation	The Mitre Corporation.	\$350,000.00	\$3,301,917.00	1/29/07	1/0/00	ONLY ONE SOURCE - OTHER
Aircraft Owners and Pilots Association (AOPA)	Earmarked funds for AOPA education efforts. A yearly OTA with AOPA.	\$220,000.00	\$220,000.00	6/14/07	7/8/08	ONLY ONE SOURCE - OTHER

Medeco Security Locks	The PR is to purchase locks for the Office of Security	\$ 30,914.67	\$ 30,914.67	8/29/07	9/30/07	ONLY ONE SOURCE - OTHER
EGS, Inc	Bridge for EGS	\$100,000.00	\$100,000.00	9/17/07	10/1/07	ONLY ONE SOURCE - OTHER
INFINITY TECHNOLOGY, LLC	PROGRAM MANAGEMENT/SUPPORT SERVICES	\$171,360	\$171,360	05/26/2008	06/22/2009	AUTHORIZED BY STATUTE
TRIUMPH ENTERPRISES, INCORPORATED	PROGRAM MANAGEMENT/SUPPORT SERVICES	\$480,473	\$480,473	08/01/2008	08/03/2013	AUTHORIZED BY STATUTE
TERACORE, INC	ADP SYSTEMS DEVELOPMENT SERVICES	\$135,648	\$276,058	09/15/2008	09/28/2010	AUTHORIZED BY STATUTE
INTERNATIONAL BUSINESS MACHINES CORPORATION	TECHNICAL ASSISTANCE	\$1,201,082	\$1,201,082	02/01/2008	10/31/2009	UNIQUE SOURCE
MIRACLE SYSTEMS LIMITED LIABILITY COMPANY	PROGRAM MANAGEMENT/SUPPORT SERVICES	\$1,270,087	\$2,672,261	02/29/2008	03/02/2010	AUTHORIZED BY STATUTE
SOLUTIONS THROUGH INNOVATIVE TECHNOLOGIES INC	AUDITING SERVICES	\$199,938	\$852,505	09/18/2008	09/28/2012	AUTHORIZED BY STATUTE
TRIUMPH ENTERPRISES, INCORPORATED	OTHER PROFESSIONAL SERVICES	\$3,123,740	\$3,123,740	05/30/2008	06/02/2009	AUTHORIZED BY STATUTE
SEKON ENTERPRISE, INC.	OTHER PROFESSIONAL SERVICES	\$275,000	\$902,725	09/15/2008	09/15/2009	AUTHORIZED BY STATUTE
TACTICAL OFFICE SOLUTIONS	INSTALL OF FURNITURE	\$250,000	\$250,000	06/18/2008	06/18/2012	AUTHORIZED BY STATUTE
THOMAS CONSTRUCTION COMPANY, INC.	CONSTRUCTION (BASIC)	\$183,237	\$183,237	09/02/2008	11/14/2008	AUTHORIZED BY STATUTE
TERACORE, INC	PROGRAM MANAGEMENT/SUPPORT SERVICES	\$701,926	\$3,425,873	06/14/2008	06/13/2009	AUTHORIZED BY STATUTE
MACROSYS RESEARCH & TECHNOLOGY	DATA COLLECTION SERVICES	\$192,435	\$424,657	04/07/2008	12/24/2011	AUTHORIZED BY STATUTE
BANNER STAFFING	OTHER ADMINISTRATIVE SUPPORT SVCS	\$71,980	\$382,100	03/13/2008	03/14/2009	AUTHORIZED BY STATUTE
CONSOLIDATED SAFETY SERVICES INCORPORATED	SCIENTIFIC DATA STUDIES	\$173,300	\$173,300	07/14/2008	07/13/2009	AUTHORIZED BY STATUTE
KOLA NUT TRAVEL INC	TRAVEL AGENT SERVICES	\$49,996	\$107,000	09/15/2008	10/31/2009	AUTHORIZED BY STATUTE
DELOITTE CONSULTING L.L.P.	OTHER PROFESSIONAL SERVICES	\$822,970	\$822,970	05/01/2008	06/16/2008	ONLY ONE SOURCE - OTHER
FREIGHTDESK TECHNOLOGIES, INC	OTHER PROFESSIONAL SERVICES	\$400,000	\$400,000	06/24/2008	02/23/2009	ONLY ONE SOURCE - OTHER
RAILINC CORP.	DATA COLLECTION SERVICES	\$123,000	\$601,344	09/26/2008	09/25/2013	ONLY ONE SOURCE - OTHER
BAYFIRST SOLUTIONS LLC	OTHER PROFESSIONAL SERVICES	\$398,280	\$398,280	04/01/2008	12/04/2008	AUTHORIZED BY STATUTE

BAYFIRST SOLUTIONS LLC	OTHER PROFESSIONAL SERVICES	\$847,600	\$847,600	09/08/2008	09/30/2009	AUTHORIZE D BY STATUTE
ID SOLUTIONS INCORPORATED	ADP SOFTWARE	\$427,270	\$1,107,580	02/19/2008	02/18/2012	FOLLOW-ON CONTRACT
MANAGEMENT SOLUTIONS, INC.	CONSTRUCTION OF OFFICE BUILDINGS	\$2,133,000	\$2,133,000	09/23/2008	09/23/2008	AUTHORIZE D BY STATUTE
EXECUTIVE TECHNOLOGY, INC.	OTHER ADP & TELECOMMUNICATIONS SVCS	\$530,187	\$530,187	04/18/2008	04/17/2010	AUTHORIZE D BY STATUTE
ADVERTISING COUNCIL, INC. THE	MISCELLANEOUS ITEMS	\$1,299,980	\$1,299,980	09/16/2008	09/23/2009	AUTHORIZE D BY STATUTE
BAYFIRST SOLUTIONS LLC	PROGRAM EVALUATION SERVICES	\$74,793	\$74,793	03/06/2008	07/08/2008	AUTHORIZE D BY STATUTE
GAP SOLUTIONS, INC.	OTHER PROFESSIONAL SERVICES	\$0	\$0	10/22/2008	10/22/2009	AUTHORIZE D BY STATUTE
SIM-G TECHNOLOGIES, LLC	MISC ALARM, SIGNAL, SEC SYSTEMS	\$1,072,595	\$1,072,595	06/20/2008	06/20/2009	AUTHORIZE D BY STATUTE
TERACORE INCORPORATED	ADP SYSTEMS ANALYSIS SERVICES	\$658,327	\$658,327	02/27/2008	02/29/2012	AUTHORIZE D BY STATUTE
BATTLE RESOURCE MANAGEMENT, INC	PROGRAM MANAGEMENT/SUPPORT SERVICES	\$190,944	\$291,190	09/23/2008	03/22/2010	AUTHORIZE D BY STATUTE
DIXON GROUP, INC., (THE)	PATENT AND TRADEMARK SERVICES	\$91,024	\$91,024	08/01/2008	12/05/2008	AUTHORIZE D BY STATUTE
TURNER, MARSHA	CUSTODIAL JANITORIAL SERVICES	\$206,000	\$1,099,313	08/12/2008	09/01/2009	AUTHORIZE D BY STATUTE
DAY CONSULTANTS, INC.	OTHER PROFESSIONAL SERVICES	\$315,808	\$1,948,840	09/23/2008	07/23/2013	AUTHORIZE D BY STATUTE
A.B.P. MAINTENANCE CORP.	CUSTODIAL JANITORIAL SERVICES	\$22,395	\$22,395	03/27/2008	03/31/2009	AUTHORIZE D BY STATUTE
TERACORE, INC	ADP SYSTEMS DEVELOPMENT SERVICES	\$0	\$0	03/09/2009	12/21/2010	AUTHORIZE D BY STATUTE
MIRACLE SYSTEMS LIMITED LIABILITY COMPANY	PROGRAM MANAGEMENT/SUPPORT SERVICES	\$1,402,174	\$1,402,174	02/19/2009	03/02/2010	AUTHORIZE D BY STATUTE
GMG MANAGEMENT CONSULTING INC.	FINANCIAL SERVICES	\$570,612	\$0	03/11/2009	03/31/2011	AUTHORIZE D BY STATUTE
TRIUMPH ENTERPRISES, INCORPORATED	OTHER PROFESSIONAL SERVICES	-\$225,994	-\$225,994	01/30/2009	06/02/2009	AUTHORIZE D BY STATUTE
BANNER STAFFING	OTHER ADMINISTRATIVE SUPPORT SVCS	\$74,120	\$74,120	02/19/2009	03/14/2010	AUTHORIZE D BY STATUTE
AITHERAS, LLC	OTHER ADMINISTRATIVE SUPPORT SVCS	\$216,995	\$443,990	01/22/2009	09/21/2009	AUTHORIZE D BY STATUTE
GLOBAL TECHNOLOGY SOLUTIONS, LLC	PROGRAM MANAGEMENT/SUPPORT SERVICES	\$894,081	\$1,814,894	02/10/2009	02/09/2010	AUTHORIZE D BY STATUTE

MIRACLE SYSTEMS LLC	AUTOMATED INFORMATION SYSTEM SVCS	\$1,488,880	\$1,488,880	01/30/2009	02/04/2010	AUTHORIZED BY STATUTE
ACCENTURE LLP	TECHNICAL ASSISTANCE	\$5,548,689	\$5,548,689	01/01/2009	02/28/2010	URGENCY
DAMMEL CLEANING ENTERPRISE, INC	CUSTODIAL JANITORIAL SERVICES	\$56,881	\$296,010	02/27/2009	02/28/2014	AUTHORIZED BY STATUTE
MANAGEMENT SOLUTIONS, INC.	CONSTRUCTION OF OFFICE BUILDINGS	\$0	\$0	03/17/2009	03/23/2009	AUTHORIZED BY STATUTE
FACILITY SERVICES PROFESSIONALS	CUSTODIAL JANITORIAL SERVICES	\$0	\$0	03/19/2009	04/30/2008	ONLY ONE SOURCE - OTHER
DIXON GROUP, INC., (THE)	PATENT AND TRADEMARK SERVICES	-\$2,544	-\$2,544	02/04/2009	12/05/2008	AUTHORIZED BY STATUTE

Question: Please provide for the record a list of all contracts over \$1 million in total value executed by TSA in 2008. Organize by contractor, purpose, dollar award, full performance value, contract start date, contract end date, and contract type (e.g., firm fixed price, etc.).

ANSWER: The following chart provides information regarding contracts over \$1 million as of March 24, 2009.

Vendor Name	Description	Obligation	Base and Exercised Options Value	Date Signed	Completion Date	Type of Contract
3H TECHNOLOGY LIMITED LIABILITY COMPANY	COMPUTER FACILITIES MANAGEMENT SERVICES	\$1,500,000	\$1,500,000	7/26/07	7/25/08	FIXED PRICE
A TEK INCORPORATED	ALL OTHER TRAVEL ARRANGEMENT AND RESERVATION SERVICES	\$1,281,834	\$1,281,834	10/20/06	9/30/07	TIME AND MATERIALS
ACCENTURE LLP	ADMINISTRATIVE MANAGEMENT AND GENERAL MANAGEMENT CONSULTING SERVICES	\$ 39,360,364	\$ 39,360,364	11/16/06	12/11/07	FIXED PRICE
ACCENTURE LLP	ADMINISTRATIVE MANAGEMENT AND GENERAL MANAGEMENT CONSULTING SERVICES	\$ -	\$280,914,424	12/8/06	1/31/07	FIXED PRICE
ACCENTURE LLP	ADMINISTRATIVE MANAGEMENT AND GENERAL MANAGEMENT CONSULTING SERVICES	\$9,417,891	\$9,417,891	5/11/07	12/11/07	FIXED PRICE
ACE INFO SOLUTIONS INCORPORATED	OFFICE ADMINISTRATIVE SERVICES	\$1,259,000	\$1,259,000	5/30/07	6/17/12	LABOR HOURS
AMERICAN OPERATIONS CORPORATION	SECURITY SYSTEMS SERVICES (EXCEPT LOCKSMITHS)	\$1,072,255	\$1,072,255	2/26/07	7/9/07	COMBINATION (APPLIES TO AWARDS WHERE TWO OR MORE OF THE ABOVE APPLY)

AMERICAN OPERATIONS CORPORATION	SECURITY SYSTEMS SERVICES (EXCEPT LOCKSMITHS)	\$1,759,923	\$1,759,923	8/9/07	9/30/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
AMERICAN OPERATIONS CORPORATION	SECURITY SYSTEMS SERVICES (EXCEPT LOCKSMITHS)	\$2,400,000	\$2,400,000	1/12/07	1/15/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
AMERICAN OPERATIONS CORPORATION	SECURITY SYSTEMS SERVICES (EXCEPT LOCKSMITHS)	\$1,296,840	\$1,296,840	3/8/07	3/8/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
AMERICAN OPERATIONS CORPORATION	SECURITY SYSTEMS SERVICES (EXCEPT LOCKSMITHS)	\$1,039,523	\$1,039,523	3/8/07	3/8/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
AMERICAN OPERATIONS CORPORATION	SECURITY SYSTEMS SERVICES (EXCEPT LOCKSMITHS)	\$2,156,979	\$2,156,979	3/28/07	5/2/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
AMERICAN OPERATIONS CORPORATION	SECURITY SYSTEMS SERVICES (EXCEPT LOCKSMITHS)	\$1,077,336	\$1,077,336	5/2/07	4/2/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
AMERICAN OPERATIONS CORPORATION	SECURITY SYSTEMS SERVICES (EXCEPT LOCKSMITHS)	\$1,022,240	\$1,022,240	8/22/07	9/14/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
AMERICAN OPERATIONS CORPORATION	SECURITY SYSTEMS SERVICES (EXCEPT LOCKSMITHS)	\$1,394,224	\$1,394,224	7/25/07	7/30/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
AMERICAN OPERATIONS CORPORATION	SECURITY SYSTEMS SERVICES (EXCEPT LOCKSMITHS)	\$6,420,449	\$6,420,449	7/26/07	7/30/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)

AMERICAN OPERATIONS CORPORATION	SECURITY SYSTEMS SERVICES (EXCEPT LOCKSMITHS)	\$5,164,326	\$5,164,326	9/25/07	6/11/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
AMMUNITION ACCESSORIES	SMALL ARMS AMMUNITION MANUFACTURING	\$1,835,106	\$1,835,106	3/10/07	3/9/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
ANALOGIC CORPORATION	SEARCH, DETECTION, NAVIGATION, GUIDANCE, AERONAUTICAL, AND NAUTICAL SYSTEM AND INSTRUMENT MANUFACTURING	\$7,947,855	\$7,947,855	9/26/07	9/25/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
AOC SOLUTIONS INCORPORATED	FINANCIAL TRANSACTIONS PROCESSING, RESERVE, AND CLEARINGHOUSE ACTIVITIES	\$1,224,400	\$1,224,400	3/15/07	3/14/09	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
BATTELLE MEMORIAL INSTITUTE	ALL OTHER PROFESSIONAL, SCIENTIFIC, AND TECHNICAL SERVICES	\$1,670,101	\$1,670,101	2/5/07	12/31/09	COMBINATI ON (APPLIES TO AWARDS WHERE TWO OR MORE OF THE ABOVE APPLY)
BATTELLE MEMORIAL INSTITUTE	ALL OTHER PROFESSIONAL, SCIENTIFIC, AND TECHNICAL SERVICES	\$6,000,000	\$6,000,000	9/5/07	8/31/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
BATTELLE MEMORIAL INSTITUTE	ALL OTHER PROFESSIONAL, SCIENTIFIC, AND TECHNICAL SERVICES	\$2,423,998	\$2,423,998	9/10/07	9/5/08	COMBINATI ON (APPLIES TO AWARDS WHERE TWO OR MORE OF THE ABOVE APPLY)
BEARAK REPORTS INC	CREDIT BUREAUS	\$2,989,000	\$2,989,000	5/7/07	5/6/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)

BOOZ ALLEN HAMILTON INC.	ADMINISTRATIVE MANAGEMENT AND GENERAL MANAGEMENT CONSULTING SERVICES	\$1,670,000	\$1,670,000	6/12/07	12/3/09	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
BOOZ ALLEN HAMILTON INC.	ADMINISTRATIVE MANAGEMENT AND GENERAL MANAGEMENT CONSULTING SERVICES	\$1,759,546	\$1,759,546	12/4/06	12/3/09	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
BOOZ ALLEN HAMILTON INCORPORATED (3626)	ADMINISTRATIVE MANAGEMENT AND GENERAL MANAGEMENT CONSULTING SERVICES	\$1,014,937	\$1,014,937	12/4/06	5/31/07	LABOR HOURS
BOOZ ALLEN HAMILTON INCORPORATED (3626)	ADMINISTRATIVE MANAGEMENT AND GENERAL MANAGEMENT CONSULTING SERVICES	\$1,111,339	\$1,111,339	1/4/07	5/31/07	LABOR HOURS
BOOZ ALLEN HAMILTON INCORPORATED (3626)	ADMINISTRATIVE MANAGEMENT AND GENERAL MANAGEMENT CONSULTING SERVICES	\$1,500,000	\$1,500,000	9/25/07	12/3/10	LABOR HOURS
BOOZ ALLEN HAMILTON INCORPORATED (3626)	CUSTOM COMPUTER PROGRAMMING SERVICES	\$1,650,000	\$1,650,000	8/30/07	2/28/12	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
CACI INCORPORATED FEDERAL	ADMINISTRATIVE MANAGEMENT AND GENERAL MANAGEMENT CONSULTING SERVICES	\$1,100,000	\$1,100,000	9/25/07	9/30/09	LABOR HOURS
CACI TECHNOLOGIES INCORPORATED	OTHER SCIENTIFIC AND TECHNICAL CONSULTING SERVICES	\$4,938,641	\$4,938,641	9/20/07	10/1/11	FIXED PRICE AWARD FEE
CARTER AND BURGESS INCORPORATED	ENGINEERING SERVICES	\$1,245,130	\$1,245,130	2/21/07	12/31/09	COMBINATI ON (APPLIES TO AWARDS WHERE TWO OR MORE OF THE ABOVE APPLY)
CARTER AND BURGESS INCORPORATED	ENGINEERING SERVICES	\$1,878,342	\$1,878,342	9/13/07	9/30/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)

CARTER AND BURGESS INCORPORATED	ENGINEERING SERVICES	\$3,954,568	\$3,954,568	5/16/07	5/21/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
CARTER AND BURGESS INCORPORATED	ENGINEERING SERVICES	\$8,600,293	\$8,600,293	5/16/07	5/21/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
CARTER AND BURGESS INCORPORATED	ENGINEERING SERVICES	\$4,810,247	\$4,810,247	5/16/07	5/15/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
CARTER AND BURGESS INCORPORATED	ENGINEERING SERVICES	\$9,283,248	\$9,283,248	9/12/07	10/16/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
CLARK COUNTY DEPT OF AVIATION	LESSORS OF NONRESIDENTIAL BUILDINGS (EXCEPT MINIWAREHOUSES)	\$369	\$1,257,811	1/10/07	2/28/09	FIXED PRICE
CLARK COUNTY DEPT OF AVIATION	LESSORS OF NONRESIDENTIAL BUILDINGS (EXCEPT MINIWAREHOUSES)	\$572,243	\$1,829,685	2/28/07	2/28/08	FIXED PRICE
CLP INDUSTRIAL PROPERTIES LIMITED LIABILITY COMPANY	LESSORS OF NONRESIDENTIAL BUILDINGS (EXCEPT MINIWAREHOUSES)	\$167,140	\$ 16,845,121	1/12/07	6/30/07	FIXED PRICE WITH ECONOMIC PRICE ADJUSTMENT
CLP INDUSTRIAL PROPERTIES LIMITED LIABILITY COMPANY	LESSORS OF NONRESIDENTIAL BUILDINGS (EXCEPT MINIWAREHOUSES)	\$184,893	\$ 17,030,014	3/15/07	6/30/07	FIXED PRICE WITH ECONOMIC PRICE ADJUSTMENT
CLP INDUSTRIAL PROPERTIES LIMITED LIABILITY COMPANY	LESSORS OF NONRESIDENTIAL BUILDINGS (EXCEPT MINIWAREHOUSES)	\$724,022	\$ 17,754,036	8/2/07	11/12/13	FIXED PRICE WITH ECONOMIC PRICE ADJUSTMENT
CLP INDUSTRIAL PROPERTIES LIMITED LIABILITY COMPANY	LESSORS OF NONRESIDENTIAL BUILDINGS (EXCEPT MINIWAREHOUSES)	\$1,455,083	\$1,455,083	11/9/06	11/13/13	FIXED PRICE WITH ECONOMIC PRICE ADJUSTMENT

COMMERCIAL NET LEASE REALTY INCORPORATED	LESSORS OF NONRESIDENTIAL BUILDINGS (EXCEPT MINIWAREHOUSES)	\$5,200,750	\$ 76,939,399	1/17/07	3/31/14	FIXED PRICE WITH ECONOMIC PRICE ADJUSTMENT
COMMERCIAL NET LEASE REALTY INCORPORATED	LESSORS OF NONRESIDENTIAL BUILDINGS (EXCEPT MINIWAREHOUSES)	\$4,430,750	\$ 81,370,149	5/2/07	3/31/14	FIXED PRICE WITH ECONOMIC PRICE ADJUSTMENT
COMMERCIAL NET LEASE REALTY INCORPORATED	LESSORS OF NONRESIDENTIAL BUILDINGS (EXCEPT MINIWAREHOUSES)	\$5,177,994	\$ 86,548,143	7/3/07	3/31/14	FIXED PRICE WITH ECONOMIC PRICE ADJUSTMENT
COMMUNICATIONS RESOURCE INCORPORATED	OTHER SCIENTIFIC AND TECHNICAL CONSULTING SERVICES	\$1,916,677	\$1,916,677	6/5/07	4/16/08	COMBINATION (APPLIES TO AWARDS WHERE TWO OR MORE OF THE ABOVE APPLY)
COOPERATIVE PERSONNEL SERVICES	ADMINISTRATIVE MANAGEMENT AND GENERAL MANAGEMENT CONSULTING SERVICES	\$ 34,000,000	\$ 34,000,000	6/8/07	12/25/07	COST PLUS AWARD FEE
COOPERATIVE PERSONNEL SERVICES	ADMINISTRATIVE MANAGEMENT AND GENERAL MANAGEMENT CONSULTING SERVICES	\$5,000,000	\$5,000,000	9/6/07	12/25/07	COST PLUS AWARD FEE
CORT BUSINESS SERVICES CORPORATION	OFFICE FURNITURE (EXCEPT WOOD) MANUFACTURING	\$2,563,169	\$2,563,169	12/29/06	1/28/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
CORT BUSINESS SERVICES CORPORATION	FURNITURE STORES	\$1,304,320	\$1,304,320	12/22/06	12/31/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
COVENANT AVIATION SECURITY LIMITED LIABILITY COMPANY	SECURITY GUARDS AND PATROL SERVICES	\$7,220,984	\$167,587,320	11/20/06	10/31/06	COST PLUS AWARD FEE
COVENANT AVIATION SECURITY LIMITED LIABILITY COMPANY	SECURITY GUARDS AND PATROL SERVICES	\$2,468,189	\$2,468,189	11/6/06	9/30/10	COST PLUS AWARD FEE
COVENANT AVIATION SECURITY LIMITED LIABILITY COMPANY	SECURITY GUARDS AND PATROL SERVICES	\$ -	\$2,552,237	9/11/07	9/30/10	COST PLUS AWARD FEE
COVENANT AVIATION SECURITY LIMITED LIABILITY COMPANY	SECURITY GUARDS AND PATROL SERVICES	\$ 12,838,681	\$ 12,838,681	11/1/06	9/30/10	COST PLUS AWARD FEE

COVENANT AVIATION SECURITY LIMITED LIABILITY COMPANY	SECURITY GUARDS AND PATROL SERVICES	\$ 18,829,033	\$ 18,829,033	11/1/06	9/30/10	COST PLUS AWARD FEE
COVENANT AVIATION SECURITY LIMITED LIABILITY COMPANY	SECURITY GUARDS AND PATROL SERVICES	\$ 19,066,764	\$ 19,066,764	11/1/06	9/30/10	COST PLUS AWARD FEE
COVENANT AVIATION SECURITY LIMITED LIABILITY COMPANY	SECURITY GUARDS AND PATROL SERVICES	\$ 19,878,265	\$ 19,878,265	11/1/06	9/30/10	COST PLUS AWARD FEE
COVENANT AVIATION SECURITY LIMITED LIABILITY COMPANY	SECURITY GUARDS AND PATROL SERVICES	\$ -	\$ 84,136,594	11/1/06	9/30/10	COST PLUS AWARD FEE
COVENANT AVIATION SECURITY LIMITED LIABILITY COMPANY	SECURITY GUARDS AND PATROL SERVICES	\$6,223,803	\$6,223,803	11/1/06	9/30/10	COST PLUS AWARD FEE
COVENANT AVIATION SECURITY LIMITED LIABILITY COMPANY	SECURITY GUARDS AND PATROL SERVICES	\$6,915,336	\$6,915,336	11/1/06	9/30/10	COST PLUS AWARD FEE
COVENANT AVIATION SECURITY LIMITED LIABILITY COMPANY	SECURITY GUARDS AND PATROL SERVICES	\$ 17,749,364	\$ 17,749,364	11/1/06	9/30/10	COST PLUS AWARD FEE
CREATIVE COMPUTING SOLUTIONS INCORPORATED	ADMINISTRATIVE MANAGEMENT AND GENERAL MANAGEMENT CONSULTING SERVICES	\$1,820,749	\$1,820,749	4/26/07	11/25/08	TIME AND MATERIALS
CURTIS, T. & CO, PC	OFFICES OF CERTIFIED PUBLIC ACCOUNTANTS	\$1,536,672	\$1,536,672	1/29/07	1/31/08	FIXED PRICE
DATAMAXX APPLIED TECHNOLOGIES INCORPORATED	SOFTWARE PUBLISHERS	\$1,083,750	\$1,083,750	3/1/07	9/30/07	LABOR HOURS
DATAMAXX GROUP INCORPORATED	CELLULAR AND OTHER WIRELESS TELECOMMUNICATIONS	\$2,191,604	\$2,191,604	1/3/07	9/30/07	FIXED PRICE
DATAMAXX GROUP INCORPORATED	SOFTWARE PUBLISHERS	\$7,078,125	\$7,078,125	10/16/06	9/30/07	FIXED PRICE
DELL MARKETING LIMITED PARTNERSHIP	ELECTRONIC COMPUTER MANUFACTURING	\$6,008,002	\$6,008,002	6/22/07	7/21/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
DELOITTE CONSULTING L.P.	CUSTOM COMPUTER PROGRAMMING SERVICES	\$6,860,300	\$6,860,300	7/16/07	4/30/08	TIME AND MATERIALS
DELOITTE CONSULTING L.P.	CUSTOM COMPUTER PROGRAMMING SERVICES	\$2,000,000	\$2,000,000	7/3/07	1/31/08	LABOR HOURS
DUN AND BRADSTREET INCORPORATED (2360)	CREDIT BUREAUS	\$6,509,950	\$6,509,950	5/22/07	5/22/08	FIXED PRICE
DYNAMIC SECURITY CONCEPTS INCORPORATED	ENGINEERING SERVICES	\$1,760,441	\$1,760,441	9/11/07	9/10/08	LABOR HOURS

EG SOLUTIONS LIMITED LIABILITY COMPANY	OTHER COMPUTER RELATED SERVICES	\$1,774,997	\$1,774,997	4/17/07	5/20/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
EG SOLUTIONS LIMITED LIABILITY COMPANY	OTHER COMPUTER RELATED SERVICES	\$2,102,503	\$2,102,503	5/7/07	6/7/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
EG SOLUTIONS LIMITED LIABILITY COMPANY	OTHER COMPUTER RELATED SERVICES	\$1,820,513	\$1,820,513	5/2/07	6/5/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
EG SOLUTIONS LIMITED LIABILITY COMPANY	OTHER COMPUTER RELATED SERVICES	\$1,016,090	\$1,016,090	6/11/07	7/10/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
EG SOLUTIONS LIMITED LIABILITY COMPANY	OTHER COMPUTER RELATED SERVICES	\$1,121,328	\$1,121,328	9/4/07	12/31/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
ELECTRONIC CONSULTING SERVICES INCORPORATED	COMPUTER SYSTEMS DESIGN SERVICES	\$4,495,000	\$4,495,000	8/29/07	9/30/12	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
ELECTRONIC CONSULTING SERVICES INCORPORATED	COMPUTER SYSTEMS DESIGN SERVICES	\$1,367,673	\$1,367,673	9/13/07	9/12/08	FIXED PRICE
ENTERPRISE SOLUTIONS REALIZED INCORPORATED	CUSTOM COMPUTER PROGRAMMING SERVICES	\$1,090,241	\$1,090,241	5/4/07	1/27/10	FIXED PRICE
EYAK TECHNOLOGY LIMITED LIABILITY COMPANY	COMPUTER AND COMPUTER PERIPHERAL EQUIPMENT AND SOFTWARE MERCHANT WHOLESALERS	\$2,468,469	\$2,468,469	12/5/06	8/29/10	FIXED PRICE
EYAK TECHNOLOGY LIMITED LIABILITY COMPANY	COMPUTER AND COMPUTER PERIPHERAL EQUIPMENT AND SOFTWARE MERCHANT WHOLESALERS	\$3,121,990	\$3,121,990	1/5/07	8/29/10	FIXED PRICE

FEDERAL SUPPLY SERVICE NATIONAL FURNITURE CENTER (3FN-CO)	HOTELS (EXCEPT CASINO HOTELS) AND MOTELS	\$1,224,202	\$1,224,202	1/18/07	7/18/08	FIXED PRICE
FIRSTLINE TRANSPORTATION SECURITY INCORPORATED	SECURITY GUARDS AND PATROL SERVICES	\$ 11,020,000	\$ 11,020,000	11/6/06	9/30/06	FIXED PRICE
FIRSTLINE TRANSPORTATION SECURITY INCORPORATED	SECURITY GUARDS AND PATROL SERVICES	\$8,539,441	\$ 20,098,352	12/27/06	3/31/06	FIXED PRICE
FIRSTLINE TRANSPORTATION SECURITY INCORPORATED	SECURITY GUARDS AND PATROL SERVICES	\$ 10,133,538	\$ 10,133,538	3/28/07	9/30/07	FIXED PRICE
FIRSTLINE TRANSPORTATION SECURITY INCORPORATED	SECURITY GUARDS AND PATROL SERVICES	\$(154,439)	\$8,030,732	6/28/07	9/30/10	FIXED PRICE
FIRSTLINE TRANSPORTATION SECURITY INCORPORATED	SECURITY GUARDS AND PATROL SERVICES	\$ -	\$ 37,895,449	8/31/07	9/30/10	FIXED PRICE
FIRSTLINE TRANSPORTATION SECURITY INCORPORATED	SECURITY GUARDS AND PATROL SERVICES	\$ -	\$2,011,267	9/28/07	9/30/10	FIXED PRICE
FORSMAN INCORPORATED	COMMERCIAL AND INSTITUTIONAL BUILDING CONSTRUCTION	\$1,160,148	\$1,160,148	7/18/07	11/30/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
GE ION TRACK INCORPORATED	OTHER MEASURING AND CONTROLLING DEVICE MANUFACTURING	\$1,503,189	\$1,503,189	12/27/06	1/31/08	FIXED PRICE
GE ION TRACK INCORPORATED (5392)	SECURITY SYSTEMS SERVICES (EXCEPT LOCKSMITHS)	\$2,220,563	\$2,220,563	3/30/07	3/28/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
GE ION TRACK INCORPORATED (5392)	SECURITY SYSTEMS SERVICES (EXCEPT LOCKSMITHS)	\$6,035,985	\$6,035,985	5/8/07	5/8/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
GMG MANAGEMENT CONSULTING INCORPORATED	ADMINISTRATIVE MANAGEMENT AND GENERAL MANAGEMENT CONSULTING SERVICES	\$1,158,445	\$1,158,445	9/27/07	9/30/12	FIXED PRICE

GOVERNMENT ACQUISITIONS INC	HARDWARE MERCHANT WHOLESALERS	\$1,885,346	\$1,885,346	1/26/07	2/28/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
GOVERNMENT ACQUISITIONS INC	HARDWARE MERCHANT WHOLESALERS	\$1,064,275	\$1,064,275	1/25/07	2/28/07	FIXED PRICE
GOVERNMENT ACQUISITIONS INCORPORATED	OTHER COMPUTER RELATED SERVICES	\$1,194,469	\$1,194,469	6/27/07	7/12/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
GRANT THORNTON LLP	OTHER MANAGEMENT CONSULTING SERVICES	\$4,226,474	\$4,226,474	11/21/06	9/30/07	FIXED PRICE
HECKLER AND KOCH DEFENSE INCORPORATED	SMALL ARMS MANUFACTURING	\$1,155,637	\$1,155,637	8/30/07	11/30/07	FIXED PRICE
HI-TEC SYSTEMS INC	ENGINEERING SERVICES	\$2,144,054	\$2,144,054	9/17/07	9/16/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
IMMIXTECHNOLOGY INC	COMPUTER SYSTEMS DESIGN SERVICES	\$9,051,884	\$9,051,884	10/6/06	9/19/07	FIXED PRICE
IMMIXTECHNOLOGY INC	COMPUTER SYSTEMS DESIGN SERVICES	\$1,484,383	\$1,484,383	7/16/07	9/28/07	FIXED PRICE
IMMIXTECHNOLOGY INC	COMPUTER SYSTEMS DESIGN SERVICES	\$1,168,061	\$1,168,061	8/28/07	9/28/07	FIXED PRICE
INFOGLIDE SOFTWARE CORPORATION	CUSTOM COMPUTER PROGRAMMING SERVICES	\$1,299,995	\$1,299,995	10/3/06	9/30/07	FIXED PRICE
INFOGLIDE SOFTWARE CORPORATION	CUSTOM COMPUTER PROGRAMMING SERVICES	\$1,970,058	\$1,970,058	3/30/07	9/30/07	FIXED PRICE
INFOGLIDE SOFTWARE CORPORATION	SOFTWARE PUBLISHERS	\$1,470,000	\$1,470,000	12/6/06	12/31/07	FIXED PRICE
INFOZEN INCORPORATED	OTHER SCIENTIFIC AND TECHNICAL CONSULTING SERVICES	\$1,964,386	\$1,964,386	11/14/06	9/27/11	COST PLUS AWARD FEE
INFOZEN INCORPORATED	OTHER SCIENTIFIC AND TECHNICAL CONSULTING SERVICES	\$2,261,351	\$2,261,351	12/19/06	9/27/11	COST PLUS AWARD FEE
INFOZEN INCORPORATED	OTHER SCIENTIFIC AND TECHNICAL CONSULTING SERVICES	\$2,286,477	\$2,286,477	3/27/07	9/27/11	COST PLUS AWARD FEE
INFOZEN INCORPORATED	OTHER SCIENTIFIC AND TECHNICAL CONSULTING SERVICES	\$1,519,688	\$1,519,688	6/14/07	9/27/11	COST PLUS AWARD FEE

INFOZEN INCORPORATED	OTHER SCIENTIFIC AND TECHNICAL CONSULTING SERVICES	\$1,195,463	\$1,195,463	9/11/07	9/27/08	COST PLUS AWARD FEE
INFOZEN INCORPORATED	OTHER SCIENTIFIC AND TECHNICAL CONSULTING SERVICES	\$3,815,524	\$3,815,524	3/31/07	3/31/12	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
INFOZEN INCORPORATED	OTHER SCIENTIFIC AND TECHNICAL CONSULTING SERVICES	\$1,822,850	\$1,822,850	7/31/07	3/31/12	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
INFOZEN INCORPORATED	OTHER SCIENTIFIC AND TECHNICAL CONSULTING SERVICES	\$1,243,094	\$1,243,094	3/14/07	9/27/11	COST PLUS AWARD FEE
INFOZEN INCORPORATED	OTHER SCIENTIFIC AND TECHNICAL CONSULTING SERVICES	\$1,209,747	\$1,209,747	7/23/07	9/27/11	COST PLUS AWARD FEE
INNOVATIONS GROUP INCORPORATED	CLAIMS ADJUSTING	\$3,795,103	\$3,795,103	8/15/07	8/31/08	COST PLUS FIXED FEE
INTERNATIONAL BUSINESS MACHINES CORPORATION	COMPUTER AND COMPUTER PERIPHERAL EQUIPMENT AND SOFTWARE MERCHANT WHOLESALERS	\$1,500,000	\$1,500,000	9/29/07	9/29/12	COST PLUS FIXED FEE
INTERNATIONAL BUSINESS MACHINES CORPORATION	COMPUTER AND COMPUTER PERIPHERAL EQUIPMENT AND SOFTWARE MERCHANT WHOLESALERS	\$1,800,000	\$1,800,000	9/29/07	9/29/12	COST PLUS FIXED FEE
INTERNATIONAL BUSINESS MACHINES CORPORATION	COMPUTER AND COMPUTER PERIPHERAL EQUIPMENT AND SOFTWARE MERCHANT WHOLESALERS	\$8,684,719	\$8,684,719	9/27/07	12/31/08	COST PLUS FIXED FEE
INVISION TECHNOLOGIES INCORPORATED	SECURITY SYSTEMS SERVICES (EXCEPT LOCKSMITHS)	\$ 28,103,353	\$ 28,103,353	10/20/06	3/10/07	FIXED PRICE
INVISION TECHNOLOGIES INCORPORATED	SECURITY SYSTEMS SERVICES (EXCEPT LOCKSMITHS)	\$ 44,481,120	\$ 44,481,120	3/16/07	3/10/10	FIXED PRICE
INVISION TECHNOLOGIES INCORPORATED	SECURITY SYSTEMS SERVICES (EXCEPT LOCKSMITHS)	\$ 12,244,119	\$ 12,244,119	8/21/07	3/10/10	FIXED PRICE
INVISION TECHNOLOGIES INCORPORATED	ARCHITECTURAL SERVICES	\$2,340,000	\$2,340,000	8/28/07	8/28/07	TIME AND MATERIALS
INVISION TECHNOLOGIES INCORPORATED	ARCHITECTURAL SERVICES	\$1,100,000	\$1,100,000	8/30/07	8/30/07	TIME AND MATERIALS

INVISION TECHNOLOGIES INCORPORATED	ARCHITECTURAL SERVICES	\$1,258,200	\$1,258,200	8/29/07	8/29/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
INVISION TECHNOLOGIES INCORPORATED	ARCHITECTURAL SERVICES	\$1,832,000	\$1,832,000	8/28/07	8/28/07	TIME AND MATERIALS
INVISION TECHNOLOGIES INCORPORATED	ARCHITECTURAL SERVICES	\$1,514,220	\$1,514,220	8/29/07	8/29/07	TIME AND MATERIALS
INVISION TECHNOLOGIES INCORPORATED	ARCHITECTURAL SERVICES	\$ 76,080,000	\$ 76,080,000	6/26/07	1/31/08	FIXED PRICE
INVISION TECHNOLOGIES INCORPORATED	ARCHITECTURAL SERVICES	\$1,376,788	\$1,376,788	8/6/07	8/13/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
INVISION TECHNOLOGIES INCORPORATED	ARCHITECTURAL SERVICES	\$1,020,000	\$1,020,000	6/29/07	8/30/07	FIXED PRICE
JACKSON HOLE AIRPORT BOARD	SECURITY GUARDS AND PATROL SERVICES	\$ -	\$4,716,063	8/31/07	9/30/10	FIXED PRICE
JACOBS CONSULTANCY	ADMINISTRATIVE MANAGEMENT AND GENERAL MANAGEMENT CONSULTING SERVICES	\$2,276,447	\$2,276,447	8/1/07	7/31/08	FIXED PRICE
KADIX SYSTEMS LIMITED LIABILITY COMPANY	ADMINISTRATIVE MANAGEMENT AND GENERAL MANAGEMENT CONSULTING SERVICES	\$1,458,706	\$1,458,706	3/20/07	3/20/08	FIXED PRICE
KASEMAN LIMITED LIABILITY COMPANY	ALL OTHER TRANSIT AND GROUND PASSENGER TRANSPORTATION	\$ -	\$2,895,969	4/2/07	3/31/08	FIXED PRICE
KASEMAN LIMITED LIABILITY COMPANY	ENGINEERING SERVICES	\$1,637,022	\$1,637,022	6/6/07	6/10/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
KASEMAN LIMITED LIABILITY COMPANY	ENGINEERING SERVICES	\$1,800,355	\$1,800,355	5/3/07	2/28/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)

KASEMAN LIMITED LIABILITY COMPANY	ENGINEERING SERVICES	\$1,303,255	\$1,303,255	8/3/07	8/12/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
KASEMAN LLC	ENGINEERING SERVICES	\$1,905,000	\$1,905,000	9/19/07	9/30/10	COMBINATI ON (APPLIES TO AWARDS WHERE TWO OR MORE OF THE ABOVE APPLY)
KASEMAN LLC	ENGINEERING SERVICES	\$1,188,602	\$1,188,602	6/1/07	5/31/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
KLN STEEL PRODUCTS COMPANY	OFFICE FURNITURE (EXCEPT WOOD) MANUFACTURING	\$1,910,540	\$1,910,540	8/13/07	12/21/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
KLN STEEL PRODUCTS COMPANY	OFFICE FURNITURE (EXCEPT WOOD) MANUFACTURING	\$1,928,933	\$1,928,933	6/7/07	12/7/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
KNOWLEDGE CONSULTING GROUP	MARKETING RESEARCH AND PUBLIC OPINION POLLING	\$4,445,384	\$4,445,384	7/5/07	6/22/11	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
KROLL GOVERNMENT SERVICES	ALL OTHER PROFESSIONAL, SCIENTIFIC, AND TECHNICAL SERVICES	\$3,350,292	\$3,350,292	10/31/06	11/1/07	FIXED PRICE
L 3 COMMUNICATIONS CORPORATION (4475)	ENGINEERING SERVICES	\$ -	\$174,010,000	3/22/07	9/9/07	FIXED PRICE
L 3 COMMUNICATIONS CORPORATION (4475)	ENGINEERING SERVICES	\$ 23,826,534	\$ 23,826,534	10/18/06	3/10/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
L 3 COMMUNICATIONS CORPORATION (4475)	ENGINEERING SERVICES	\$ 32,190,665	\$ 32,190,665	3/16/07	9/30/07	FIXED PRICE

L-3 COMMUNICATIONS CORPORATION (4475)	ENGINEERING SERVICES	\$2,062,500	\$2,062,500	8/15/07	3/10/08	FIXED PRICE
L-3 COMMUNICATIONS CORPORATION (4475)	ENGINEERING SERVICES	\$5,125,633	\$5,125,633	9/18/07	10/31/07	COMBINATI ON (APPLIES TO AWARDS WHERE TWO OR MORE OF THE ABOVE APPLY)
L-3 COMMUNICATIONS CORPORATION (4475)	ENGINEERING SERVICES	\$6,485,170	\$6,485,170	9/17/07	3/10/08	COMBINATI ON (APPLIES TO AWARDS WHERE TWO OR MORE OF THE ABOVE APPLY)
L-3 COMMUNICATIONS CORPORATION (4475)	NATIONAL SECURITY	\$1,700,000	\$1,700,000	9/20/07	7/24/09	FIXED PRICE
L-3 COMMUNICATIONS CORPORATION (4475)	NATIONAL SECURITY	\$1,891,576	\$1,891,576	8/3/07	2/3/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
L-3 COMMUNICATIONS SECURITY AN	ENGINEERING SERVICES	\$ -	\$223,091,093	12/5/06	5/31/07	TIME AND MATERIALS
L-3 COMMUNICATIONS SECURITY AN	ENGINEERING SERVICES	\$ -	\$223,494,036	3/30/07	9/30/07	FIXED PRICE
L-3 COMMUNICATIONS SECURITY AN	ENGINEERING SERVICES	\$361,403	\$1,730,097	6/27/07	6/30/08	FIXED PRICE
L-3 COMMUNICATIONS SECURITY AN	ENGINEERING SERVICES	\$ -	\$223,494,036	3/30/07	9/30/07	FIXED PRICE
L-3 COMMUNICATIONS SECURITY AN	ENGINEERING SERVICES	\$ -	\$224,294,702	2/8/07	2/28/07	FIXED PRICE
L-3 COMMUNICATIONS SECURITY AN	ENGINEERING SERVICES	\$ 54,520	\$154,884,166	7/17/07	8/28/07	FIXED PRICE
L-3 COMMUNICATIONS SECURITY AN	ENGINEERING SERVICES	\$ -	\$223,091,093	1/3/07	1/31/07	COMBINATI ON (APPLIES TO AWARDS WHERE TWO OR MORE OF THE ABOVE APPLY)

L-3 COMMUNICATIONS SECURITY AN	ENGINEERING SERVICES	\$ 81,221	\$225,101,931	3/21/07	6/30/07	TIME AND MATERIALS
L-3 COMMUNICATIONS SECURITY AN	ENGINEERING SERVICES	\$520,000	\$225,020,710	3/6/07	9/30/07	TIME AND MATERIALS
L-3 COMMUNICATIONS SECURITY AN	ENGINEERING SERVICES	\$1,664,000	\$2,184,000	6/25/07	11/6/07	TIME AND MATERIALS
L-3 COMMUNICATIONS SECURITY AN	ENGINEERING SERVICES	\$2,698,305	\$2,698,305	7/2/07	12/31/07	FIXED PRICE
L-3 COMMUNICATIONS SECURITY AN	ENGINEERING SERVICES	\$1,203,609	\$1,203,609	12/20/06	11/20/07	TIME AND MATERIALS
L-3 COMMUNICATIONS SECURITY AN	ENGINEERING SERVICES	\$ 35,770,792	\$ 35,770,792	6/28/07	12/30/08	FIXED PRICE
L-3 COMMUNICATIONS SECURITY AN	ENGINEERING SERVICES	\$1,638,209	\$1,638,209	8/27/07	6/30/08	TIME AND MATERIALS
L-3 COMMUNICATIONS SECURITY AN	ENGINEERING SERVICES	\$3,569,948	\$3,569,948	9/17/07	7/31/08	COMBINATI ON (APPLIES TO AWARDS WHERE TWO OR MORE OF THE ABOVE APPLY)
L-3 COMMUNICATIONS SECURITY AN	ENGINEERING SERVICES	\$1,485,409	\$1,485,409	7/12/07	5/31/08	FIXED PRICE
L-3 COMMUNICATIONS SECURITY AN	ENGINEERING SERVICES	\$1,682,594	\$1,682,594	9/7/07	6/30/08	COMBINATI ON (APPLIES TO AWARDS WHERE TWO OR MORE OF THE ABOVE APPLY)
L-3 COMMUNICATIONS SECURITY AN	ENGINEERING SERVICES	\$1,775,000	\$1,775,000	9/17/07	6/30/08	COMBINATI ON (APPLIES TO AWARDS WHERE TWO OR MORE OF THE ABOVE APPLY)
L-3 COMMUNICATIONS SECURITY AN	ENGINEERING SERVICES	\$6,105,000	\$6,105,000	6/28/07	12/31/08	FIXED PRICE
L-3 COMMUNICATIONS SECURITY AN	ENGINEERING SERVICES	\$1,411,380	\$1,411,380	9/28/07	9/30/08	FIXED PRICE
LANIER WORLDWIDE INCORPORATED	PHOTOGRAPHIC AND PHOTOCOPYING EQUIPMENT MANUFACTURING	\$1,164,981	\$1,164,981	3/9/07	4/30/11	FIXED PRICE

LOCKHEED MARTIN CORPORATION	ADMINISTRATIVE MANAGEMENT AND GENERAL MANAGEMENT CONSULTING SERVICES	\$1,128,000	\$1,128,000	1/29/07	1/31/12	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
LOCKHEED MARTIN CORPORATION	ADMINISTRATIVE MANAGEMENT AND GENERAL MANAGEMENT CONSULTING SERVICES	\$1,128,000	\$1,128,000	6/8/07	1/31/12	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
LOCKHEED MARTIN CORPORATION	ADMINISTRATIVE MANAGEMENT AND GENERAL MANAGEMENT CONSULTING SERVICES	\$1,075,409	\$1,075,409	7/25/07	1/31/12	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
LOCKHEED MARTIN CORPORATION	ADMINISTRATIVE MANAGEMENT AND GENERAL MANAGEMENT CONSULTING SERVICES	\$2,634,325	\$2,634,325	6/20/07	9/7/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
LOCKHEED MARTIN CORPORATION	ADMINISTRATIVE MANAGEMENT AND GENERAL MANAGEMENT CONSULTING SERVICES	\$2,484,795	\$2,484,795	7/12/07	12/31/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
LOCKHEED MARTIN TECHNICAL SERVICES INCORPORATED	PROFESSIONAL AND MANAGEMENT DEVELOPMENT TRAINING	\$5,040,559	\$5,040,559	1/8/07	5/6/07	FIXED PRICE INCENTIVE
LOCKHEED MARTIN TECHNICAL SERVICES INCORPORATED	PROFESSIONAL AND MANAGEMENT DEVELOPMENT TRAINING	\$1,611,109	\$ 19,447,343	2/8/07	2/8/07	FIXED PRICE INCENTIVE
LOCKHEED MARTIN TECHNICAL SERVICES INCORPORATED	PROFESSIONAL AND MANAGEMENT DEVELOPMENT TRAINING	\$591,897	\$ 20,039,240	2/21/07	2/21/07	FIXED PRICE INCENTIVE
LOCKHEED MARTIN TECHNICAL SERVICES INCORPORATED	PROFESSIONAL AND MANAGEMENT DEVELOPMENT TRAINING	\$1,741,398	\$1,741,398	8/10/07	5/6/08	FIXED PRICE INCENTIVE
LOCKHEED MARTIN TECHNICAL SERVICES INCORPORATED	PROFESSIONAL AND MANAGEMENT DEVELOPMENT TRAINING	\$3,148,940	\$3,148,940	11/1/06	5/6/07	FIXED PRICE INCENTIVE
LOCKHEED MARTIN TECHNICAL SERVICES INCORPORATED	PROFESSIONAL AND MANAGEMENT DEVELOPMENT TRAINING	\$2,564,416	\$ 48,462,006	1/31/07	5/12/07	FIXED PRICE INCENTIVE

LOCKHEED MARTIN TECHNICAL SERVICES INCORPORATED	PROFESSIONAL AND MANAGEMENT DEVELOPMENT TRAINING	\$ 42,275	\$ 48,504,281	4/9/07	11/15/07	FIXED PRICE INCENTIVE
LOCKHEED MARTIN TECHNICAL SERVICES INCORPORATED	PROFESSIONAL AND MANAGEMENT DEVELOPMENT TRAINING	\$1,295,238	\$1,295,238	10/31/06	10/31/07	FIXED PRICE INCENTIVE
LOCKHEED MARTIN TECHNICAL SERVICES INCORPORATED	PROFESSIONAL AND MANAGEMENT DEVELOPMENT TRAINING	\$ -	\$5,733,111	3/13/07	3/13/07	FIXED PRICE INCENTIVE
LOCKHEED MARTIN TECHNICAL SERVICES INCORPORATED	PROFESSIONAL AND MANAGEMENT DEVELOPMENT TRAINING	\$122,619	\$ 10,559,004	2/20/07	4/30/07	FIXED PRICE INCENTIVE
LOCKHEED MARTIN TECHNICAL SERVICES INCORPORATED	PROFESSIONAL AND MANAGEMENT DEVELOPMENT TRAINING	\$4,070,181	\$4,070,181	8/10/07	5/6/08	FIXED PRICE INCENTIVE
LOCKHEED MARTIN TECHNICAL SERVICES INCORPORATED	PROFESSIONAL AND MANAGEMENT DEVELOPMENT TRAINING	\$2,837,715	\$2,837,715	9/6/07	5/6/08	FIXED PRICE INCENTIVE
LOCKHEED MARTIN TECHNICAL SERVICES INCORPORATED	PROFESSIONAL AND MANAGEMENT DEVELOPMENT TRAINING	\$ 13,615,334	\$ 80,701,810	1/25/07	6/30/07	FIXED PRICE INCENTIVE
LOCKHEED MARTIN TECHNICAL SERVICES INCORPORATED	PROFESSIONAL AND MANAGEMENT DEVELOPMENT TRAINING	\$4,465,632	\$4,465,632	4/25/07	11/30/07	FIXED PRICE INCENTIVE
LOCKHEED MARTIN TECHNICAL SERVICES INCORPORATED	PROFESSIONAL AND MANAGEMENT DEVELOPMENT TRAINING	\$2,935,693	\$2,935,693	10/31/06	1/31/07	COMBINATI ON (APPLIES TO AWARDS WHERE TWO OR MORE OF THE ABOVE APPLY)
LOCKHEED MARTIN TECHNICAL SERVICES INCORPORATED	PROFESSIONAL AND MANAGEMENT DEVELOPMENT TRAINING	\$3,129,136	\$ 17,356,706	1/26/07	5/12/07	COMBINATI ON (APPLIES TO AWARDS WHERE TWO OR MORE OF THE ABOVE APPLY)
LOCKHEED MARTIN TECHNICAL SERVICES INCORPORATED	PROFESSIONAL AND MANAGEMENT DEVELOPMENT TRAINING	\$713,992	\$3,669,767	1/24/07	3/31/07	COMBINATI ON (APPLIES TO AWARDS WHERE TWO OR MORE OF THE ABOVE APPLY)

LOCKHEED MARTIN TECHNICAL SERVICES INCORPORATED	PROFESSIONAL AND MANAGEMENT DEVELOPMENT TRAINING	\$3,260,200	\$ 17,666,322	6/7/07	5/6/08	COMBINATI ON (APPLIES TO AWARDS WHERE TWO OR MORE OF THE ABOVE APPLY)
LOCKHEED MARTIN TECHNICAL SERVICES INCORPORATED	PROFESSIONAL AND MANAGEMENT DEVELOPMENT TRAINING	\$3,422,720	\$3,422,720	7/26/07	12/31/07	COMBINATI ON (APPLIES TO AWARDS WHERE TWO OR MORE OF THE ABOVE APPLY)
LTM INCORPORATED	OTHER COMPUTER RELATED SERVICES	\$7,601,263	\$7,601,263	8/30/07	9/30/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
MISCELLANEOUS FOREIGN CONTRACTORS	HOTELS (EXCEPT CASINO HOTELS) AND MOTELS	\$600,000	\$1,163,360	1/18/07	7/18/07	FIXED PRICE
NOBLE SALES COMPANY INCORPORATED	HARDWARE STORES	\$1,019,951	\$1,019,951	6/28/07	4/10/11	FIXED PRICE
NOMADICS INCORPORATED	OTHER APPAREL ACCESSORIES AND OTHER APPAREL MANUFACTURING	\$3,382,509	\$3,382,509	8/31/07	4/1/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
NORTHROP GRUMMAN SPACE AND MISSION SYSTEMS CORPORATION	ADMINISTRATIVE MANAGEMENT AND GENERAL MANAGEMENT CONSULTING SERVICES	\$3,820,435	\$3,820,435	8/6/07	11/26/07	FIXED PRICE
NORTHROP GRUMMAN SYSTEMS CORPORATION (5430)	ENGINEERING SERVICES	\$ -	\$ 25,271,315	12/29/06	2/28/07	FIXED PRICE
NORTHROP GRUMMAN SYSTEMS CORPORATION (5430)	ENGINEERING SERVICES	\$ -	\$ 37,447,568	2/22/07	3/31/07	FIXED PRICE
NORTHROP GRUMMAN SYSTEMS CORPORATION (5430)	ENGINEERING SERVICES	\$ -	\$ 30,617,561	3/30/07	6/30/07	FIXED PRICE
NORTHROP GRUMMAN SYSTEMS CORPORATION (5430)	ENGINEERING SERVICES	\$4,200,000	\$4,300,085	3/20/07	6/28/07	FIXED PRICE

NORTHROP GRUMMAN SYSTEMS CORPORATION (5430)	ENGINEERING SERVICES	\$1,113,395	\$1,113,395	5/7/07	6/28/07	FIXED PRICE
OBERON ASSOCIATES INCORPORATED	CUSTOM COMPUTER PROGRAMMING SERVICES	\$1,561,331	\$1,561,331	4/3/07	5/17/08	TIME AND MATERIALS
OMNIPLEX WORLD SERVICES CORPORATION	SECURITY GUARDS AND PATROL SERVICES	\$6,427,385	\$6,439,632	2/15/07	1/14/08	LABOR HOURS
ONYX OF ALEXANDRIA INCORPORATED	CUSTOM COMPUTER PROGRAMMING SERVICES	\$1,211,537	\$1,211,537	9/21/07	9/23/08	FIXED PRICE
ORACLE SOLUTION AND SERVICES LIMITED LIABILITY COMPANY	CUSTOM COMPUTER PROGRAMMING SERVICES	\$1,378,960	\$1,378,960	1/23/07	1/31/08	FIXED PRICE
P3 PARTNERS LIMITED LIABILITY COMPANY	ALL OTHER PROFESSIONAL, SCIENTIFIC, AND TECHNICAL SERVICES	\$2,000,000	\$2,000,000	7/6/07	7/4/10	FIXED PRICE
PERFORMANCE ASSESSMENT NETWORK INCORPORATED	HUMAN RESOURCES CONSULTING SERVICES (2007), HUMAN RESOURCES AND EXECUTIVE SEARCH CONSULTING SERVICES (2002)	\$1,172,877	\$1,172,877	5/24/07	5/31/07	FIXED PRICE
PLANNING SYSTEMS INCORPORATED	NATIONAL SECURITY	\$3,000,000	\$3,000,000	9/21/07	9/21/09	FIXED PRICE
PRAGMATICS INCORPORATED	COMPUTER SYSTEMS DESIGN SERVICES	\$780,000	\$5,187,427	9/25/07	9/24/08	LABOR HOURS
PRICEWATERHOUSECOOPERS LLP (8324)	ADMINISTRATIVE MANAGEMENT AND GENERAL MANAGEMENT CONSULTING SERVICES	\$2,512,631	\$2,512,631	8/20/07	9/19/08	FIXED PRICE
PRICEWATERHOUSECOOPERS LLP (8324)	ADMINISTRATIVE MANAGEMENT AND GENERAL MANAGEMENT CONSULTING SERVICES	\$1,015,381	\$1,015,381	9/10/07	9/19/08	FIXED PRICE
PROFESSIONAL SOLUTIONS LIMITED LIABILITY COMPANY	OTHER SCIENTIFIC AND TECHNICAL CONSULTING SERVICES	\$1,559,572	\$1,559,572	5/1/07	4/30/12	FIXED PRICE
PROGRAM MANGT ASSO	ADMINISTRATIVE MANAGEMENT AND GENERAL MANAGEMENT CONSULTING SERVICES	\$3,340,403	\$3,340,403	4/3/07	6/27/09	FIXED PRICE
RAPISCAN SECURITY PRODUCTS (USA) INCORPORATED	SEARCH, DETECTION, NAVIGATION, GUIDANCE, AERONAUTICAL, AND NAUTICAL SYSTEM AND INSTRUMENT MANUFACTURING	\$9,269,768	\$9,269,768	9/27/07	9/25/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)

RAYTHEON TECHNICAL SERVICES COMPANY LIMITED LIABILITY COMPANY (5772)	ENGINEERING SERVICES	\$1,383,275	\$1,383,275	5/31/07	10/31/07	LABOR HOURS
RAYTHEON TECHNICAL SERVICES COMPANY LIMITED LIABILITY COMPANY (5772)	ENGINEERING SERVICES	\$3,000,000	\$3,000,000	4/6/07	4/5/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
RAYTHEON TECHNICAL SERVICES COMPANY LIMITED LIABILITY COMPANY (5772)	ENGINEERING SERVICES	\$ 11,069,664	\$ 11,069,664	9/20/07	4/5/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
RAYTHEON TECHNICAL SERVICES COMPANY LIMITED LIABILITY COMPANY (5772)	ENGINEERING SERVICES	\$5,496,000	\$5,496,000	9/19/07	9/18/08	TIME AND MATERIALS
RAYTHEON TECHNICAL SERVICES COMPANY LIMITED LIABILITY COMPANY (5772)	SECURITY GUARDS AND PATROL SERVICES	\$2,016,050	\$2,016,050	5/24/07	9/30/11	COST PLUS AWARD FEE
RESOURCE MANAGEMENT CONCEPTS,	ENVIRONMENTAL CONSULTING SERVICES	\$3,039,972	\$3,039,972	6/12/07	7/11/09	FIXED PRICE
REVEAL IMAGING TECHNOLOGIES INCORPORATED	ALL OTHER MISCELLANEOUS MANUFACTURING	\$9,856,500	\$9,856,500	2/8/07	9/30/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
REVEAL IMAGING TECHNOLOGIES INCORPORATED	ALL OTHER MISCELLANEOUS MANUFACTURING	\$ 11,168,200	\$ 11,168,200	6/20/07	9/30/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
REVEAL IMAGING TECHNOLOGIES INCORPORATED	ALL OTHER MISCELLANEOUS MANUFACTURING	\$1,097,400	\$1,097,400	8/29/07	9/23/10	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)

REVEAL IMAGING TECHNOLOGIES INCORPORATED	ALL OTHER MISCELLANEOUS MANUFACTURING	\$ 10,758,600	\$ 10,758,600	9/11/07	9/23/10	COMBINATI ON (APPLIES TO AWARDS WHERE TWO OR MORE OF THE ABOVE APPLY)
REVEAL IMAGING TECHNOLOGIES INCORPORATED	SEARCH, DETECTION, NAVIGATION, GUIDANCE, AERONAUTICAL, AND NAUTICAL SYSTEM AND INSTRUMENT MANUFACTURING	\$5,865,710	\$5,865,710	9/26/07	9/25/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
ROBBINS GIOIA LIMITED LIABILITY COMPANY	ADMINISTRATIVE MANAGEMENT AND GENERAL MANAGEMENT CONSULTING SERVICES	\$1,879,565	\$1,879,565	11/17/06	12/26/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
ROBBINS GIOIA LIMITED LIABILITY COMPANY	ADMINISTRATIVE MANAGEMENT AND GENERAL MANAGEMENT CONSULTING SERVICES	\$3,267,671	\$3,267,671	2/12/07	6/27/09	LABOR HOURS
ROBBINS GIOIA LIMITED LIABILITY COMPANY	ADMINISTRATIVE MANAGEMENT AND GENERAL MANAGEMENT CONSULTING SERVICES	\$1,382,901	\$1,382,901	8/16/07	6/27/09	LABOR HOURS
SCIENCE APPLICATIONS INTERNATIONAL CORPORATION	ENGINEERING SERVICES	\$4,053,877	\$4,053,877	12/26/06	3/31/07	COMBINATI ON (APPLIES TO AWARDS WHERE TWO OR MORE OF THE ABOVE APPLY)
SCIENCE APPLICATIONS INTERNATIONAL CORPORATION	ENGINEERING SERVICES	\$1,400,000	\$1,400,000	3/28/07	6/30/07	COMBINATI ON (APPLIES TO AWARDS WHERE TWO OR MORE OF THE ABOVE APPLY)
SCIENCE APPLICATIONS INTERNATIONAL CORPORATION	ENGINEERING SERVICES	\$1,350,000	\$1,350,000	4/6/07	6/30/07	COMBINATI ON (APPLIES TO AWARDS WHERE TWO OR MORE OF THE ABOVE APPLY)
SCIENCE APPLICATIONS INTERNATIONAL CORPORATION	ENGINEERING SERVICES	\$2,239,217	\$2,239,217	6/15/07	12/31/07	COMBINATI ON (APPLIES TO AWARDS WHERE TWO OR MORE OF THE ABOVE APPLY)

SCIENCE APPLICATIONS INTERNATIONAL CORPORATION	ENGINEERING SERVICES	\$1,299,508	\$1,299,508	11/30/06	9/30/07	COST PLUS AWARD FEE
SCIENCE APPLICATIONS INTERNATIONAL CORPORATION	REMEDATION SERVICES	\$6,931,922	\$6,931,922	10/24/06	9/14/11	FIXED PRICE
SCIENCE APPLICATIONS INTERNATIONAL CORPORATION	COMPUTER FACILITIES MANAGEMENT SERVICES	\$818,113	\$1,460,145	8/30/07	8/31/08	COST PLUS AWARD FEE
SETA CORPORATION	CUSTOM COMPUTER PROGRAMMING SERVICES	\$1,628,419	\$1,628,419	1/5/07	1/11/09	COST PLUS AWARD FEE
SETA CORPORATION	CUSTOM COMPUTER PROGRAMMING SERVICES	\$4,885,257	\$4,885,257	4/10/07	1/11/09	COST PLUS AWARD FEE
SETA CORPORATION	CUSTOM COMPUTER PROGRAMMING SERVICES	\$1,809,276	\$1,809,276	1/10/07	1/11/09	COST PLUS AWARD FEE
SIEMENS MAINTENANCE SERVICES LIMITED LIABILITY COMPANY	PROCESS, PHYSICAL DISTRIBUTION, AND LOGISTICS CONSULTING SERVICES	\$ 84,856,595	\$ 84,856,595	10/26/06	9/30/07	FIXED PRICE
SIEMENS MAINTENANCE SERVICES LIMITED LIABILITY COMPANY	PROCESS, PHYSICAL DISTRIBUTION, AND LOGISTICS CONSULTING SERVICES	\$6,250,000	\$6,250,000	2/6/07	9/30/07	FIXED PRICE
SIEMENS MAINTENANCE SERVICES LIMITED LIABILITY COMPANY	PROCESS, PHYSICAL DISTRIBUTION, AND LOGISTICS CONSULTING SERVICES	\$1,500,000	\$1,500,000	3/20/07	9/30/07	FIXED PRICE
SIEMENS MAINTENANCE SERVICES LIMITED LIABILITY COMPANY	PROCESS, PHYSICAL DISTRIBUTION, AND LOGISTICS CONSULTING SERVICES	\$ 10,000,000	\$ 10,000,000	7/26/07	9/30/08	FIXED PRICE
SMITHS DETECTION DANBURY	SEARCH, DETECTION, NAVIGATION, GUIDANCE, AERONAUTICAL, AND NAUTICAL SYSTEM AND INSTRUMENT MANUFACTURING	\$6,853,316	\$6,853,316	3/30/07	3/28/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
SMITHS DETECTION DANBURY	SEARCH, DETECTION, NAVIGATION, GUIDANCE, AERONAUTICAL, AND NAUTICAL SYSTEM AND INSTRUMENT MANUFACTURING	\$ 16,533,682	\$ 16,533,682	5/8/07	5/8/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
SMITHS DETECTION INCORPORATED (2823)	SEARCH, DETECTION, NAVIGATION, GUIDANCE, AERONAUTICAL, AND NAUTICAL SYSTEM AND INSTRUMENT MANUFACTURING	\$ 20,960,000	\$ 20,960,000	9/26/07	9/26/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)

ST NET APPTIS FIRSTSOURCE JOINT VENTURE	OTHER COMPUTER RELATED SERVICES	\$1,081,374	\$1,081,374	6/18/07	7/18/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
SYSTEMS INTEGRATION INCORPORATED	OTHER COMPUTER RELATED SERVICES	\$6,471,806	\$6,471,806	3/8/07	4/30/09	FIXED PRICE AWARD FEE
SYSTEMS RESEARCH AND APPLICATI	ADMINISTRATIVE MANAGEMENT AND GENERAL MANAGEMENT CONSULTING SERVICES	\$2,018,730	\$2,018,730	12/1/06	12/31/07	FIXED PRICE LEVEL OF EFFORT
SYTEX INCORPORATED	OTHER APPAREL ACCESSORIES AND OTHER APPAREL MANUFACTURING	\$1,786,432	\$1,786,432	8/24/07	12/27/10	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
SYTEX, INC.	OTHER APPAREL ACCESSORIES AND OTHER APPAREL MANUFACTURING	\$1,781,692	\$1,781,692	1/3/07	12/27/10	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
SYTEX, INC.	OTHER APPAREL ACCESSORIES AND OTHER APPAREL MANUFACTURING	\$1,400,000	\$1,400,000	4/2/07	12/27/10	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
THE MITRE CORPORATION	ENGINEERING SERVICES	\$3,301,917	\$3,301,917	1/29/07	10/1/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
TKC TECHNOLOGY SOLUTIONS LIMITED LIABILITY COMPANY	DATA PROCESSING, HOSTING, AND RELATED SERVICES	\$1,693,250	\$1,693,250	11/20/06	9/30/07	FIXED PRICE
TOTAL ENTERPRISES INCORPORATED	FINANCIAL TRANSACTIONS PROCESSING, RESERVE, AND CLEARINGHOUSE ACTIVITIES	\$1,808,355	\$3,530,611	12/22/06	12/31/07	FIXED PRICE
UNISYS CORPORATION	ALL OTHER SUPPORT SERVICES	\$2,907,407	\$2,907,407	1/9/07	12/31/07	FIXED PRICE
UNISYS CORPORATION	ALL OTHER SUPPORT SERVICES	\$2,254,571	\$2,254,571	12/11/06	12/31/07	FIXED PRICE
UNISYS CORPORATION	ALL OTHER SUPPORT SERVICES	\$4,992,750	\$4,992,750	9/27/07	6/30/08	FIXED PRICE

UNISYS CORPORATION	ALL OTHER SUPPORT SERVICES	\$2,211,294	\$2,211,294	10/26/06	10/31/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
UNISYS CORPORATION	ALL OTHER SUPPORT SERVICES	\$2,087,616	\$2,087,616	10/26/06	10/31/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
UNISYS CORPORATION	ALL OTHER SUPPORT SERVICES	\$1,044,633	\$1,044,633	12/20/06	12/31/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
UNISYS CORPORATION	ALL OTHER SUPPORT SERVICES	\$3,310,186	\$3,310,186	5/15/07	12/31/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
UNISYS CORPORATION	ALL OTHER SUPPORT SERVICES	\$1,268,984	\$1,268,984	7/12/07	12/31/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
UNISYS CORPORATION	ALL OTHER SUPPORT SERVICES	\$1,583,046	\$1,583,046	1/17/07	7/31/07	FIXED PRICE
UNISYS CORPORATION	ALL OTHER SUPPORT SERVICES	\$1,059,048	\$1,059,048	1/29/07	12/31/07	FIXED PRICE
UNISYS CORPORATION	ALL OTHER SUPPORT SERVICES	\$1,359,843	\$1,359,843	1/10/07	9/30/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
UNISYS CORPORATION	ALL OTHER SUPPORT SERVICES	\$2,195,680	\$2,195,680	5/11/07	5/10/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
UNISYS CORPORATION	ALL OTHER SUPPORT SERVICES	\$7,254,468	\$7,254,468	12/5/06	9/30/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)

UNISYS CORPORATION	ALL OTHER SUPPORT SERVICES	\$1,098,336	\$1,098,336	12/28/06	3/31/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
UNISYS CORPORATION	ALL OTHER SUPPORT SERVICES	\$4,208,614	\$4,208,614	5/3/07	9/30/07	FIXED PRICE
UNISYS CORPORATION	ALL OTHER SUPPORT SERVICES	\$2,188,075	\$2,188,075	9/13/07	12/31/07	FIXED PRICE
UNISYS CORPORATION	ALL OTHER SUPPORT SERVICES	\$ 82,912,931	\$ 82,912,931	1/1/07	3/31/07	FIXED PRICE
UNISYS CORPORATION	ALL OTHER SUPPORT SERVICES	\$ 24,708,805	\$ 24,708,805	3/30/07	12/31/07	FIXED PRICE
UNISYS CORPORATION	ALL OTHER SUPPORT SERVICES	\$ 25,298,689	\$ 25,298,689	7/1/07	12/31/07	FIXED PRICE
UNISYS CORPORATION	ALL OTHER SUPPORT SERVICES	\$ 24,114,515	\$ 24,114,515	9/10/07	12/31/07	FIXED PRICE
UNISYS CORPORATION	ALL OTHER SUPPORT SERVICES	\$1,530,581	\$1,530,581	1/23/07	9/30/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
UNISYS CORPORATION	ALL OTHER SUPPORT SERVICES	\$1,052,469	\$1,052,469	3/23/07	12/31/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
UNISYS CORPORATION	ALL OTHER SUPPORT SERVICES	\$2,381,624	\$2,381,624	8/20/07	12/31/07	FIXED PRICE
UNISYS CORPORATION	ALL OTHER SUPPORT SERVICES	\$1,756,240	\$1,756,240	3/29/07	12/31/07	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
UNISYS CORPORATION	ALL OTHER SUPPORT SERVICES	\$1,294,541	\$1,294,541	8/23/07	8/15/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
UNISYS CORPORATION	ALL OTHER SUPPORT SERVICES	\$1,683,512	\$1,683,512	7/26/07	8/31/08	OTHER (APPLIES TO AWARDS WHERE NONE OF THE ABOVE APPLY)
UNISYS CORPORATION	ALL OTHER SUPPORT SERVICES	\$1,262,670	\$1,262,670	9/12/07	9/11/08	TIME AND MATERIALS
UNISYS CORPORATION	ALL OTHER SUPPORT SERVICES	\$1,049,217	\$1,049,217	8/13/07	12/31/07	TIME AND MATERIALS

VF IMAGEWEAR INCORPORATED	INDUSTRIAL LAUNDERERS	\$8,500,000	\$8,500,000	2/21/07	3/31/08	FIXED PRICE
VF IMAGEWEAR INCORPORATED	INDUSTRIAL LAUNDERERS	\$4,000,000	\$ 40,124,476	7/18/07	6/30/08	FIXED PRICE
VIC THOMPSON COMPANY	ENGINEERING SERVICES	\$1,119,404	\$1,119,404	12/19/06	2/22/07	FIXED PRICE
VIC THOMPSON COMPANY	ENGINEERING SERVICES	\$2,877,283	\$2,877,283	3/21/07	3/21/08	TIME AND MATERIALS
WRIGHT SOLUTIONS, INC.	OFFICE ADMINISTRATIVE SERVICES	\$222,982	\$1,962,051	3/19/07	3/22/08	FIXED PRICE
INFINITY TECHNOLOGY, LLC	PROGRAM MANAGEMENT/SUPPORT SERVICES	\$171,360	\$171,360	05/26/2008	06/22/2009	TIME AND MATERIALS
TRIUMPH ENTERPRISES, INCORPORATED	PROGRAM MANAGEMENT/SUPPORT SERVICES	\$480,473		08/01/2008	08/03/2009	FIXED PRICE LEVEL OF EFFORT
E L HAMM & ASSOCIATES INCORPORATED	LOGISTICS SUPPORT SERVICES	\$850,000	\$850,000	09/30/2008	03/13/2013	FIRM FIXED PRICE
TERACORE, INC	ADP SYSTEMS DEVELOPMENT SERVICES	\$135,648	\$135,648	09/15/2008	09/28/2010	LABOR HOURS
INTERNATIONAL BUSINESS MACHINES CORPORATION	TECHNICAL ASSISTANCE	\$1,201,082	\$1,201,082	02/01/2008	10/31/2009	FIRM FIXED PRICE
MIRACLE SYSTEMS LIMITED LIABILITY COMPANY	PROGRAM MANAGEMENT/SUPPORT SERVICES	\$1,270,087	\$1,270,087	02/29/2008	03/02/2010	FIRM FIXED PRICE
GMG MANAGEMENT CONSULTING INC.	FINANCIAL SERVICES	\$528,870		03/04/2008	03/31/2011	FIRM FIXED PRICE
SOLUTIONS THROUGH INNOVATIVE TECHNOLOGIES INC	AUDITING SERVICES	\$199,938	\$199,938	09/18/2008	09/28/2012	FIRM FIXED PRICE
JSIG, JOINT SECURITY INFRASTRUCTURE GROUP, INC.	MAINT-REP OF ELECT-ELCT EQ	\$185,270	\$185,270	09/15/2008	09/15/2011	FIRM FIXED PRICE
AMTIS, INC.	TRAINING AIDS	\$171,818	\$171,818	09/15/2008	10/28/2011	FIRM FIXED PRICE
TRIUMPH ENTERPRISES, INCORPORATED	OTHER PROFESSIONAL SERVICES	\$3,123,740	\$3,123,740	05/30/2008	06/02/2009	FIRM FIXED PRICE
SEKON ENTERPRISE, INC.	OTHER PROFESSIONAL SERVICES	\$275,000	\$275,000	09/15/2008	09/15/2009	LABOR HOURS
TACTICAL OFFICE SOLUTIONS	INSTALL OF FURNITURE	\$250,000	\$250,000	06/18/2008	06/18/2012	TIME AND MATERIALS
PREFERRED BUILDING SVC INC	CUSTODIAL JANITORIAL SERVICES	\$12,240	\$12,240	08/20/2008	09/14/2011	FIRM FIXED PRICE
THOMAS CONSTRUCTION COMPANY, INC.	CONSTRUCTION (BASIC)	\$183,237	\$183,237	09/02/2008	11/14/2008	FIRM FIXED PRICE
TERACORE, INC	PROGRAM MANAGEMENT/SUPPORT SERVICES	\$701,926		06/14/2008	06/13/2009	FIRM FIXED PRICE
MACROSYS RESEARCH & TECHNOLOGY	DATA COLLECTION SERVICES	\$192,435	\$192,435	04/07/2008	12/24/2011	FIRM FIXED PRICE
BANNER STAFFING	OTHER ADMINISTRATIVE SUPPORT SVCS	\$71,980	\$71,980	03/13/2008	03/14/2009	FIRM FIXED PRICE
CONSOLIDATED SAFETY SERVICES INCORPORATED	SCIENTIFIC DATA STUDIES	\$173,300	\$173,300	07/14/2008	07/13/2009	ORDER DEPENDENT

LOCKHEED MARTIN INTEGRATED SYSTEMS, INC	SERVICES (MANAGEMENT/SUPPORT)	\$195,140,022	\$195,140,022	07/03/2008	01/02/2017	FIXED PRICE AWARD FEE
KOLA NUT TRAVEL INC	TRAVEL AGENT SERVICES	\$49,996	\$49,996	09/15/2008	10/31/2009	FIRM FIXED PRICE
DELOITTE CONSULTING L.L.P.	OTHER PROFESSIONAL SERVICES	\$822,970	\$822,970	05/01/2008	06/16/2008	LABOR HOURS
FREIGHTDESK TECHNOLOGIES, INC	OTHER PROFESSIONAL SERVICES	\$400,000	\$400,000	06/24/2008	02/23/2009	FIRM FIXED PRICE
RAILINC CORP.	DATA COLLECTION SERVICES	\$123,000	\$123,000	09/26/2008	09/25/2013	FIRM FIXED PRICE
BAYFIRST SOLUTIONS LLC	OTHER PROFESSIONAL SERVICES	\$398,280	\$398,280	04/01/2008	12/04/2008	FIRM FIXED PRICE
BAYFIRST SOLUTIONS LLC	OTHER PROFESSIONAL SERVICES	\$847,600	\$847,600	09/08/2008	09/30/2009	LABOR HOURS
PROFESSIONAL SOLUTIONS LLC	MISCELLANEOUS ITEMS	\$1,852,900	\$1,852,900	09/30/2008	09/29/2018	COST PLUS FIXED FEE
ID SOLUTIONS INCORPORATED	ADP SOFTWARE	\$427,270	\$427,270	02/19/2008	02/18/2012	FIRM FIXED PRICE
ACCENTURE NATIONAL SECURITY SERVICES, LLC	MISCELLANEOUS ITEMS	\$11,366,149	\$11,366,149	09/03/2008	09/02/2013	ORDER DEPENDENT
CAPITAL CARD SYSTEMS INCORPORATED	MISC MATERIALS HANDLING EQ	\$305,243	\$305,243	12/30/2008	12/30/2012	FIRM FIXED PRICE
DATACARD CORPORATION	PLASTICS FABRICATED MATERIALS	\$547,995	\$547,995	01/04/2008	01/04/2013	FIRM FIXED PRICE
AITHERAS, LLC	TECH REP SVCS/ADP EQ & SUPPLIES	\$996,547	\$996,547	12/19/2008	12/18/2009	LABOR HOURS
BOOZ ALLEN HAMILTON INC.	PROGRAM MANAGEMENT/SUPPORT SERVICES	\$1,338,154	\$1,338,154	11/17/2008	11/23/2013	ORDER DEPENDENT
MANAGEMENT SOLUTIONS, INC.	CONSTRUCTION OF OFFICE BUILDINGS	\$2,133,000	\$2,133,000	09/23/2008	09/23/2008	FIRM FIXED PRICE
EXECUTIVE TECHNOLOGY, INC.	OTHER ADP & TELECOMMUNICATIONS SVCS	\$530,187	\$530,187	04/18/2008	04/17/2010	FIRM FIXED PRICE
EXTROPY GROUP, LLC	OTHER ADP & TELECOMMUNICATIONS SVCS	\$1,189,595	\$1,189,595	09/09/2008	09/10/2009	FIRM FIXED PRICE
ALON INC	OTHER ADP & TELECOMMUNICATIONS SVCS	\$748,280	\$748,280	09/30/2008	09/25/2009	FIRM FIXED PRICE
ADVERTISING COUNCIL, INC. THE	MISCELLANEOUS ITEMS	\$1,299,980	\$1,299,980	09/16/2008	09/23/2009	COST PLUS FIXED FEE
SAPIENT GOVERNMENT SERVICES, INC	COMMUNICATIONS SERVICES	\$646,596	\$646,596	05/29/2008	05/28/2009	FIRM FIXED PRICE
CENTER FOR CONFLICT RESOLUTION, INC., THE	OTHER SPECIAL STUDIES AND ANALYSES	\$241,500	\$241,500	09/30/2008	09/30/2012	FIRM FIXED PRICE
ALION SCIENCE AND TECHNOLOGY CORPORATION	ADP SOFTWARE	\$76,864	\$128,502	07/31/2008	08/03/2013	FIRM FIXED PRICE
BAYFIRST SOLUTIONS LLC	PROGRAM EVALUATION SERVICES	\$74,793	\$74,793	03/06/2008	07/08/2008	LABOR HOURS
NATIONAL LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEMS INCORPORATED	MISCELLANEOUS ITEMS	\$48,000	\$48,000	11/14/2008	12/31/2009	FIRM FIXED PRICE
ACE INFO SOLUTIONS, INC.	MISCELLANEOUS ITEMS	\$1,400,000	\$1,400,000	09/02/2008	09/21/2013	LABOR HOURS

OMNIPLEX WORLD SERVICES CORP	GUARD SERVICES	\$2,106,777	\$2,106,777	09/30/2008	12/15/2009	FIRM FIXED PRICE
GAP SOLUTIONS, INC.	OTHER PROFESSIONAL SERVICES	\$0	\$0	10/22/2008	10/22/2009	FIRM FIXED PRICE
SIM-G TECHNOLOGIES, LLC	MISC ALARM, SIGNAL, SEC SYSTEMS	\$1,072,595	\$1,072,595	06/20/2008	06/20/2009	FIRM FIXED PRICE
L-3 COMMUNICATIONS CORPORATION	MISC ALARM, SIGNAL, SEC SYSTEMS	\$2,845,147	\$2,845,147	09/30/2008	09/30/2010	FIRM FIXED PRICE
SURESCAN CORPORATION	MISC ALARM, SIGNAL, SEC SYSTEMS	\$5,257,796	\$5,257,796	10/07/2008	09/30/2009	FIRM FIXED PRICE
RAPISCAN SYSTEMS NEUTRONICS AND ADVANCED TECHNOLOGIES CORPOR	MISC ALARM, SIGNAL, SEC SYSTEMS	\$5,792,325	\$5,792,325	10/07/2008	09/30/2009	FIRM FIXED PRICE
SMITHS DETECTION INC.	MAINT-REP OF ALARM & SIGNAL SYSTEM	\$6,078,005	\$6,078,005	09/30/2008	09/29/2009	FIRM FIXED PRICE
VIC THOMPSON COMPANY	CONSTRUCT/OTHER ADMIN & SVCS BLDGS	\$22,797,901	\$22,797,901	04/18/2008	09/14/2011	FIRM FIXED PRICE
PLANNING SYSTEMS INCORPORATED	MISC ALARM, SIGNAL, SEC SYSTEMS	\$2,355,656	\$2,355,656	08/27/2008	09/21/2009	FIRM FIXED PRICE
LOGICAL ESSENCE LLC	STUDY/DATA - OTHER THAN SCIENTIFIC	\$652,871	\$652,871	11/14/2008	11/13/2009	FIRM FIXED PRICE
CARTER AND BURGESS INCORPORATED	PROGRAM MANAGEMENT/SUPPORT SERVICES	\$2,478,562	\$2,478,562	12/10/2008	04/30/2009	FIRM FIXED PRICE
GENERAL PROJECTION SYSTEMS, INC.	INSTALL OF MISC EQ	\$45,841	\$45,841	08/12/2008	11/07/2008	FIRM FIXED PRICE
BATTLE RESOURCE MANAGEMENT, INC	PROGRAM MANAGEMENT/SUPPORT SERVICES	\$190,944	\$190,944	09/23/2008	03/22/2010	FIRM FIXED PRICE
SKYLINE MANAGEMENT GROUP	CUSTODIAL JANITORIAL SERVICES	\$198,218	\$198,218	03/31/2008	03/31/2013	FIRM FIXED PRICE
GRAND RAPIDS BUILDING SERVICES, INC	CUSTODIAL JANITORIAL SERVICES	\$5,856	\$5,856	03/26/2008	03/25/2009	FIRM FIXED PRICE
AMERICAN ALUMINUM ACCESSORIES INC	SPECIAL METAL CONTAINER MFG MACH	\$144,075	\$144,075	05/23/2008	10/30/2010	FIRM FIXED PRICE
DIXON GROUP, INC., (THE)	PATENT AND TRADEMARK SERVICES	\$91,024	\$91,024	08/01/2008	12/05/2008	FIRM FIXED PRICE
TURNER, MARSHA	CUSTODIAL JANITORIAL SERVICES	\$206,000	\$206,000	08/12/2008	09/01/2009	FIRM FIXED PRICE
DIAMOND SERVICES, INC	CUSTODIAL JANITORIAL SERVICES	\$48,228	\$48,228	09/19/2008	09/18/2009	FIRM FIXED PRICE
XTK CLEANING	CUSTODIAL JANITORIAL SERVICES	\$15,600	\$15,600	09/26/2008	09/25/2013	FIRM FIXED PRICE
DAY CONSULTANTS, INC.	OTHER PROFESSIONAL SERVICES	\$315,808	\$315,808	09/23/2008	07/23/2013	FIRM FIXED PRICE
DIAMOND SERVICES, INC	CUSTODIAL JANITORIAL SERVICES	\$72,360	\$72,360	09/22/2008	09/21/2013	FIRM FIXED PRICE
FIRSTLINE TRANSPORTATION SECURITY INCORPORATED	GUARD SERVICES	\$363,313	\$363,313	01/14/2008	10/22/2008	COST PLUS AWARD FEE
INNOVATA LIMITED LIABILITY COMPANY	DATA COLLECTION SERVICES	\$51,700	\$51,700	01/30/2008	12/13/2012	FIRM FIXED PRICE
MISCELLANEOUS FOREIGN CONTRACTORS	EDUCATIONAL SERVICES	\$7,300	\$7,300	02/04/2008	12/31/2008	FIRM FIXED PRICE

DESERT LAKES HOLDINGS	OTHER ED & TRNG SVCS	\$27,500	\$27,500	02/19/2008	12/31/2008	FIRM FIXED PRICE
PRESTIGE BUILDING SERVICES LLC	CUSTODIAL JANITORIAL SERVICES	\$13,200	\$13,200	03/27/2008	03/31/2009	FIRM FIXED PRICE
A.B.P. MAINTENANCE CORP.	CUSTODIAL JANITORIAL SERVICES	\$22,395	\$22,395	03/27/2008	03/31/2009	FIRM FIXED PRICE
AVALANCHE AIR CONDITIONING & HEATING INC	MAINT-REP OF PLUMBING-HEATING EQ	\$6,203	\$6,203	03/31/2008	03/31/2009	FIRM FIXED PRICE
FAB CONSTRUCTION INC	CONSTRUCTION (BASIC)	\$232,700	\$232,700	08/29/2008	12/29/2008	FIRM FIXED PRICE
NASSAU, COUNTY OF	EDUCATIONAL SERVICES	\$66,407	\$66,407	09/22/2008	09/30/2009	FIRM FIXED PRICE
SMITH, JOHN E	INFORMATION TRAINING	\$111,355	\$111,355	09/22/2008	02/16/2009	FIRM FIXED PRICE
NEWTON DESIGN & FABRICATION, INC.	AIRFRAME STRUCTURAL COMPONENTS	\$7,295,558	\$7,295,558	09/17/2008	09/25/2009	FIRM FIXED PRICE
CHAMPION ARMS	EDUCATIONAL SERVICES	\$39,600	\$39,600	11/05/2008	11/09/2009	FIRM FIXED PRICE
RAMOS CLEANING, LLC.	CUSTODIAL JANITORIAL SERVICES	\$30,768	\$30,768	11/05/2008	12/05/2008	FIRM FIXED PRICE

Question: Please provide for the record a list of all TSA contracts, grants and other transactions where work is performed outside of the United States. Organize by contractor, purpose, dollar award, full performance value, contract start date, and contract end date.

ANSWER: The following chart provides information regarding contracts where work was performed outside the United States from October 1, 2004, through March 24, 2009. No grants or other transactions were performed outside the United States.

Contractor	Purpose	Dollar Award	Full Performance Value	Contract Start Date	Contract End Date
EKMAN GROUP TRAINING DIVISION THE	TRAINING AIDS	\$990,900	\$1,044,900	07/13/2007	08/18/2007
SOREQ NAHAL SOREQ NUCLEAR RESEARCH CENTER	R&D-OTHER R & D-OPSY DEV	\$1,316,669	\$1,316,669	09/29/2005	09/29/2007

QUESTIONS FOR THE RECORD SUBMITTED BY

CHAIRMAN DAVID PRICE

W. Ross Ashley, Assistant Administrator of Grant Programs,
Federal Emergency Management Agency
Securing the Nation's Rail and Transit Systems

Transit and Passenger Rail Grant Funding

Question: TSA and FEMA are both involved in the grant process: TSA determines the criteria and what is eligible to receive a grant while FEMA distributes the funding. According to GAO, transit agencies have reported that the lack of predictability in how TSA will assess grant projects against funding priorities makes it difficult to engage in long-term planning of security initiatives. Specifically, transit agencies have reported receiving funding to begin projects—such as retrofitting their transit fleet with security cameras or installing digital video recording systems—but are not able to finish these projects in subsequent years because TSA had changed its funding priorities. Mr. Ashley, who's responsible for deciding priorities, FEMA or TSA?

ANSWER: FEMA and TSA work together on developing priorities for each year's grant guidance. In addition, we both work with external stakeholders to solicit ideas on process improvements and potential focus areas for the next year. TSA is the subject matter expert for the TSGP grants, while FEMA provides the expertise for grants management function within the grants.

Question: Mr. Ashley, please explain how transit agencies are to complete long term projects, which usually address large vulnerabilities, if the rules of the game continue to change?

ANSWER: FEMA partners with the Transportation Security Administration (TSA) as the subject matter experts for the transportation sector, in administration of the Transit Security Grant Program. Each year, the Program Guidance is enhanced with input from our stakeholders, including transit agencies and national associations. This input is reviewed by both FEMA and TSA and where feasible, incorporated into the program development process. Although the rules may change for newly funded projects each fiscal year, grantees are given a three year period of performance for each specific grant award to complete their projects, with the opportunity to request an extension of the period if necessary. This ensures funding remains available and projects can be completed as proposed. FEMA and TSA program staff work closely with our transit partners on a daily basis to assist them throughout the grant process.

Question: The Committee has heard numerous complaints from mass transit and passenger rail entities that TSA does not support investments in complex infrastructure hardening projects which require multi-year funding. States have also noted that without the ability to plan and undertake long term projects, funds will be used for off-the-shelf technologies, such as closed circuit television cameras, which may not mitigate risk as much as more ambitious projects would do. How do you respond to these concerns? What is FEMA's involvement to make sure that multi-year, complex infrastructure investments are funded?

ANSWER: Complex infrastructure hardening projects requiring multi-year funding should be evaluated on their risk reduction benefit and approved in a phased approach that allows each successive phase to be funded

with the next grant cycle. DHS, in evaluating these types of projects, must be made aware of the entire scope and its' individual phases in order to address risk reduction on a holistic basis. Using a multi-year funding approach based the appropriations process is challenging, as public transportation agencies and DHS are hesitant to invest in phased projects that are dependent on future appropriations for completion. Therefore, each phase should accomplish measurable risk reduction.

FEMA continues to support mass transit and passenger rail entities in their efforts to reduce and mitigate risk by infrastructure hardening. FEMA has encouraged the hardening of infrastructure that requires multi-year funding by suggesting a phased approach with successive phases funded each grant cycle. The advantage to this process is the greater flexibility in managing and allowing for changes in progressive phases. The disadvantages are that the project is dependent on funds not yet appropriated, DHS approval of the successive phases, and local level ability to commit to future projects that have no funds obligated to them.

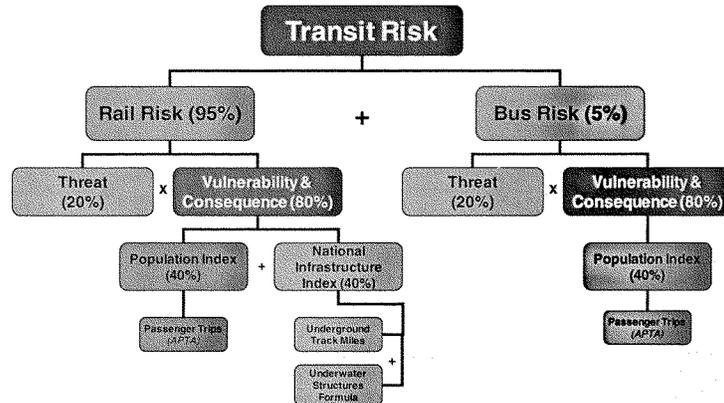
Question: Mr. Ashley, please describe the risk methodology used to award transit and rail grants.

ANSWER: The risk formula used in the TSGP grant program was developed in conjunction with the Transportation Security Administration (TSA), and all vulnerability and consequence (V&C) data was provided by TSA. The TSGP formula accounts for risks to both intracity (metro and commuter rail) rail systems and to bus systems. Since these systems have qualitatively different characteristics, the risks to these two types of systems are calculated separately and added together to arrive at the overall risk score for the TSGP. Since the rail and bus risk scores are calculated on different scales, they must be normalized and weighted before summed. In the overall transit risk score, rail risk is weighted at 95%, with bus risk at 5%.

Within the rail and bus risk formulas, the components break down similarly to other programs. There are separate threat terms for bus and rail, whose data comes from the DHS Intelligence & Analysis Directorate (I&A) as for the other risk formulas, and which are weighted at 20% compared with the V&C terms.

The Index components of V&C have weights that reflect the mission and likely consequences of an attack on an urban transportation system. Since the mission is primarily to transport people, the Population Index contributes significantly to both the rail and bus risks. Neither the rail nor the bus formulas include an Economic Index component. The direct economic consequences of a typical transit system attack are minimal (replacement costs, etc.), and the potentially sizable indirect costs are difficult to predict with certainty. Since the economic impact is dependent on the ridership of the system, economic consequences are indirectly captured through the Population Index term. Similarly, the TSGP formula does not include a NSI term, since transit systems typically have only minor impacts on national missions. Only the rail portion of the risk formula includes a NII term, as typical bus system infrastructure is not nearly as important as the people traveling on the buses.

In summary, rail risk is driven by people and infrastructure, and bus risk is driven entirely by people. The following graphic illustrates the TSGP transit risk formula.



Question: According to Mr. Eckles during the hearing, the Federal Transit Authorities' (FTA) grants process is often less burdensome than DHS' grants process. Mr. Ashley, has TSA or FEMA ever considered operating the Transit Security Grants more like FTA grants to simplify the process?

ANSWER: The FTA has a number of different grants for transit systems, including both competitive and formula grants. FEMA has not looked into operating the TSGP in a similar manner, but does work with FTA on a regular basis and could explore the viability of adopting some of their methods. However, DHS does not currently have block grants, so we may only be able to adapt certain portions of their programs if they fit into our general construct.

Working with the Department of Transportation

Question: The title of this hearing is "Securing the Nation's Rail and Transit Systems". That has never been more important given the infrastructure investments that will take place in this country over the next few years as a result of the American Recovery and Reinvestment Act-- \$8.4 billion was provided for Transit grants and \$1.4 billion for Amtrak. GAO said it best "The nation's economic vitality and the quality of life of its citizens depend significantly on the availability, dependability, and security of its surface transportation network." Given the relatively small amount of funds DHS has for Transit Security grants, \$400 million in FY 2009 and \$150 million in the American Recovery and Reinvestment Act, what is FEMA doing to leverage these security resources to ensure our nation's growing infrastructure remains safe?

ANSWER: Along with its partners at TSA, FEMA works to clearly outline priorities for each year's funding that reflect the identified threats to our transit systems. For example, the Department continues to be concerned about the use of IEDs against our transit systems, especially in vulnerable areas such as underwater tunnels. When developing grant guidance each year, we look across all of the programs in our portfolio to see where we can leverage existing strengths and make sure that we maximize our investments across the nation, regardless of the funding source. As we put together the grant guidance for the \$150 million dollars in the ARRA, we are planning to build upon the funding priorities in the FY 2009 TSGP package, in addition to comments gathered from our stakeholders.

Secretarial Action Directives

Question: During Secretary Napolitano's confirmation hearing, she announced that she would focus on surface transportation security because "we have done an awful lot in the aviation world." Secretary Napolitano followed this up with a Secretarial directive tasking TSA to review current strategies, plans and programs for security of the air, surface, and maritime transportation sectors. The report was also to include a side by side comparison of the threat environment, resources and personnel devoted to each transportation sector. An oral report was due to her by the end of January. Did FEMA also have input into this review? If so, what advice did you offer Secretary Napolitano that might be used to improve the grant process for surface transportation security programs? Will we see changes to the grant process for either the economic recovery funds or the 2010 appropriation to reflect these recommendations?

ANSWER: FEMA is not aware of any request for input on this Secretarial directive. FEMA and its partners in the execution of the grant programs (such as TSA and USCG) are always looking for feedback on ways to improve the grant programs. Any information made available through any source will be considered.

QUESTIONS FOR THE RECORD SUBMITTED BY

THE HONORABLE HAROLD ROGERS

**John Sammon, Assistant Administrator of Transportation Sector
Network Management, Transportation Security Administration
Securing the Nation's Rail and Transit Systems**

TSA Security Assessment of Largest Mass Transit and Rail Agencies

Question: TSA recently concluded an assessment of the adequacy of security measures and emergency management processes within 48 of the 50 largest mass transit and passenger rail agencies. The assessment determined that 77% of the systems surveyed did not demonstrate satisfactory security mechanisms. How does TSA intend to work with the agencies that did not perform well to improve their security measures and processes?

ANSWER: The Transportation Security Administration (TSA) is committed to working with transit agencies to continuously improve their security measures and processes. Senior level TSA Mass Transit representatives meet with transit system representatives on a regular basis through Regional Transit System Working Group meetings, and Surface Transportation Security Inspectors engage transit system operators and workers during assessments and follow-on assessments. The areas of concern identified by TSA became funding priorities under the Transit Security Grant Program. Specifically, for fiscal year 2008, priorities included training, operational deterrence, drills, and public awareness activities. In coordination with the Federal Transit Administration (FTA), TSA also hosts Roundtable conferences focused on security and safety every six months for the top 50 transit systems. Connecting Communities is another program jointly sponsored by FTA and TSA that brings transit agencies together with local emergency first responders in a workshop setting to learn about one another's capabilities.

Anticipated Number of Additional VIPR Teams

Question: TSA has indicated that it intends to request additional VIPR teams in 2010. Does TSA intend to continue increasing the number of VIPR teams each fiscal year or will the requested amount round out the overall need for this capability?

ANSWER: The fiscal year 2010 President's request of \$50 million for an increase to Visible Intermodal Prevention and Response teams specific to the Surface mode of transportation will enable the Transportation Security Administration (TSA) to significantly strengthen security in the non-aviation transportation sectors. TSA will continue to use a risk-based approach that incorporates intelligence, critical analysis, and state and local partner input to assess future needs.

Recent DHS IG Report on Surface Inspectors

Question: A recent DHS IG report evaluated the effectiveness of TSA's deployment and training of surface transportation inspectors. The IG noted that the program appears understaffed for the long term and indicates that the aviation-focused command structure within TSA has reduced the quality and morale of the workforce. Address how TSA intends to improve the skill levels of these inspectors and demonstrate that they are valued within the TSA workforce.

ANSWER: The Transportation Security Administration (TSA) will continue to invest in a wide variety of training to enhance the operational capabilities of this critical segment of the TSA workforce. The Surface Transportation Security Inspection Program (STSIP) National Training Program consists of six weeks of initial training that includes two weeks of TSA-specific training, one week each of Transportation of Hazardous Materials, Transit System Security and Transit Rail Incident Investigation training provided by the Department of Transportation's Transportation Safety Institute and a one week Railroad Operations, Safety and Security training at the Emergency Response Training Center. Additionally, to achieve advanced skill levels and interaction with other Department of Homeland Security components, the STSIP regularly sends surface inspectors to a myriad of courses conducted at the Federal Law Enforcement Training Center (FLETC) and New Mexico Tech's Energetic Materials Research and Testing Center (EMTRC). FLETC courses include: Physical Security Training Program, Fundamentals of Terrorism Training Program, National Investigative Interview Training Program, Critical Infrastructure/Key Resources Protection Training Program, Introduction to Criminal Investigations Training Program and Operations Security for Public Safety Agencies Counterterrorism Training Program. EMTRC courses include: Incident Response to Terrorist Bombing Incidents and Preventing and Responding to Suicide Bombing Incidents. Finally, Surface Transportation Security Inspectors also complete several Federal Emergency Management Agency on-line courses that include training on the Incident Command System and the National Incident Management System.

Surface Inspectors Role in Larger Surface Security Strategy

Question: TSA claims that the surface inspectors are a key component of the security strategy for the surface sector. Yet, it remains unclear how the deployment of these inspectors fits into this larger strategy. If their deployment is intended to address security vulnerabilities, the basis of decisions to deploy these assets should be directly linked to identified risks within specific rail or transit systems - rather than fulfilling a predetermined deployment schedule. Address how surface inspector deployments fit into the security strategy for the surface sector and whether the deployment decisions for these assets are linked to identified risks within specific rail or transit systems.

ANSWER: Surface Transportation Security Inspectors are assigned across the Nation in a risk-based deployment strategy based on a number of factors such as:

- High Threat Urban Area ranking;
- Transit system ranking based on ridership;
- Ranking in tons of Toxic Inhalation Hazard shipments relative to population density; and
- Increasing the Surface Transportation Security Inspection Program presence on the Northeast Corridor due to concentration of rail traffic.

These and other factors such as inspector safety are considered before inspectors are assigned to field offices. Consequently, the deployment of Surface Transportation Security Inspectors is consistent with the strategic

priorities of the Transportation Security Administration and the Department of Homeland Security to reduce risk and ensure freedom of movement for people and commerce.

Surface Transportation Security Inspectors are deployed under a risk-based approach that takes a regional view considering the threat and attendant consequences of terrorist attacks to surface transportation systems nationwide. Surface Transportation Security Inspector duty stations are assigned based on criteria such as High Threat Urban Area designation and ranking, total number of mass transit passenger trips, total tonnage of Toxic Inhalation Hazard materials transported by rail, and other criteria such as safety considerations. Specific vulnerabilities in transportation systems are identified in particular transit or transportation systems through surface inspector assessments.

TSA Pilot Program Within NYC Subway System

Question: Does TSA intend to report on the progress of the pilot program soon to be implemented within the New York City subway system?

ANSWER: Planning and preparations for implementation of this joint initiative are ongoing through a joint working group consisting of New York Police Department (NYPD), New York Metropolitan Transportation Authority (NY MTA), and Transportation Security Administration (TSA) officials. TSA will provide updates as progress continues on the initiative to augment capabilities of the NYPD Transit Bureau and NY MTA in conducting random inspections of passengers' bags throughout the New York City subway system.

QUESTIONS FOR THE RECORD SUBMITTED BY

THE HONORABLE NITA M. LOWEY

**W. Ross Ashley, Assistant Administrator of Grant Programs,
Federal Emergency Management Agency
Securing the Nation's Rail and Transit Systems**

Grant Program Expenditures

Question: Prior to FY09, New York State used the 3% management funding it received as the State Administrative Agency (SAA) from the Transit Security Grant Program to support the New York National Guard's Empire Shield initiative. Empire Shield is an excellent program that provides surge capacity to protect critical infrastructure, particularly the metropolitan area's transit system, during periods of heightened alert. However, in FY09 the state was removed as the administrator of the transit grant program. Would you support making the New York National Guard an eligible subgrantee for the FY10 Transit Security Grant Program?

ANSWER: FEMA awards grants directly to the transit systems under the Transit Security Grant Program. The decision for making sub-grants rests with the transit system, as they have the best understanding of their own priorities and resourcing decisions. In other grants that FEMA administers, National Guard entities have served as subgrantees, and provided valuable capabilities to States and local jurisdictions. However, FEMA will defer to the transit system on final subgrantee decisions.

Transit Grants Allocation Methodology

Question: When FEMA creates a risk formula for urban areas to distribute the TSGP, the formula values threat at 20% and vulnerability and consequence at 80%. I have been told that the value of threat is so low because there is not always adequate information to increase its relative weight. However, the history of recent terrorist attacks would seem to overlap with what we perceive as the likeliest targets, such as attacks in London, Madrid, and Mumbai and last fall's threat against transit in New York. Why is the actual threat of an attack worth only one-fifth of the risk formula?

ANSWER: The threat term is treated the same way across all grant programs. Threat is weighted at 20%, compared with vulnerability and consequence (V&C) at 80%, in all risk formulas. Threat scores are derived from intelligence data compiled by the DHS Intelligence & Analysis Directorate (I&A). For each grant program, a list of relevant entities (e.g., for the UASI program, the 100 largest Metropolitan Statistical Areas in the U.S.) is sent to I&A for review and prioritization. All entities in a given level receive that same score for threat in the risk formula. This score represents the average likelihood of attack on an entity in that level, allowing for uncertainty both in the likelihood of attack and also in the level assignments. The risk formula used in the TSGP grant program was developed in conjunction with the U.S. Transportation Security Administration (TSA), and all V&C data was provided by TSA. The decision to use 20%, or one-fifth, is a policy decision by the Department of Homeland Security, and reflects the Secretary's belief in how the variables should be weighted. All formulas are reviewed each year for potential changes, including the weight of the threat variable.

QUESTIONS FOR THE RECORD SUBMITTED BY

THE HONORABLE NITA M. LOWEY

**John Sammon, Assistant Administrator of Transportation Sector
Network Management, Transportation Security Administration
Securing the Nation's Rail and Transit Systems**

Grant Program Expenditures

Question: Prior to FY09, New York State used the 3% management funding it received as the State Administrative Agency (SAA) from the Transit Security Grant Program to support the New York National Guard's Empire Shield initiative. Empire Shield is an excellent program that provides surge capacity to protect critical infrastructure, particularly the metropolitan area's transit system, during periods of heightened alert. However, in FY09 the state was removed as the administrator of the transit grant program. Would you support making the New York National Guard an eligible subgrantee for the FY10 Transit Security Grant Program?

ANSWER: In fiscal year (FY) 2009, consistent with the direction of the relevant provision of the Department of Homeland Security's appropriations legislation, Transit Security Grant Program funds are to be awarded directly to the eligible transit agencies and designated primary security providers. In FY 2010, Transportation Security Administration will execute the program as directed in the FY 2010 appropriation.

Amtrak Security

Question: It is my understanding that unlike our airline industry, Amtrak remains unable to access the no-fly list or other watch-lists to cross-check them with their passenger manifests, despite Al-Qaeda's proven track record of targeting rail systems. Can you explain why Amtrak is not given access to the same security measures as the airlines? Further, do you support granting Amtrak access to no-fly lists or other watch-lists?

ANSWER: Although there have been discussions by Transportation Security Administration officials in the past with Amtrak counterparts on means to facilitate vetting of passengers, there have been no specific proposals to provide Amtrak with access to the "no fly" list.

Before Amtrak could benefit from using watch lists, some practical hurdles would need to be overcome. Vetting passengers against government watch lists involves obtaining personal information from them in advance of travel and conducting the matching. It is important to note that much Amtrak travel does not involve advance reservations. Many tickets are purchased at kiosks or counters in stations. Some form of immediate electronic check against the "no fly" or watch list would be necessary to cover this category of travelers. Additionally, Amtrak passengers can purchase a ticket on board the train, a common practice particularly at stations in remote areas or with overnight train service.

QUESTIONS FOR THE RECORD SUBMITTED BY

THE HONORABLE LUCILLE ROYBAL-ALLARD

**John Sammon, Assistant Administrator of Transportation Sector
Network Management, Transportation Security Administration
Securing the Nation's Rail and Transit Systems**

Mismanagement of the Transit Security Grant Program

Question: Mr. Eckles' testimony described a whole litany of challenges that the Los Angeles County Metropolitan Transit Authority was forced to overcome in order to obtain funding through the Transit Security Grant Program.

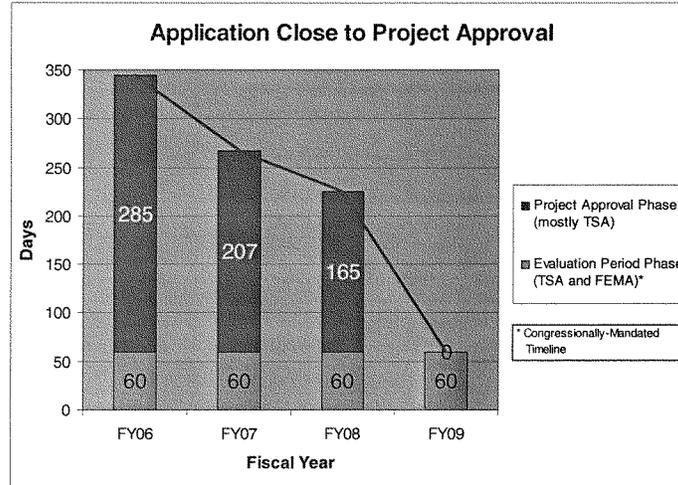
In light of the difficulties that Mr. Eckles and others have experienced, what steps are TSA and FEMA considering to improve the administration of transit security grants?

ANSWER: Mr. Eckles' concerns are related to the length of time it takes to receive programmatic approval for grant applications.

The Transportation Security Administration (TSA) has proactively made process improvements to reduce the time necessary to complete its responsibilities under the Transit Security Grant Program (TSGP) since becoming the programmatic lead in fiscal year (FY) 2006. Specifically, TSA has reduced the time necessary to complete the review and approval of Tier I applications by approximately 17 months since FY 2006.

TSA's reduction in process time is the result of significantly more outreach to our security partners; shorter deadlines for TSA, the Federal Emergency Management Agency (FEMA) and security partners alike; and other efficiencies gained as the Department of Homeland Security (DHS) and our security partners learned the process. These key factors are as follows:

1. For the first time in FY 2009, TSA and FEMA travelled to each Regional Transit Security Working Group (RTSWG) before the guidance was released to discuss with the agencies the aggressive timelines that would be pursued. This initial outreach was critical in meeting deadlines later in the process.
2. The number and frequency of RTSWG meetings has increased progressively over the course of the grant cycles since FY 2006. By FY 2009, each RTSWG met several times during the application period phase, allowing for more security and grant funding discussions upfront, and resulting in higher quality projects in a more timely fashion.
3. Eligible TSGP Tier I grant applicants were subject to more stringent deadlines for FY 2009. Draft and final Investment Justifications and Detailed Budgets were due much earlier in the FY 2009 process, and nearly mirrored the timelines of the competitive Tier II TSGP process.



Notes:

- FY 2007 Project Approval Phase consists of both base and supplemental funding resulting in longer average approval times.
- FY 2008 Project Approval Phase partially impacted by FY 2009 Appropriation Language eliminating FY 2008 match which resulted in most grantees resubmitting their investment justifications.
- FY 2009 Project Approval Phase completed prior to the end of the Evaluation Period Phase resulting in zero impact on the award schedule.

The above chart shows the number of days from grant application receipt to Tier I project approval. TSA has significantly revised the process to review and approve Tier I projects, resulting in decreases in approval times each fiscal year. After applications are received, DHS has 60 days to act on the awards, per congressionally mandated timelines. After the 60-day period, DHS announces the awards. In FY 2006, it took approximately 285 days after awards were announced to Tier I project approvals. That timeline has been reduced to 0 days for FY 2009, meaning that all Tier I projects will be approved when the awards are announced.

While significant advances have been made, there are additional areas of the TSGP that can be improved:

1. Currently additional subject matter experts assist in the security review of grant applications. This additional staff will decrease the amount of time it takes to approve the security aspects of a grant application.
2. TSA is also developing a formal Memorandum of Understanding (MOU) clarifying the roles and responsibilities of FEMA and TSA. This will prevent duplication of efforts while ensuring that the grant review and management process moves in an efficient, coordinated manner. This MOU will also be

shared with transit agencies to clearly communicate the roles and responsibilities of the TSGP with the grant community.

3. TSA will reduce the number of rounds of transit agency revisions to investment justifications required before project approval through stricter resubmission deadlines and more formalized feedback.
4. DHS will continue to adhere to aggressive timelines for project application, deadlines, reviews, and approval and communicate those deadlines early and often.

Allocation of TSA Resources to Safeguard Mass Transit

Question: Despite the fact that everyday in the United States five times more passengers travel by rail than by plane, TSA continues to allocate only a fraction of its resources to securing subways and other mass transit systems. Yet, as the London bombings tragically illustrated, these networks are extremely vulnerable to terror attacks.

Given the serious threats that mass transit faces, what accounts for this seeming imbalance in funding?

ANSWER: In accordance with Congressional appropriations, most of the Transportation Security Administration's (TSA's) funds have been directed to the security of the aviation sector. To address maritime and surface transportation, TSA and other Department of Homeland Security agencies have worked with service providers and regulatory agencies to set security standards and monitor compliance. Through the Federal Surface Transportation Security grant programs, from fiscal years (FY) 2005 – 2009, approximately \$1.4 billion has been distributed to various transit agencies for funding security improvements that implement strategies based on active deterrence.

Training for Transit, Rail and Bus Workers

Question: The 9/11 Implementation Act included very specific training mandates for transit, rail and bus workers. For example, DHS was required to develop and issue regulations governing a training program for rail workers. Unfortunately, the previous administration made limited progress in implementing these mandates.

What actions are you taking to ensure that transit, rail and bus workers receive the training they need to identify and respond appropriately to terrorist threats?

ANSWER: The Transportation Security Administration (TSA) developed and implemented a focused Security Training Initiative under the Transit Security Grant Program (TSGP) in February 2007. This initiative, developed through the Mass Transit Sector Coordinating Council formed under the National Infrastructure Protection Plan and the Transit Policing and Security Peer Advisory Group, provides guidelines to mass transit and passenger rail agencies on the types of training to be provided by category of employee. The guidance further identifies specific courses developed by the Federal Transit Administration, the Federal Emergency Management Agency, and TSA that are available. In addition, the Department of Homeland Security revised the eligible costs under the TSGP to allow coverage of overtime expenses incurred when employees receive training courses. Finally, security assessments conducted under the Baseline Assessment for Security Enhancement program confirm that security plans, which include provisions for training employees, have been developed and are being implemented.

Training for Transit, Rail and Bus Workers

Question: The formula that TSA employs to score proposals for transit security grants does not prioritize train control systems, despite the crucial role they play in ensuring the safety of rail travel. Will TSA consider reprioritizing train control as it develops its fiscal year 2010 grant guidance?

ANSWER: Although positive train control systems may provide safety and prevent high-speed accidents, it lacks critical features to protect passenger trains from access and use by unauthorized individuals and the ability to remotely disable a passenger train during an unfolding terrorist event. The Transportation Security Administration is collaborating with the Long Island Railroad to develop a suite of layered security enhancements for access control and remote disabling of commuter rail locomotives. This project is in the initial stage of engineering evaluation and solution design. The goals of the project are to provide solutions to enable authentication of authorized users of locomotives, protect idling locomotives from use by unauthorized individuals, and remotely disabling locomotives in a safe and predictable manner quickly to prevent a terrorist from conducting an attack leading to catastrophic failure of critical infrastructure and significant loss of life. Upon completion of this project, the successful solution will be considered for addition to the Authorized Equipment List for the Transit Security Grant Program.

QUESTIONS FOR THE RECORD SUBMITTED BY

THE HONORABLE KEN CALVERT

**John Sammon, Assistant Administrator of Transportation Sector
Network Management, Transportation Security Administration
Securing the Nation's Rail and Transit Systems**

Rail Car Tracking

Question: As you may know, Riverside, California has some of the highest goods movement traffic in the nation. Goods coming into and out of the Ports of Long Beach and Los Angeles come through Riverside County.

Specifically addressing Rail Security Strategy, what is TSA's plan to reduce the risk in high urban areas, and can you explain how rail car tracking and readers assist in securing the highest risk shipments and enable appropriate security response as shipments move through urban areas and highly populated rail corridors which extend from our ports and port cities?

Does the current rail car tracking system and readers have the capability of allowing first responders to monitor hazardous shipments in railroad containers as they move through their area of responsibility?

ANSWER: The Transportation Security Administration's (TSA's) strategy for reducing the risk within High Threat Urban Areas (HTUA), and minimizing the consequences from an attack, consists of both collaborative and mandatory measures. Collaborative initiatives in which the industry is an equal partner in determining implementation steps helps TSA react quickly and effectively to emerging threats. These collaborative initiatives include 24 Security Action Items (SAIs) that were issued on June 23, 2006, and which were augmented by three Supplemental Security Action Items (SSAIs) on November 21, 2006. The collaborative measures involved working with industry to reduce risk through supply chain efficiencies that result in rail cars containing rail security-sensitive materials spending less time in HTUAs, as well as an increased employee focus on shipments of rail security-sensitive materials. TSA assesses industry implementation of the SAIs and SSAIs, and conveys its findings to the industry. Mandatory measures are also necessary to ensure consistency in implementation, and serve as the foundation of layered security. The mandatory measures, as set forth in 49 CFR Part 1580, mandate the designation of industry Rail Security Coordinators; require enhanced location and shipping information capability; and require adherence to chain of custody protocols for rail cars containing rail security-sensitive materials, including those in HTUAs or destined to enter an HTUA. In addition, under 49 CFR 1580.105, regulated parties must report significant security concerns to the Department of Homeland Security.

The use of rail car tracking and automated equipment identification readers provide the operating railroad location reporting for all in-transit shipments, including shipments of Rail Security Sensitive Materials (RSSM). This reporting enables the operating railroad to convey timely information to emergency services, which enhances the ability to both respond quickly and to mitigate consequences from a potential terrorist attack. The reported information is archived by the Association of American Railroads (AAR). The Transportation Security Administration (TSA) receives from the AAR the tracking data generated by all RSSM shipments in the continental United States. The RSSM data is sorted by location and by railroad carrier, and is analyzed by

TSA to ascertain traffic patterns and volumes. The analysis enables TSA to determine the locations where RSSM volume is greatest and assign inspection resources accordingly. Additionally, the analyses are provided to the railroad carriers to apprise them of TSA's finding and to encourage enhanced domain awareness at those locations.

The current rail car tracking system and readers do not have the capability of allowing first responders to monitor hazardous shipments as they move through their respective areas. However, the system and readers provide car location data which the railroad operations centers monitor very closely. During emergency situations, railroad operations centers quickly relay important information to the first responders as to location and commodities involved in a particular incident.

QUESTIONS FOR THE RECORD SUBMITTED BY

THE HONORABLE KEN CALVERT

**Jack Eckles, Deputy Executive Officer for System Safety and
Security, Los Angeles County
Metropolitan Transportation Authority
Securing the Nation's Rail and Transit Systems**

Closed Circuit Television

Question: Rail Operators have embarked on programs designed to upgrade existing security technology closed circuit television (CCTV) to monitor their stations, yards, or trains. While these cameras cannot be monitored closely at all times, I understand that the technology has assisted security personnel in determining how to respond to incidents that had already occurred, and could be monitored if an operator had received information that an incident may occur at a certain time or place in their system.

Can you please describe plans for closed circuit television monitoring of high risk railroad right of ways within Southern California besides those that are already in place?

ANSWER: Currently, the Los Angeles Regional Transit Security Working Group (RTSWG) only has one rail member (Metrolink) who has attempted to obtain grant funding to monitor their right of ways (ROW). In their efforts, they were only able to secure grant funding for tunnel intrusion detection systems. As I understand the proposed system, it includes CCTV cameras connected to an infra-red scanner with the monitors located at Metrolink's control center. These devices are placed at the entrance to the various tunnels utilized by Metrolink. When someone or something, the size of a person or larger, enters the tunnels, the infra-red beam is broken and a monitor and alarm activates at the control center for an operator to dispatch law enforcement to investigate.

Currently, there are no plans by the Los Angeles County Metropolitan Transportation Authority to develop ROW intrusion detection. Our highest risk rail line is the Redline system and all entrances have intrusion detection systems installed. All exist and ventilation shafts have intrusion detection systems connected to them already.

Grant Guidance

Question: As we have heard, the federal grant process which provides funding to your organizations is constantly evolving.

Can you explain how an annual grant guidance issued in advance of each Fiscal Year, would be helpful to your organizations in long-range planning and please also expand on suggestions in your written testimony of other changes that would be helpful in the year-to-year grant process

ANSWER: Issuance of grant guidance in advance of a Fiscal Year would not assist in our organization's long-range planning because of the current trend by TSA in emphasizing law enforcement operations and annual

changes therein. These dictates are currently developed **without consultation with the transit agencies**, but rather with their law enforcement departments or contracted law enforcement agencies and in a few instances where the transit agency has no law enforcement the local policing agency. Therefore, there is no long-range plan for **the agencies** to develop necessary infrastructure projects that carry-over from grant year to grant year. It is simply doing it there way or not at all. Additionally, these mandates change from year-to-year with TSA. One year it's training, the next it's training and public awareness and then those same projects with O-Packs (operational packages) by law enforcement. Any hardening or infrastructure projects for **the agencies** are deliberately given low scores and are disqualified or are specifically banned from project submittal.

In suggestions for the grant process from year to year, I strongly recommend that TSA utilize its twice-a-year Safety & Security Roundtable, which gathers the safety and security representatives of the top 50 transit agencies. Have TSA provide a classified risk briefing on the state of threats to transit agencies or even a sanitized unclassified briefing. This should be followed, within the same roundtable by conferencing or coordinating on what the transit agencies needs are in specifically addressing their DHS/TSA (paid for) Threat and Vulnerability assessments. These assessments can be used to literally check-off progress agencies have made in addressing their risks and vulnerabilities. This will enable TSA to quantifiably show congress its efforts in securing mass transit agencies and simplify the grant development and approval process.

TSA could use the December Roundtable event to provide the briefing and situational updates, obtain recommendations from the agencies on objectives and let the Agencies decide on their projects they would develop to best meet those objectives (the objectives would be based upon that agency's Threat and Vulnerability Assessment-an objective standard). During the June Roundtable event, TSA would present the proposed grant guidance for that grant cycle. TSA would solicit recommendations or concurrence on the recommended guidance to be published.

In this way, the agencies can address their own agency's needs from their Threat and Vulnerability Assessment, which would allow them to plan, in advance what these project will be. At the same time it would provide TSA with a quantifiable system for objectively showing what progress has been made on securing that system. Any adjustment from changing threats can be made far enough in advance for agencies to shift, if needed, their projects to address the new threats without deviating from the overall goal of addressing their overall risk.

I would use the Threat and Vulnerability Assessment's (TVA) categories (i.e. Increase Countermeasures, Improve Response, and Improve Recovery) in determining what projects an agency can develop and implement in order to reduce that Agency's identified vulnerabilities. Currently, the guidance specifies what specific classes of projects agencies must and are given a numerical valued rating, but these projects and values usually have no relationship to our assessed vulnerabilities and in some cases, when it does, the numerical value of that particular project is too low to become an approved project. Therefore, rather than dictate whether you can or can't use a system specifically like cameras, communications equipment, or command centers; the Threat and Vulnerability Assessment would allow an agency to develop how it can best reduce a vulnerability in...say, a security countermeasure (prevention/deterrence); let an agency best decide how it can develop a project to solve the vulnerability in that category. In this way, TSA has an objective standard to which it can evaluate whether or not an agency's project(s) address that agency's identified vulnerability.

This process would simplify TSA's grant guidance development (the categories wouldn't change), improve the approval process and shorten the approval time (the project only needs to be matched against that agency's list of threats and compared to see if the project reduces the risk of that threat).

Thank you for the opportunity to address these vital concerns.

QUESTIONS FOR THE RECORD SUBMITTED BY

THE HONORABLE KEN CALVERT

**Mr. Bill Morange, Deputy Executive Director and Director of
Security, New York Metropolitan Transportation Authority
Securing the Nation's Rail and Transit Systems**

Grant Guidance

Question: As we have heard, the federal grant process which provides funding to your organizations is constantly evolving.

Can you explain how an annual grant guidance issued in advance of each Fiscal Year, would be helpful to your organizations in long-range planning and please also expand on suggestions in your written testimony of other changes that would be helpful in the year-to-year grant process

ANSWER:

Issuing the annual grant guidance in advance of the federal fiscal year would enable grantees to begin the grant process sooner and to complete the selection of ODP funded candidates prior to the federal fiscal year. Projects would then be ready to begin immediately with the authorization of the federal dollars at the beginning of the federal fiscal year (October 1st). This would accelerate the review and approval process by TSA/FEMA and enable the transit agencies to advance their projects in a more timely manner. In turn, these projects would begin to draw down their federal funds quickly and accomplish the goals of the federal security program.

In order to accomplish this, the MTA also believes that grant guidance must remain consistent from year-to-year so that agencies can submit candidate projects in advance of the federal fiscal year. Changes to grant guidance would be required to be made one year in advance.

The MTA believes that the following recommendations would also improve the overall grant process:

1. We believe the Regional Transit Security Program should broaden its emphasis areas and have identified several areas where we think federal funds are necessary:
 - Consequence Management projects to enhance; egress, lighting and signage
 - Interoperable Communications for our police and regional partners
 - Back-up power redundancy
 - Chemical/biological and radiological detection devices
2. We need flexibility to use federal funds for design, project management and construction management tasks conducted by in-house forces. Currently, these tasks are fully reimbursable only if they are done by a third party contractor. Many transit agencies have in-house departments to do design work and project and construction management. Efficiencies are gained by utilizing these departments, whose personnel possess expertise in the individual transit system that most contractors do not have. The federally-mandated annual

A133 Single Audit ensures that transit agencies have appropriate controls are in place to charge time correctly to grant-funded projects.

3. We need flexibility to fund all in-house flagging and track access work, which is currently fully reimbursable only when conducted by a third party. Individual agencies are best suited to determine needs for flagging, track access, etc., and in some cases, costs are driven by the Federal Railway Administration – Roadway Worker Protection Act, CFR Section #214.
4. We support the creation of a “One-Stop Shopping” mechanism for better coordination between FEMA and TSA. The current process requires one agency to approve the funds and the other to approve the scopes for the projects. This causes delays in approving the grant package every year. In fact, we are still awaiting approval for funding under the FY 2008 TSGP funding measure.
5. We would like to emphasize the critical role that the state has in the grant process and encourage a more active role for the State SAA in developing a regional security strategy. We would like to propose the State SAA be formally part of the TSGP and chair Regional Transit Security meetings. They should be involved in the process and to receive TSGP funding.
6. The funding sources under the TSGP process are designed to support the security needs of the Transit Agency and their primary law enforcement provider. Allocations that are directed to local municipal law enforcement agencies have the potential for a negative impact on the core objectives of the grant program.

We will expect 30 day periodic updates with the staff, and then we expect a 120 day full accounting with the Subcommittee. With that, we thank you for your work and for your testimony here today, and we turn to our second panel. During the second portion of the hearing we will hear from Ms. Gale Rossides, the acting Administrator of the Transportation Security Administration.

TUESDAY, MARCH 31, 2009.

**IMPROVING THE EFFICIENCY OF THE AVIATION
SECURITY SYSTEM**

WITNESS

GALE ROSSIDES, ACTING ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION

OPENING STATEMENT OF CHAIRMAN PRICE

Mr. PRICE. We will be focusing on TSA's efforts to improve the efficiency of the aviation security system. Now, we members have a lot of experience with this. It is one of those things that everybody has an opinion about. We fly at least twice a week, 40 weeks a year. Time and time again we encounter the aviation security system, and we also hear a lot from our constituents.

We wonder, they wonder, when we will be able to bring liquids above three ounces in our carry on bags or when we will be able to stop dragging our bags over to the explosive detection system in the middle of the airport's lobby. So we all have some experience with this but we clearly will welcome the chance this morning for a more systematic review.

Our Subcommittee's task over the years has been to help TSA find ways to more expeditiously move airline travelers, their luggage and air cargo, while at the same time strengthening security. Since 2002, Congress has appropriated over \$44 billion for aviation security activities, including \$1 billion in the recently enacted economic recovery package.

This recent appropriation should accelerate the installation of in-line explosive detection systems at airports nationwide and the development of technologies that would allow passengers to bring liquids of any size aboard on aircraft. The results have been slow in coming, and today we want to talk about what progress TSA has made in improving overall efficiency and what kind of progress we can anticipate in the future.

Our concerns have also been voiced repeatedly about the pending general aviation rule on large aircraft security. That is another thing we hear plenty about. While it is critical to ensure the security of air travel, whether in the commercial aviation sector or with general aviation, security regulations should not pose an unwieldy financial or logistical burden on the general aviation community.

Any new security requirement the government imposes on the public must strike a balance between tighter security and the need to ensure minimal disruption of the movement of goods and people in our economy. I know TSA is, as we speak, in the process of weighing these costs and benefits and continues to work with the affected stakeholders. I, and many others, have urged that course

on the agency. Today we want to discuss the status of this pending rule and what alternatives TSA is continuing.

Finally, with the adoption of the 9/11 Act, TSA was given several mandates, including tighter air cargo screening procedures. The Act specified that by February of 2009, 50 percent of all air cargo being carried on passenger aircraft must be screened and 100 percent of this cargo must be screened by August 2010.

While TSA has informed the Subcommittee that it has met the 50 percent mandate, GAO recently has questioned this assertion. On March 18, 2009, GAO testified that TSA cannot verify this level of cargo screening and that TSA is still working to establish a system to ensure 50 percent screening which might be ready by next month. Now, this in theory was the easier mandate to meet. Reaching 100 percent will be a much greater challenge.

Today we want to discuss how you can assure the Subcommittee that you are meeting the 50 percent deadline, what is working well so far and what challenges you face, and how you are going to stretch to meet this 100 percent requirement. I have publicly stated this is an important mandate. I believe that it is. I believe it is one TSA can meet, although I do recognize that it is easier said than done, perhaps, with respect to the timeframe we have set.

So welcome, Ms. Rossides. I look forward to your testimony this morning. I want to ask you, as we do all of our witnesses, to take five minutes to summarize your written statement and we will put that entire statement in the record. Before you do that, I want to recognize our distinguished Ranking Member, Mr. Rogers, for his comments.

[The information follows:]



COMMITTEE ON APPROPRIATIONS

David Price (D-NC), Chairman, Subcommittee on Homeland Security

FOR RELEASE UPON DELIVERY
Tuesday, March 31, 2009
202-225-1784

Media Contact: Phil Feagan

OPENING STATEMENT OF CHAIRMAN DAVID PRICE *Panel 2: Improving the Efficiency of the Aviation Security System* *March 31, 2009 / 10:30 am*

During this second portion of the hearing, we will hear from Ms. Gale Rossides, the Acting Administrator of the Transportation Security Administration. We'll be focusing on TSA's efforts to improve the efficiency of the aviation security system. Because most Members fly at least twice a week more than 40 weeks per year, time and time again we hear from our constituents or experience firsthand frustrations with our current aviation security system. I often wonder when we will be able to bring liquids above 3 ounces in our carry-on bags or when we will be able to stop dragging our bags over to the explosive detection system placed in the middle of the airport's lobby to be screened.

Our Subcommittee's task has been to help TSA find ways to more expeditiously move airline travelers, their luggage, and air cargo while at the same time strengthening security. Since 2002, Congress has appropriated over \$44 billion for aviation security activities, including \$1 billion in the recently enacted economic stimulus package. This recent appropriation should accelerate the installation of in-line explosive detection systems at airports nationwide and the development of technologies that would allow passengers to bring liquids of any size onboard an aircraft. But results have been slow in coming. Today we will talk about what progress TSA has made in improving overall efficiency.

Concerns have also been voiced repeatedly about the pending general aviation rule on large aircraft security. While it is critical to ensure the security of air travel, whether in the commercial aviation sector or with general aviation, security regulations should not pose an unwieldy financial or logistical burden on the general aviation community. Any new security requirement the government imposes upon the public must strike a balance between tighter security and the need to ensure minimum disruption of the movement of goods and people in our economy. I understand that TSA is in the process of weighing these costs and benefits and continues to work with affected stakeholders. Today, we will discuss the status of this pending rule and what alternatives TSA may be considering.

Finally, with the adoption of the 9/11 Act, TSA was given several mandates, including tighter air cargo screening procedures. The Act specified that, by February 2009, 50 percent of all air cargo being carried on passenger aircraft must be screened, and 100 percent must be screened by August 2010. While TSA has informed the Subcommittee that it has met the 50 percent mandate, GAO recently questioned this assertion. On March 18, 2009, GAO testified that TSA cannot verify this level of cargo screening and that TSA is still working to establish a system to ensure 50 percent screening, which might be ready by April. This, in theory, was the easier mandate to meet. Reaching 100 percent will be a much greater challenge. Today we will discuss how you can assure this Subcommittee you are meeting the 50 percent deadline, what is working well so far, what challenges you face, and how you will “stretch” to meet the 100 percent requirement. As I have publically stated, this is an important mandate; one that I believe TSA can meet, although I do recognize that this may be easier said than done within the timeframe we have set.

Welcome Ms. Rossides. I look forward to your testimony this morning. Please take five minutes to summarize your written statement. However, before we begin, let me recognize our distinguished Ranking Member Mr. Rogers for any comments he may wish to make.

###

Mr. ROGERS. Thank you, Mr. Chairman. Ms. Rossides, welcome to the Subcommittee. Despite being one of TSA's first employees, today marks your first appearance before the Subcommittee, so welcome. Thank you for appearing today. We notice you have brought along some tissue paper. I promise you we will not bring you to tears.

As I have said many times before, I am concerned TSA's approach to aviation security too often falls back upon an over reliance on costly manpower rather than efficiencies gained through technology. I acknowledge the airport environment is immensely challenging given the confluence of confined space and tight time schedules. All the more reason for investing in the latest screening technologies that can accurately and efficiently detect dangerous items while also reducing the staffing footprint.

It is no secret that this has been one of the highest priorities of this Subcommittee and the Congress since the inception of TSA. In fact, we have provided nearly \$2 billion for EDS procurement in just the last three years. Hefty sums that I hope are having the intended effects. Today, I look forward to learning more about how this sizeable investment in screening technology is allowing TSA to meet its mission requirements more effectively and more efficiently.

I also note that this major increase in funding places TSA's procurement efforts on par with the annual funding levels of other large scale DHS acquisition programs, such as SBInet and Deepwater, and yet, TSA's acquisitions continue to be based upon what appear to be year to year needs rather than a strategic multiyear approach. So I hope we can discuss that today, how TSA is managing its acquisitions to meet its goals across all of its aviation security programs.

From the inspection of carry on and checked baggage to the screening of passengers to the inspection of air cargo, TSA's efforts are certainly vital to keeping us all safe and secure. Thank you, Mr. Chairman.

[The information follows:]

OPENING STATEMENT

CONGRESSMAN
Hal Rogers



FIFTH DISTRICT • KENTUCKY

Offices in
Washington, D.C.
Somerset, Prestonsburg,
Hazard

Contact: Stefani Zimmerman

202.225.4601

**Committee on Appropriations
Subcommittee on Homeland Security**

Opening Statement (*Panel #2*):

*Securing the Nation's Rail and Transit Systems and
Improving the Efficiency of the Aviation Security System*

Witnesses:

Ms. Gale Rossides, Acting Administrator, TSA

Thank you, Mr. Chairman.

Ms. Rossides, despite being one of TSA's first employees, today marks your first appearance before the Subcommittee. So, welcome and thank you for appearing today.

As I have stated many times before, I'm concerned TSA's approach to aviation security too often falls back upon an over reliance on costly manpower rather than efficiencies gained through technology.

I acknowledge the airport environment is immensely challenging given the confluence of confined space with tight time schedules—all the more reason for investing in the latest screening technologies that can accurately and efficiently detect dangerous items while also reducing the staffing footprint.

It's no secret this has been one of the highest priorities of this Subcommittee and the Congress since the inception of TSA. In fact, we've provided nearly \$2 billion for EDS procurement in just the last three years -- hefty sums that I hope are having the intended effects.

Today, I look forward to learning more about how this sizable investment in screening technology is allowing TSA to meet its mission requirements more effectively and efficiently.

I also note that this major increase in funding places TSA's procurement efforts on par with the annual funding levels of other large-scale DHS acquisition programs such as SBInet and Deepwater. And yet, TSA's acquisitions continue to be based upon what appear to be year-to-year needs, rather than a strategic, multi-year approach.

So, I hope that we can discuss today how TSA is managing its acquisitions to meet its goals across all of its aviation security programs. From the inspection of carry-on and

checked baggage, to the screening of passengers, to the inspection of air cargo, TSA's efforts are certainly vital to keeping us all safe and secure.

Thank you, Mr. Chairman.

###

Mr. PRICE. Thank you. Ms. Rossides, please proceed.

OPENING STATEMENT OF GALE ROSSIDES

Ms. ROSSIDES. Good morning, Chairman Price, Ranking Member Rogers, and distinguished members of the Subcommittee. Thank you for the opportunity to appear today to testify on the Transportation Security Administration's efforts to improve aviation security. As we are pressed for time, I will keep this brief and request that my written testimony be included in the official hearing record.

I am appearing before you today to discuss aviation security while serving in an acting capacity which is required in order to maintain a level of security during the transition period between the administrations. In the Department of Homeland Security, continuity of our mission was assured by designating the career position of Deputy Administrator of TSA as the acting Assistant Secretary.

As such, I am honored to serve in these positions and to appear before you today. I would like to begin by thanking the members of the Subcommittee for their leadership, their oversight, and support of our evolving initiatives which are continually discussed in transportation security. By providing us with our 2009 appropriation at the beginning of this fiscal year we have been able to sustain progress on our planned enhancements through the Presidential transition.

In addition, I especially want to thank the Subcommittee for the resources that were provided to TSA in the American Recovery and Reinvestment Act. We are working to ensure the prompt expenditure of these funds, which will further accelerate the deployment of TSA's explosives detection capabilities in airports throughout the country.

The Subcommittee's efforts over these seven short years since TSA was created have enabled us to grow from a small cadre of employees to a dedicated workforce of over 50,000—protecting every domestic commercial airport, strengthening security in all transportation modes and doing so through the strong stakeholder engagement in the U.S. and around the world.

We have continually improved our people, processes, technologies, and partnerships and achieved some noteworthy milestones during this transition period. First, I am pleased to announce that on January 27, Secure Flight began operational cut over of the first air carrier and now has four carriers participating. TSA truly appreciates the cooperation of these volunteer air carriers. Our experience thus far has been a good one and has validated the program choices we made.

This initial operating capability is a major milestone in the history of our agency and is a credit to all in both branches of our government who made this security enhancement a reality. In addition to my staff, I would like to thank, specifically, the DHS Screening Coordination Office, and especially Ms. Cathy Berrick and the GAO staff for their superb work with us in this program.

Our goal for the Secure Flight Program is to assume responsibility for watch list matching of passengers for all domestic com-

mercial flights by the late spring of 2010 and all international commercial flights by the end of 2010.

Second, in February, we were to have met the mandate to screen 50 percent of cargo transported on passenger aircraft. I am pleased to inform the Subcommittee that based on the carriers' reports, a conservative analysis of the data indicates that the milestone has been met.

Third, on March 26, we issued our one millionth transportation worker identification credential, and to address the surge we expect in the final and two largest sectors that are to come into compliance, L.A./Long Beach and Houston, we have set up additional enrollment centers. Finally, I will close by thanking this Subcommittee for the support of our workforce transformation efforts over the last several years.

These accomplishments have been remarkable and can be represented by the role our Transportation Security Officers (TSOs) Inspectors and Federal Air Marshals played in the Presidential inauguration. Three hundred TSOs served in support of the United States Secret Service and provided screening expertise at checkpoints along the parade route and for the inauguration.

FAMs, TSOs, and inspectors served on VIPR teams and more than 30 TSA canine teams were deployed. TSA personnel at the Transportation Security Operations Center provided an around the clock watch in partnership with the FAA, Department of Defense, and other DHS, state and local agencies to coordinate and monitor activities through the four-day event. The FAMs provided significant coverage of all commercial flights in and out of the National Capitol Region.

It truly is my honor to serve alongside the men and women of TSA who are, in my opinion, everyday heroes. I could report even more, but in the interest of time will end my remarks. I thank you, and I am happy to answer your questions.

UNITED STATES DEPARTMENT OF HOMELAND SECURITY
TRANSPORTATION SECURITY ADMINISTRATION

Statement of

GALE D. ROSSIDES
ACTING ADMINISTRATOR

Before the

SUBCOMMITTEE ON HOMELAND SECURITY
COMMITTEE ON APPROPRIATIONS
UNITED STATES HOUSE OF REPRESENTATIVES

MARCH 31, 2009

Good morning Chairman Price, Ranking Member Rogers, and distinguished members of the Subcommittee. Thank you for the opportunity to appear today to provide an update on the Transportation Security Administration's (TSA) efforts to improve aviation security.

I would like to begin by thanking the members of the Subcommittee for their support of TSA's ongoing initiatives to improve transportation security and especially for the leadership of this Committee which provided us with our fiscal year (FY) 2009 annual appropriation on October 1, 2009. Your efforts made a difference in accelerating planned enhancements and positions us well for a successful Presidential transition. I especially want to thank the Subcommittee for the resources you provided TSA in the American Recovery and Reinvestment Act of 2009, P.L. 111-5, (ARRA), which will enhance TSA's explosives detection capabilities in airports throughout the country and will significantly accelerate the deployment of more effective and efficient detection technologies.

Building On Our Joint Success

As someone who has experienced first-hand the growth and maturation of TSA from its creation following the tragic events of September 11, 2001 (9/11) to the current high-performing global organization protecting Americans and our transportation systems, I also want to express my sincere gratitude to the Members of this Subcommittee. Your efforts over these seven short years have enabled TSA to successfully fulfill our mission. TSA has grown from a small cadre of employees to a dedicated workforce of over 50,000 protecting every domestic commercial airport, strengthening our nation's surface transportation modes, and working with our international partners around the world. We

began with the challenge of hiring, training, and placing the first Federal screeners, now known as Transportation Security Officers (TSO), in airports and tasked them with stopping the obvious prohibited items, such as guns, knives, and razor blades. Now, TSA employs a highly-trained, professional, multi-skilled TSO workforce performing physical and behavioral screening to counter constantly changing threats and operating state-of-the-art screening equipment. In 2002, TSA was known primarily for screening passengers at fixed airport security checkpoints. Today, TSA conducts security operations and inspections throughout the airport environment and in multiple modes of transportation utilizing our screening, inspection, and law enforcement resources.

Ongoing Threat

Continuing TSA's success is as important today as it has ever been. Our Nation's threat level for all commercial aviation operating in or destined for the United States remains at "High," or "Orange." Terrorists continue to pose a significant threat to the United States and focus on prominent infrastructure targets with the goal of producing mass casualties and significant economic aftershocks. The threats facing us are real and evolving. We must remain vigilant and never lose focus on our mission.

Ensuring an Effective Transition

The reason I am appearing before you today to discuss aviation security is due to a deliberate strategy by the Department of Homeland Security (DHS) to ensure TSA, as well as other DHS components, were poised to maintain our high level of security during the critical Presidential transition period. Continuity is essential for an agency that conducts security operations 24 hours a day, seven days a week, and 365 days a year. Designating the Deputy Administrator at TSA as a career position helps ensure that continuity. I am honored to serve in this position and humbled to testify before you today as the agency's Acting Administrator. Other transition efforts included TSA personnel participating in joint exercises with our DHS and other Federal colleagues to ensure we could have effectively responded to a terrorist attack during this period. We have assembled a talented team of dedicated public servants to carry on our mission and enable President Obama, Secretary Napolitano, and the new administration to assume the important responsibility of protecting our Nation's transportation security systems.

I have already had the pleasure of working with Secretary Napolitano as she immediately focused on TSA and our operations by requesting a review of security programs and strategies for the aviation, surface, and maritime modes of transportation. We are working closely with the Secretary and her office. The Secretary strongly supports TSA's mission and has already shown significant interest in TSA's important role in an overall homeland security strategy.

Implementing ARRA Funding

ARRA's additional \$1 billion for the purchase and installation of explosives detection systems and equipment will greatly enhance our ability to accelerate the deployment of

these technologies and our detection capabilities. This funding will be allocated to the Electronic Baggage Screening Program, which includes airport baggage handling system and facility modifications, and the Passenger Screening Program (PSP) to improve explosives detection capabilities in passenger screening. The plan to expend the ARRA funding is consistent with our risk-based approach to security.

As a result of the ARRA funding, TSA notified airports in eleven states, including several small and medium sized airports, that their optimal baggage screening solution projects are being considered for funding. TSA is currently in the process of project validations and agreement negotiations with these airports.

For the PSP, TSA plans to use ARRA funding for the purchase of Advanced Technology X-rays (AT X-ray), Whole Body Imagers (WBI), Universal Conveyor systems, Bottled Liquid Scanners (BLS), and Next Gen Explosives Trace Detectors. With the purchases made possible through ARRA, there will be a tremendous advancement of our prior projected schedules toward full system operating capacity of these technologies, greatly enhancing checkpoint security for the traveling public.

In addition, TSA is providing subject matter expertise and assistance to the Federal Emergency Management Agency (FEMA) for the award of the \$150 million appropriated in ARRA for public transportation and railroad security assistance grants.

Preliminary FY2010 Budget

Although the complete FY2010 Budget has not been determined, I would like to address several items that were previously announced by the President on February 26, 2009.

Visible Intermodal Protection and Response (VIPR) teams. The FY2010 Budget includes \$50 million for 15 additional VIPR teams to increase our random and surge force protection capability by deploying at transit hubs unannounced. VIPR teams are capable of protecting any mode of transportation through risk-based targeted or unpredictable deployment of integrated TSA assets in coordination with state and local officials. VIPR teams may consist of any combination of TSOs, Transportation Security Inspectors (TSI), Federal Air Marshals (FAM), Behavior Detection Officers (BDO), Explosives Security Specialists, Bomb Appraisal Officers (BAO), as well as local, state, and Federal security and law enforcement partners. This increase is a strong signal of President Obama's and Secretary Napolitano's commitment to enhance surface transportation security.

Bomb Appraisal Officers. The FY2010 Budget adds 109 BAO positions by the end of FY2010 to strengthen security at domestic airports. BAOs are highly skilled individuals who have undergone specialized training in the identification and disposal of explosive ordinance. BAOs provide continual interaction and formal training to TSOs to increase their ability to recognize potential improvised explosive devices (IED) and IED components. BAOs also assist in clearing suspicious articles presented at checkpoints, often avoiding the need to call bomb squads, which results in lengthy airport delays.

Infrastructure for Identity Vetting. The FY2010 Budget provides an additional \$64 million to modernize the information technology infrastructure used to vet the identity of travelers and covered transportation workers. The funding will allow TSA to strengthen and enhance the existing infrastructure used to conduct vetting operations on populations involving several of our most important security programs, such as the Secure Flight program, background checks for airport workers, the Transportation Worker Identification Credential (TWIC), Hazardous Materials Commercial Driver's License Endorsement, and alien flight students. The infrastructure funding will also allow TSA to vet new populations as directed by Congress in the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53, (9/11 Act).

Passenger Security Fee. To better align the costs of aviation security with the beneficiaries, the President announced we will pursue an increase to the Aviation Passenger Security Fee beginning in 2012. Since its establishment in 2001 as part of the Aviation and Transportation Security Act, P.L. 107-71 (ATSA), the Passenger Security Fee has been limited to \$2.50 per passenger enplanement with a maximum fee of \$5.00 per one-way trip. Congress anticipated that the aviation industry would pay for airline security costs through a combination of the Passenger Security Fee and an air carrier fee. However, the cost of providing security has increased substantially since 2001, leaving Federal taxpayers, rather than passengers and air carriers, to shoulder most of the expense of civil aviation security. For example, in FY2008, Passenger Security Fee collections covered only about 31 percent of the discretionary costs for civil aviation security. Appropriated funds covered 60 percent of the discretionary costs and air carriers covered the remaining 9 percent of the discretionary costs. The adjustment in 2012 will fulfill the original intent of ATSA by more closely allocating the cost of aviation security services to the individuals who directly benefit from this unique government service and simultaneously reducing the burden on the general taxpayer. The Administration and TSA will work closely with Congress to obtain the necessary authorization to begin the fee adjustments in FY2012.

Our Security Strategy

Our transportation security strategy begins with intelligence. We are an intelligence-driven operation applying a risk-based approach to security. Our daily operational decisions are influenced by the latest intelligence, whether it is adjusting the FAM coverage on flights, the location of VIPR operations, or informing the public and appropriately sharing classified information with our industry partners.

An effective security system must constantly adapt to ever-changing threats and the security environment. TSA is in the process of upgrading security effectiveness at checkpoints, which encompasses people, process, and technology. This is the most significant change in passenger screening since 9/11, and even since the checkpoint was first established in the 1970's. TSA has taken a fresh look at our checkpoint operations to see how we can improve security. We identified possible changes to the checkpoint that we are piloting after reviewing inputs from the intelligence and law enforcement communities, our employees, passengers, and evaluations of readily deployable

technology. A full pilot checkpoint is now being tested in Terminal B at Baltimore/Washington International Thurgood Marshall Airport (BWI).

Air travelers are noticing a new look at the checkpoint, but the most significant aspect is that the new checkpoint supports a team approach that is calmer and more conducive to smart security. The goal is to improve security through better training, process, and technology, providing passengers with a calmer checkpoint process. A six week pilot program using kiosks to obtain passenger feedback at BWI yielded very positive results. Passengers gave TSA high marks on all eight questions asked, ranging from passenger satisfaction with security procedures to thoroughness of screening, length of time of the screening process and quality of information available before traveling. The responses range from 79 percent to 84 percent positive.

People. The effectiveness of our security screening relies on our people—they are TSA's biggest investment and most valuable asset. We work hard to take care of our employees and we are making significant progress. Our workforce attrition rates continue to decrease. The latest FY2009 voluntary attrition rate of full-time TSOs is 7.5 percent—an improvement of more than 40 percent since FY2006. The number of workplace injuries has fallen over 75 percent from FY2004 to FY2008 and continues to fall.

Every TSO working at a checkpoint is undergoing an extensive 16-hour retraining called ENGAGE!, which brings together the latest thinking from intelligence, explosives detection, and inhuman factors that can affect security. This training is designed to develop a cadre of more analytical, rather than "checklist-oriented", security professionals. Additionally, all supervisory personnel are required to complete a second 16-hour training course called COACH! to help reinforce the ENGAGE! training and provide guidance to TSOs. We have revised our checkpoint Standard Operating Procedures to enable officers to use their judgment in achieving sensible security results. This will give us the approach we need to make security smarter and harder to beat.

As part of TSA's improved security measures, we are deploying our workforce where we can achieve the best security result, most efficiently, and with minimal hassle for travelers. These improvements and this Subcommittee's support have enabled TSA to add critical new security layers based on risk.

The Travel Document Checker (TDC) program is now operating at all Federalized airports and enhances security by disrupting and detecting individuals who attempt to board an aircraft with fraudulent documents.

We have deployed hundreds of BDOs at the nation's busiest airports as part of the Screening Passengers by Observation Technique (SPOT) program. The SPOT program uses non-intrusive behavior observation and analysis techniques to identify potentially high-risk passengers based solely on their exhibited behavior. BDOs are trained to detect individuals exhibiting behaviors that indicate they may be a threat. The program is a derivative of other successful behavioral analysis programs that have been employed by law enforcement and security personnel both in the U.S. and around the world. Some of

our law enforcement partners at the local and Federal level have asked TSA to provide training on this successful program.

TSA believes a highly motivated workforce enhances our nation's security. We implemented a pay for performance system to recognize and reward individual and organizational performance, and created a career progression program for TSOs with new job classifications and opportunities to acquire new security skills. Our flexible personnel system authorities enable TSA to offer creative pay incentives, such as full-time health benefits for part-time TSOs. And most importantly, we listen to our employees. Through the National Advisory Council (NAC) – a formal group of TSOs nationwide elected by their peers and meet in person with TSA's senior leadership on a quarterly basis – and the Model Workplace program, TSA strives for continuous improvement by addressing employee concerns. At TSA, these programs reflect a genuine commitment by senior leadership. I have participated in every quarterly meeting of the NAC and many of their monthly conference calls.

Process. As mentioned earlier, TSA is continuing to implement innovations in the checkpoint process as well. The current checkpoint during a peak travel period can be noisy and congested, which has the potential to conceal the actions of someone with hostile intent. The checkpoint pilot strives to provide a more convenient layout for passengers with more information explaining the screening process together with a better security environment.

Another simple yet effective program that improves the checkpoint process is the Diamond Self-Select program. Our self-select screening lanes are designated by signage (modeled after the familiar ski icons) that directs passengers to the appropriate lane based on their travel needs and knowledge. Green is the queue line for travelers who need extra time or special assistance, such as families traveling with children, people with disabilities or those who need prescription liquid medications or other liquids for medical conditions. The blue lane is for casual travelers who are somewhat familiar with the security procedures. The black diamond lane is for expert travelers who know the TSA security requirements and arrive at the checkpoint ready to go through efficiently.

These dedicated lanes give passengers some measure of control over their own experience and also provide a better, less stressful environment for us to do our job. The result has been more effective and robust security. In cities with self-select lanes, we are seeing considerably lower alarm rates in the green lane because there is more time to prepare and remove prohibited items.

We have also provided airlines with more flexibility to allow passengers to check in remotely on line or at a kiosk who had previously been unable to do so because they have a name similar to someone on a watch list. Airlines are now able to create a system to verify and securely store a passenger's date of birth to clear up watch list misidentifications. By voluntarily providing this limited biographical data to an airline and verifying that information once at the ticket counter, travelers who were previously

inconvenienced on every trip now have an opportunity for a more convenient travel experience.

Technology. Through the support of this Subcommittee, we will be able to expedite the upgrading of technology at passenger checkpoints and for checked baggage screening. AT X-Ray and WBI technologies greatly enhance our ability to detect small IED components made of common items, which remain the greatest threat. AT X-Ray provides a greatly enhanced image with the ability to target novel threat items, resulting in fewer bag checks and faster throughput, as well as the ability to upgrade the system with enhanced algorithms. WBI technologies enable TSA to detect prohibited items such as weapons, explosives, and other metallic and non-metallic objects concealed under layers of clothing without physical contact. Bottled Liquid Scanners are an integral technology TSA will continue to deploy through 2009. These are used to ensure sealed containers do not contain threat liquids. Additionally, TSA will purchase and install reduced-size explosive detection systems (EDS) to increase security effectiveness and improve operational efficiencies through improved throughput.

Deploying new technology is important, and certainly a step this Subcommittee has encouraged, but we are also taking critical steps to reassess both the technology and the search methods used by our TSOs. TSA has commissioned three National Laboratories to work with us to keep these screening technologies advancing ahead of terrorist tradecraft, which seeks to exploit ingenious devices and ingredients.

Implementation of the 9/11 Act

I want to thank the Subcommittee for its ongoing support in providing \$20 million to TSA in FY2009 to implement new regulations and activities authorized by the 9/11 Act. TSA plans to use \$3.6 million to upgrade the Automatic Detection and Processing Terminal (ADAPT) system that determines threats in the airspace and reduces the time and energy spent tracking an unknown anomaly that presents no threat. As explained in the TSA Spend Plan recently provided to the Subcommittee, the remainder of the FY09 funding for 9/11 Act implementation will be used for surface security measures, including the hiring of an additional 50 TSIs for Surface, completing vulnerability and threat assessments for surface modes, developing the Inter-Modal Security Training and Exercise Program, and developing a transportation security Information Sharing and Analysis Center.

Air Cargo. The 9/11 Act included two air cargo security requirements that mandate the screening of 50 percent of cargo transported on passenger aircraft by February 2009 and 100 percent by August 2010. I am happy to report that while much remains to be done to fulfill this requirement, we are confident that the industry is currently screening at least 50 percent of air cargo transported on passenger aircraft on flights originating in the United States. The data analysis completed thus far shows that the 50 percent requirement is being met by the air carriers. We predict that the 100 percent screening requirement will be met by August 2010 for domestic cargo through our Certified Cargo Screening Program (CCSP). Under this program, the responsibility for screening is distributed throughout the supply chain to improve security while minimizing the

potential negative impact on the integrity and movement of commerce. The requirement in the 9/11 Act to also screen 100 percent of inbound air cargo from international departure points continues to present significant challenges. Although it is unlikely that we can meet the ambitious timetable set by Congress, we are working with our international partners to address the many challenges and expect to continue to see significant improvements in the level of security for inbound air cargo on passenger aircraft as we move forward.

A key component of achieving these milestones is the requirement, developed in coordination with air carriers and other stakeholders, that 100 percent of cargo transported on narrow-body (single-aisle) aircraft be screened. This requirement went into effect in October 2008. The passenger security impact of this screening is significant: although these aircraft carry only 25 percent of domestic air cargo on passenger aircraft, they account for the majority—approximately 95 percent—of domestic passenger flights. More importantly, these flights carry more than 80 percent of all passengers on flights originating in the United States. Thus, even at the statutory deadline for screening 50 percent of air cargo aboard passenger aircraft, we are effectively protecting the vast majority of the flying public.

Secure Flight

Beginning with the FY2005 DHS Appropriations Act, P.L. 108-334, Congress provided TSA with very specific guidance to address concerns with the implementation of the Secure Flight program and gave the Government Accountability Office (GAO) a proactive role in reporting on our progress. It is important to acknowledge that your oversight and our partnership with GAO towards meeting the ten conditions mandated by Congress made Secure Flight a better program and that it is now poised to effectively fulfill the mandate of assuming the prescreening process of comparing passenger information against the watchlists. Specifically, Secure Flight provides a consistent watch list matching process across all aircraft operators; allows for earlier law enforcement notification and coordination, if necessary; and decreases the chance of compromised watch list data thanks to its limited distribution. The Secure Flight program will also provide an integrated redress process that clears individuals who have been previously misidentified, have applied for redress, and have been placed on the Cleared List. Given the completion of the rulemaking process and operational testing and the progress in the oversight effort, I am pleased to report that the Secure Flight program began operational cutovers from certain aircraft operators on selected flights beginning on January 27, 2009. To date, four operators have successfully begun cutover and one has begun testing. I also do want to mention that TSA truly appreciates the cooperation and assistance these volunteer air carriers provided to the program during its initial rollout. We also appreciate GAO's efforts that enabled TSA to proceed with the initial operating capability of the program. TSA believes that the Secure Flight program will be able to assume responsibility for watch list matching of passengers for all domestic commercial flights by the end of the first quarter of calendar year 2010, and all international commercial flights by the end of calendar year 2010.

Global Outreach

As TSA continues to adapt to changing threats, we recognize the need to expand our zone of security and interdict threats before they arrive on our shores. By building trust through collaboration and partnership, TSA promotes the implementation of effective global transportation security processes worldwide while ensuring compliance with international and TSA standards. Focusing on closing gaps and providing enhanced capability, TSA seeks to manage risks and work with our international partners to harmonize security measures. The increasing influence we have in multinational organizations allows us to work with like-minded partners to raise the baseline for security. The global transportation community is only as strong as its weakest link; by prioritizing harmonization and capacity building efforts, TSA believes it can make a positive impact.

One example of our global efforts is our Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS) robust liaison relations with foreign air security partners. OLE/FAMS conducts training for foreign air marshals in relation to international terrorism. As shown in August 2006 in response to the discovery in the United Kingdom of a plot to use liquid explosives to take down passenger aircraft bound for the United States, TSA, to include the FAMS, worked with our international partners to respond overnight to conduct missions at unprecedented tempo and complexity in an effort to combat the threat and help preserve the confidence of passengers and air crews in the security of commercial aviation. Another example is the Aviation Security Sustainable International Standards Team (ASSIST). This program works to effectively build sustainable institutions through information sharing and best practices. Key focus areas include training needs, equipment, current aviation programs, and aviation security legislation. St. Lucia is the first nation to partner with TSA in this new program and we look forward to continuing this effort in other locations.

Conclusion

Mr. Chairman, thank you again for this opportunity to discuss TSA's efforts in aviation security. I look forward to our continued work together and would be pleased to respond to your questions.

AIR CARGO SCREENING PROGRESS

Mr. PRICE. Thank you, and let me say we are particularly pleased to receive the report about the 50 percent target. We know there has been some scrutiny of this by the GAO. We will look forward to their scrutiny of the documentation you can provide for the achievement you cite this morning. Let me move to what I think we would all agree is a more difficult question and that is the next goal of 100 percent screening of the cargo to be carried in the hold of passenger planes. That is what we are talking about here.

We know that this 100 percent goal by August of next year is an ambitious goal but an important one. To reach that goal you developed the certified cargo screening program which would permit certified supply chain facilities to screen air cargo using a variety of technologies prior to delivering the cargo to the air carrier through a secure chain of custody. I think we all understand that making that system work is absolutely essential to reaching this goal.

The certified cargo screening facilities must adhere to TSA mandated security standards. Earlier this year you began a limited Phase I roll out in the 18 major gateways focusing on shippers in nine cities and freight forwarders in all 18 airport markets. This work is all being done domestically. Eventually, a similar program is going to need to occur overseas.

I know you plan to evaluate the success of this program, before it can be expanded nationwide. So let me ask you just a few related questions on this matter. First of all, what kind of general assessment can you give us of how these certified cargo screening pilots have gone? What kind of problems have you encountered? Easier, harder than expected?

Part of all this of course is having the ability to secure cargo with tamper evident technology so that there is assurance that it has been screened at the point of assembly of the pallet, let us say, and that it has not been tampered with. How are you ensuring that once physical screening has been completed and the package or pallet has been sealed it will not be tampered with later in the process?

How far are we toward assuring this technology is working as it will need to? Then there is the matter of cargo coming from overseas. I think it would be helpful to the Committee just to have your realistic assessment of how you see this going short-term and longer term. Is the best way forward to screen most of this cargo overseas or should we assume, at least for the near term, that most of the cargo heading to our shores is going to have to be screened here and that we are going to have to have a system for doing that?

Here, too, this is a major component of that 100 percent goal. So that is what I am asking you. How are these various efforts proceeding? What are the biggest challenges to meeting the 100 percent screening requirement by August of next year?

Ms. ROSSIDES. Thank you, sir. First of all, let me break it down in terms of the domestic versus international. With respect to the domestic side, we are very confident that we will meet the 100 percent screening requirement by August of 2010 for domestic air cargo. We are doing that through a number of ways. First of all,

our inspectors will be going out and certifying these cargo screening facilities.

We are doing extensive out reach with the industry to identify these facilities. Of course, the supply chain solution is an excellent one to be able to spread the screening requirement across the supply chain so that we do not have a complete bottleneck at the airport locations. So, on the domestic side, we are quite confident, particularly working with the largest carriers. As you mentioned, it is really focused on 18 cities.

On the international side, the challenge is much greater. As much as I would like to say that we are certain we would make that 100 percent milestone I would have to say, in all honesty it is probably unlikely that we could make the 100 percent milestone by August of 2010. Our best estimate is perhaps about 75 percent of the progress will be made on the international front. The challenge there is it represents basically 98 countries that ship by air cargo into the United States, and so our approach literally has to be country by country.

Now, for example, in the U.K., their system, which has really served as a model for us, is a very, very good system, but we literally have to work with our partners through ICAO and our partners that we make through these other efforts with foreign countries get their systems to a standard that is commensurate with ours. That is going to be a challenge.

We still believe that the model of the supply chain approach with the certified cargo screening facilities in these countries is the only way that we hope to have them achieve this. We will use our Inspector cadre to go out and provide both support and inspect these facilities, and we will also be doing a tremendous amount of outreach. Your third point about technology, the challenges are in the technology arena.

As you know, the approach we are taking is that we are literally requiring the screening by piece of what is either assembled in a pallet or is shipped as a single airway billing, and so that requirement will help us ensure that it is commensurate with baggage screening, but that also puts quite a challenge on the industry. The technology that we are looking at today is everything from an ETD machine, which we use in the baggage area, to an EDS.

We have also been working with the DHS Office of Science and Technology to see what other new technologies we can really be leveraging. We have asked them to invite various industry in to try to help provide a solution for this challenge, but it is a challenge from the technology, especially once everything is in a pallet of this size.

TAMPER-PROOF TECHNOLOGY

Mr. PRICE. Does the assurance you have given us just now that this 100 percent requirement with respect to domestic cargo can be reached by August of next year, does that assume that well in advance of that date, this tamper-proof technology has been certified and has been recommended by you for use in securing these supply chains?

Ms. ROSSIDES. No, sir, I cannot speak to that specifically. I would have to follow up with a specific—

Mr. PRICE. I do not see how you can offer the assurance about the 100 percent goal until this tampering problem is more definitively dealt with.

Ms. ROSSIDES. I will take the question back. What the staff advises me on, with respect to the domestic, is by employing these certified screening facilities and ensuring that along the chain we have the proper measures in place, that will get us to the 100 percent milestone. But, with respect to the specific answer on the tamper proof technology, I will have to get back to you.

[The information follows:]

AIR CARGO CHAIN OF CUSTODY

A key characteristic of the Certified Cargo Screening Program (CCSP) is the rigorous tracking of the chain of custody, including the use of tamper-evident technology to assure that, once screened, cargo remains secured in transit to the aircraft. TSA is continually evaluating chain of custody technology and has issued procedures to all entities involved in the CCSP, as well as other members of the air cargo supply chain, to ensure that cargo remains secure as it moves along the air cargo supply chain. These procedures are Sensitive Security Information and TSA would be pleased to provide these to the Committee and discuss this matter further in the appropriate venue at the Committee's convenience.

INTERNATIONAL AIR CARGO SCREENING

Mr. PRICE. All right. And then, with regard to the second question about how this international cargo is going to be dealt with, I am not sure you stated your assumption totally clearly about how much of this is going to need to be dealt with in our domestic ports, as opposed to being handled overseas.

Ms. ROSSIDES. Well, one of the things we are looking at is those countries, for example, like the U.K. and Japan, what percentage are they actually bringing in today. And they represent about 40 percent.

And so wherever we have countries that are meeting the standards today, that will be the solution we have in place. If we get to the point where we have other countries that cannot make it, we are going to have to take a decision down the line as to what to do in terms of those foreign countries, and whether we have to create some system here in the U.S. to address it.

But, right now, our goal is to try to get the compliance and the level of screening commensurate in those countries at the point of origin.

Mr. PRICE. All right. So when you say 75 percent by the appointed date for the international cargo, you are basing that on an assumption that you can do 75 percent of this cargo at the point of origination.

Ms. ROSSIDES. Right, in these foreign countries. Correct. So what we are hoping is that these countries will be compliant, and then we will only have to go after smaller countries where actually the load that is coming in is much smaller.

Mr. PRICE. Well, it does seem to me that dealing with that problem should not have to wait until a determination some years from now, that we are not going to be able to achieve this kind of screening at the point of origin.

Ms. ROSSIDES. Oh, no.

Mr. PRICE. Because there needs to be a provision obviously in the near term for screening this cargo on our shores, when this cannot

be arranged overseas. And clearly, we are not going to reach 100 percent for some time in that regard.

Ms. ROSSIDES. Right. And right now, literally, our folks are working with folks in the U.K., in the E.U. We are reaching out. We are visiting foreign countries right now. We are not waiting for later in 2010 to address this issue. We have people who are working in these foreign countries right now, trying to get an assessment and trying to get those capabilities up in those countries.

I did not mean to suggest that we are going to wait until 2010 to say we have a problem. We will know much sooner than that.

Mr. PRICE. No, I am talking about having a problem in terms of our ability to screen that cargo here, when it has not been screened overseas.

Ms. ROSSIDES. Right. And we will know that sooner, rather than—

Mr. PRICE. All right. Mr. Rogers.

Mr. ROGERS. I am assuming that most of that international cargo will be palletized cargo?

Ms. ROSSIDES. For the most part, yes, sir. When it is coming in the large numbers, like from the U.K. and Japan.

Mr. ROGERS. If you do not mind, move that microphone closer.

Ms. ROSSIDES. I am sorry.

EQUIPMENT FOR INSPECTION OF AIR CARGO

Mr. ROGERS. But we do not have an explosives detection machine yet to examine palletized cargo, do we?

Ms. ROSSIDES. That is correct.

Mr. ROGERS. So how will you, how will you inspect international cargo, either there or here, without a machine?

Ms. ROSSIDES. Well, sir, the requirement is that it be inspected by the piece. So that means, it has to be inspected by the piece before it can be put in the palletized configuration. That is the expectation. And then that can be done via the ETD equipment, EDS equipment, canine, physical hand search of each piece, before it is palletized.

UPGRADE SECURITY EQUIPMENT

Mr. ROGERS. In the last three fiscal years, TSA has received nearly \$2 billion for EDS procurements.

Ms. ROSSIDES. Yes, sir.

Mr. ROGERS. Specifically, \$1 billion within the recent stimulus bill, which comes on top of the \$294 million that was provided in 2009. And this large infusion of funding in 2009 is more than four times the amount of funding received for FY-08.

So happily, there is then a great infusion of monies into the explosion-detection machine field, because we have been way behind in that.

However, that large infusion of money I think represents an opportunity to upgrade the security equipment at a significant number of airports. Do you have a schedule now in place about the airports you are going to upgrade?

Ms. ROSSIDES. Yes, sir. As part of the stimulus funding, we actually have 16 airports that we are working with right now. And, as

part of our Fiscal Year 2009 planned purchases, we have other airports that we are looking at.

We have a schedule, we have a strategic plan. And the beauty of these investments is, particularly with the additional stimulus funds, it has allowed us to accelerate our checkpoint technology plan by about two years. And for our baggage area, it has allowed us to address airports that are ready with proposals in to us, so that we can ensure some quick spending of this stimulus money.

Mr. ROGERS. Do you have the list of the 16 airports that are on the list?

Ms. ROSSIDES. I do not have it with me, but yes, sir, we have those established. And we have notified them. We have given them interim letters of commitment.

Mr. ROGERS. Will you file that with your testimony?

Ms. ROSSIDES. Yes, sir. Yes, sir.

[The information follows:]

ARRA Airports Under Consideration for Funding

The following airports are under consideration for funding for checked baggage explosive detection system projects under the American Recovery and Reinvestment Act.

- Honolulu International Airport (HNL)
- Kahului Airport (OGG)
- Philadelphia International Airport (PHL)
- Norman Y. Mineta San Jose International Airport (SJC)
- Tallahassee Regional Airport (TLH)
- Portland International Jetport (PWM)
- San Francisco International Airport (SFO)
- Sacramento International Airport (SMF)
- Jackson Hole Airport (JAC)
- Huntsville International – Carl T. Jones Field Airport (HSV)
- Orland International Airport (MCO)
- John Wayne Airport – Orange County (SNA)
- James M. Cox Dayton International Airport (DAY)
- Port Columbus International Airport (CMH)
- Hartsfield – Jackson Atlanta International Airport (ATL)
- Louis Armstrong New Orleans International Airport (MSY)

In addition, the following airports are candidates for reduced size equipment for recapitalization purpose or to replace ETDs as primary screening equipment:

- Denver International Airport (DEN)
- Chicago O'Hare Airport (ORD)
- Philadelphia International Airport (PHL)
- Seattle-Tacoma International Airport (SEA)
- Bradley International Airport (BDL)
- Birmingham International Airport (BHM)
- El Paso International Airport (ELP)
- Guam International Airport (GUM)
- Lihue Airport (LIH)
- Adams Field Airport (LIT)
- Kansas City International Airport (MCI)
- Memphis International Airport (MEM)
- Metropolitan Oakland International Airport (OAK)
- San Diego International Airport (SAN)
- Akron-Canton Regional Airport (CAK)
- The Eastern Iowa Airport (CID)
- Gerald R. Ford International Airport (GRR)
- Hilo International Airport (ITO)

- Eppley Airfield Airport (OMA)
- Santa Barbara Municipal Airport (SBA)
- City of Colorado Springs Municipal Airport (COS)
- Springfield-Branson National Airport (SGF)
- Roanoke Regional/Woodrum Field Airport (ROA)
- Henry E Rohlsen Airport (STX)
- Kalamazoo/Battle Creek International Airport (AZO)
- San Luis Obispo County Regional Airport (SBP)
- Meadows Field Airport (BFL)
- Gainesville Regional Airport (GNV)
- Montgomery Regional Airport (MGM)
- Craven County Regional Airport (EWN)
- Rochester International Airport (RST)
- Bethel Airport (BET)
- Kenai Airport (ENA)
- Greater Binghamton/Edwin A Link Field Airport (BGM)
- Nome Airport (OME)
- Erie International/Tom Ridge Field Airport (ERI)
- Pago Pago International (PPG)
- Monroe Regional Airport (MLU)
- Ralph Wien Memorial Airport (OTZ)
- Redding Municipal Airport (RDD)
- Elmira/Corning Regional Airport (ELM)
- Mercedita Airport (PSE)
- Laredo International Airport (LRD)
- Brownsville/South Padre Island International (BRO)
- Great Falls International Airport (GTF)
- Florence Regional Airport (FLO)
- Columbus Metropolitan Airport (CSG)
- Abraham Lincoln Capital Airport (SPI)
- Lewiston-Nez Perce County (LWS)
- Branson Airport (BBG)

Mr. ROGERS. Now, what will happen at those airports?

Ms. ROSSIDES. It is a combination. They will be having optimal screening systems put in, focusing on checked baggage. It runs a range from replacing in-line, replacing lobby solutions, to in-line solutions. In some cases it may be some new terminal work with additional EDS technology and in-line systems.

And there, the advantage to us with these programs, as I said, they have already had their plans and proposals in to us. So, we are hoping that we are going to be able to address them very quickly.

Mr. ROGERS. Are these the larger airports?

Ms. ROSSIDES. For the most part, yes, sir. But in addition, what we are looking at, the combination of Fiscal Year 2009 dollars and stimulus dollars, is also to address some of the requirements of CAT 2 and 3 airports, with a reduced-size EDS, and trying to really look across the whole system as to how to best maximize the use of these dollars.

Mr. ROGERS. Well, it has been my experience that the place where we could gain fewer personnel and more technology were the small- and medium-sized airports, where, up until fairly recently, a lot of the activity was being done manually in the lobbies. And a single machine could save us a lot of personnel costs.

Is that still the operating philosophy?

Ms. ROSSIDES. Yes, sir, that is one of them. We are actually looking at equipment in our new Transportation Security Integration Facility over at DCA, as to how that kind of technology can be used for both, you know, carry-on and checked baggage in the smaller airports.

NUMBER OF SCREENERERS

Mr. ROGERS. And getting to the bottom line, how many screeners do you have there?

Ms. ROSSIDES. Sir, we have, not including our screening managers, approximately 44,500, FTE dedicated screeners.

Mr. ROGERS. Forty-four thousand, five hundred.

Ms. ROSSIDES. Yes, Yes, sir.

Mr. ROGERS. Well, that is 500 short of 45,000, is not it?

Ms. ROSSIDES. Yes, it is, sir.

SECURE FLIGHT

Mr. ROGERS. Magically. Secure Flight is going well?

Ms. ROSSIDES. Yes, sir, it is, it is going very well. We have some, as I mentioned in my oral statement, we have four carriers already. We have three in the queue. We actually have a schedule now that we are working out with the major U.S. carriers in terms of their cut-off, cut-over dates. It is going very well.

We are working with GAO on the final tenth condition to satisfy that requirement. And, I believe it is going to be very, very successful, sir.

Mr. ROGERS. Question.

Ms. ROSSIDES. Yes, sir.

Mr. ROGERS. I am a Secure Flight recipient, say. What does that get me?

Ms. ROSSIDES. Well, sir, by providing your name, your date of birth, and your gender, we are confident that we will have far fewer misidentifications for persons who are currently experiencing misidentification with names on the watchlist.

So, the real benefit is for those persons who frequently get misidentified, who get stopped at the ticket counter, who cannot print their boarding passes in advance, who get questioned as to having to go through a redirect process. We are confident that once Secure Flight is on line for all carriers, that those misidentifications will be dramatically reduced.

MASS TRANSIT SECURITY HELP

Mr. ROGERS. TSA really is the face of Homeland Security for most Americans, because it is where we encounter inspections and uniforms, and the like.

However, a lot of people say the most vulnerable aspect of what TSA is doing is mass transit. Subways, rail, and the like. And as you know, we have just concluded the second hearing of FEMA, and TSA's people on getting these rail grants, mass transit grants out there.

We are all frustrated with that. Can you help us out?

Ms. ROSSIDES. Yes, sir. Several things. One is that, as a result of the prior hearing really several weeks ago, we have done a "deep dive" within TSA in terms of how can we better enable that process to support both the FEMA process and the agencies that are the recipients of those funds.

We are committed to really doing follow-up work with those agencies in terms of what difficulties they are having in putting their final plans together to execute those funds. Because our goal in the end, frankly, is to get those grants out, and get the intended use in place, that is the security advantage we are looking for.

The other thing that we are looking at is in doing our extensive outreach with both rail and mass transit. We are looking at what other ways can we support them in not only the grants area, but in things like our VIPR teams and trying to find additional ways that we can really, you know, support their needs at the local level with respect to rail and mass transit.

Mr. ROGERS. Well, it is a very difficult problem.

Ms. ROSSIDES. Yes, sir.

Mr. ROGERS. Given the number of people that use the mass transit and the exposure of the rail lines and the tunnels, and so on. And the need to be unobtrusive in your efforts. So I understand the difficulty of the task.

However, because of the numbers involved, numbers of users of mass transit, it has to be addressed, and it has to be done forthwith. We have been frustrated by appropriating huge amounts of money, only to see it lay there being unused. And we get bureaucratic gobbledygook when we try to understand what the problem is, and how we can solve it.

We are going to have to have you crack some heads.

Ms. ROSSIDES. Yes, sir.

FEMA PROBLEMS

Mr. ROGERS. And I realize that part of the difficulty is in FEMA, which is not under your direct jurisdiction, of course. And we do not expect you to defend or condemn them.

But we are frustrated. Are you frustrated?

Ms. ROSSIDES. Yes, sir. I am, and I share your frustrations and understand them.

My experience prior to TSA with respect to grants is that they are sometimes very difficult to administer. I am not making excuses for FEMA at all, but I do know that there are challenges, both to the Federal Government in putting the funds out and for the recipient agencies to bring those funds in. And, we have to look at the whole process and make improvements on it.

Mr. ROGERS. Well, we are looking to you for that. Thank you.

Mr. PRICE. Thank you. Mr. Serrano.

FOCUS ON AIR TRANSPORTATION VERSUS OTHER MODES

Mr. SERRANO. Thank you, Mr. Chairman. Thank you for your testimony, and thank you for your service.

I probably will live to regret this statement, because I take Amtrak. And it seems that the kind of screening is nowhere near what we know happens at airports. And I say I will probably regret it, because starting next trip, I will probably receive it, too.

My question is, have we weighed heavily on the side of air transportation as a reaction to September 11? And if so, are we then going after the kind of attack that already took place rather than paying attention, or equal attention, to the kind of attack that could take place?

Again, no traveler, no commuter likes to be imposed upon. I have just touched on that. Or to be in the way, so to speak. But it is clear that there is a total difference in one.

Now, that may be based on information that even the committee may not have as to what is special out there. It just seems to me that maybe, maybe, I am asking you, have we gone too heavy on that side, and not looking at the others?

Ms. ROSSIDES. Well, sir, it is really a set of different models. In the aviation domain, ATSA, which created TSA, required very specific things to be done in aviation. And yes, I believe that was in response to 9/11, but it also, I think, demonstrated the support of the Subcommittee, the tremendous work that has been done and improvements in the aviation domain.

The other modes of transportation really, from a federal perspective, are secured in a variety of different ways with tremendous reliance upon the state and local agency level to provide the resources, the police, the security value.

What we do at TSA is maintain very close coordination with the security directors in all these different modes of transportation, and with people like the Amtrak security director. We see our job as multi-purpose.

One is to feed them information on what the intel is, the levels of threat that are here in the United States to those other modes of transportation.

We also have done training in the area of security in mass transit. We have looked at how do we supplement their resources with our program—our VIPR program, which deploys Federal Air Marshals, Inspectors, and TSOs into these other modes of transportation.

We recognize that we do not have the federal resources to bear to apply the exact same model that we have in aviation, but we have the shared responsibility for securing those modes, as do the agencies and state and local governments.

And, it is a question of how do you secure those modes, and not impact, commerce and the passengers, and recognizing we have, millions of people that travel through those other modes every day.

So, I would say that I believe that the Congress and TSA's response in the aftermath of September 11 has shored up and strengthened aviation. And, I think that what we are doing with these other modes of transportation is very good in terms of providing them support in a different way.

Mr. SERRANO. Yes. It just seems to me that there is a disconnect of some sort. Because your statement, and it is correct, sort of leaves other modes of transportation at the local level, with your involvement. Yet the other, aviation, is totally federally controlled.

Where I may take issue, and it is not necessarily with you personally, but a statement in general about a lack of resources to expand. I have been on this Subcommittee since it was formed, and if there was a Subcommittee that had a blank check, certainly for a while, it was this Subcommittee. We just printed the money I think somewhere in the basement, and a lot, a lot of money, as a matter of fact.

I do not know what the figure is, Ranking Member, but it is has been quite a bit of money. I think only the FBI ranks up there in terms of the same issue where we give the FBI through Congress just to assign the stakes, anything they wanted.

So I just think that there is a need to inform them as a Congress a little bit more about what is being done in other areas, so we do not have any surprises. Thank you.

Mr. PRICE. Thank you. Ms. Lowey.

EMPLOYEE SCREENING

Ms. LOWEY. Thank you, Mr. Chairman. Madame Administrator, the Subcommittee was told many times by former Administrator Harley, others at the Department, that 100 percent screening of airport employees was not reasonable, and would significantly slow airport operations.

Yet when this Subcommittee provided TSA with the resources to conduct the screening pilot program last year, the doomsday scenario, I understand, that was previously predicted was never realized. And in fact, the largest airport in the program, Boston's Logan International, is likely to implement 100 percent employee screening on a full-time basis.

Frankly, it is hard to believe that implementing this requirement nationally would be impossible, when two of the busiest airports in the world, Heathrow and de Gaulle, already do it successfully, and two large domestic airports, Miami and Orlando, find it critically important to their security.

If you could describe to the Subcommittee what, if any, negative consequences were witnessed at the airports involved in last year's pilot program, I would be appreciative. And do you believe it would be a valuable exercise to once again pilot the effectiveness of 100 percent employee screening at another set of airports in Fiscal Year 2010?

Ms. ROSSIDES. Yes, Rep. Lowey. As you know, we did a pilot of seven airports, Logan and Denver were the two CATXs that were part of that pilot. Logan did 100 percent employee screening.

We owe you, and we owe the Subcommittee, a report, which I am very sorry has not gotten to you yet, on the evaluation that was done by the Homeland Security Institute on those seven pilots.

In essence, the pilot program showed was that there was no clear distinction of the screening effectiveness between the 100 percent and the aggressive random screening. And, by that, what it showed is that every airport is different and you have to consider the operational impact and the infrastructure of an airport as to whether or not you could actually effectively do 100 percent screening without putting significant costs into the infrastructure and the operations.

I would respectfully request, when we get that report to the Subcommittee as soon as possible, that we will come up and brief you, and then see what the way ahead would be and what the Subcommittee would be interested in doing.

Ms. LOWEY. Okay, so we will wait for that. But I would be interested in knowing if there were any negative consequences as a result of those pilots. So if you could include that, I would be appreciative.

Ms. ROSSIDES. Yes, ma'am.

COLLECTIVE BARGAINING FOR TSA EMPLOYEES

Ms. LOWEY. Administrator Rossides, you called the employees of TSA your biggest investment and most valuable asset. Yet the more than 40,000 transportation security officers continue to be denied the same basic collective bargaining rights granted to other front-line security personnel in the federal workforce employees: Customs and Border Control, Immigration Customs Enforcement, Capital Police, Pentagon Force Protection Agency.

And before the House adjourns this week, I will be introducing legislation to grant all TSA employees the right to bargain collectively. And I hope the members of this Subcommittee will join the effort.

Secretary Napolitano testified before the authorizing Committee that she was checking with general counsel on the issue of TSO collective bargaining.

Number one, I would like to know if you have an update on these discussions. Your testimony highlights the lowered attrition rates among TSO. Where does the 7.5 percent rank as compared to other federal agencies? And what is the attrition breakdown between full-time and part-time TSOs?

Ms. ROSSIDES. Yes, Rep. Lowey. First of all, let me start my comments by saying that during my 30-plus years working in the Federal Government, I worked at the Treasury Department where we

had collective bargaining for the workforce. So, I am very used to that in the federal workforce.

Yes, Secretary Napolitano has indicated that she first would like to have a permanent Administrator in place at TSA, and is looking at what options she has available to her on the subject.

I would like to offer to you that whatever the Secretary decides, or this Subcommittee decides, and the Congress decides, we will do at TSA, and we will do it very well. Because, if there are two corporate principles that I and the leadership of TSA believe in, it is that we owe it to the American People to provide a level of security that is the best in the world. And, we owe it to our employees to provide the very best quality of work life that we can provide to them.

You mentioned the attrition rate with progress we have made in four years. The attrition rate and the time. The full-time attrition rate four years ago was over 30 percent. Today, for the voluntary full-timers, it is 7.5 percent. The part-time attrition rate four years ago was over 50 percent, and today, it is 17 percent.

The progress in that area goes right to the heart of involving our employees in telling us what are things that they would like to see in the workplace that we could put in effect.

So, for example, for the part-time employees, we provide full-time health benefits. Just doing that has significantly contributed to reducing the attrition.

I would like to talk about injuries. Another area that TSA has tremendously focused on in its workforce initiatives was in the area of injuries. I will tell you today that we do not have the worst injury rate in the Federal Government because we have made dramatic improvements in cutting those injury rates by more than 50 percent.

All of this has been because our employees have been able to be a part of giving us the solutions.

I believe that collective bargaining is a very serious issue. I have full respect for our employees' ability today to join a union. We allow the employee's representatives to represent them if there is any kind of discipline issue.

And I believe that in the end, what we all want is what is in the best interest of our commitment to providing our mission, and what is in the best interest of our workforce.

I will tell you, in all honesty, that my involvement in TSA has been a labor of love. And, I do not think you will meet anybody on this planet that wants something for the welfare of our workforce as I do.

So, whatever the Secretary ultimately decides, we are 100 percent ready to make it in the best interest of our workforce.

Ms. LOWEY. Thank you. And thank you, Mr. Chairman.

Mr. PRICE. Thank you. Mr. Rodriguez.

Mr. RODRIGUEZ. Thank you very much. And let me first follow up, you have not had to use a tissue—

[Laughter.]

BUS TRAVEL

Mr. RODRIGUEZ. That is good. Let me follow up on what Congressman Serrano had talked about. We usually talk about air and

rail. I wanted to see if you could, if nothing else, later on get me some information on bus travel. Because I know hundreds of thousands of people go through the bus, and I think we only provide some security, and we have a strategy in that area.

Secondly, I wanted to ask you, I know we have, you know, somewhat successfully established an international register travel program on air and land with Canada. But with Mexico, we have not. I know we have done something there with the air program, but not with land. I mean, excuse me, not with the air program, and yes, with the land.

And Mexico is the second-largest market for inbound travel for both business and leisure to the U.S. For both consecutive years, Mexico has been record levels on travel in the United States, totaling 9.6 billion in 2007, and the second trading partner, and in terms of leisure travel, as well as business.

Why have not we established a register to travel program with both Canada and Mexico?

Ms. ROSSIDES. Sir, I will have to get back to you on that. I do not have an answer that I can give you right now, but we will definitely follow up.

[The information follows:]

TSA BUS SECURITY ACTIVITIES

TSA's Highway and Motor Carrier Division, Passenger Carrier Branch has actively initiated and broadened its security awareness training of commercial motor coach operators nationwide using awareness programs created both by the industry and by TSA/DHS grant initiatives. These programs provide 24/7 reporting facilities that are in direct contact with TSA's Freedom Center operations. TSA has also leveraged DHS grant programs averaging \$8 million to \$10 million per year since 2003 to implement driver shield, passenger screening and security training initiatives in the commercial motor coach industry.

Motor carriers of passengers in the southern border region have long practiced heightened security procedures in direct recognition of a history of violent encounters at the border. However, the highway-specific Information Sharing and Analysis Center (ISAAC) created under a grant by TSA to the "First Observer" awareness program in 2008 has recently issued an alert of all motor carriers along the southern border. That alert focuses attention on the heightened threat of vehicle hijacking and kidnapping. It was distributed to the entire highway motor carrier community early in March.

TSA works closely with major bus companies on security improvement. In addition, TSA works with Customs and Border Protection to coordinate security efforts in this region.

Mr. RODRIGUEZ. Okay, thank you. And then, because I think if we can do that and see what we need to do to make that happen. Because next to Canada, Mexico is our second partner in terms of leisure travel, as well as trade. And if we can expedite that and make that happen, it would be great.

And then the second question regarding the bus travel. We have thousands of people in there, and my understanding is that we only have, you know, in major metropolitan areas, and that is about it on bus.

Ms. ROSSIDES. Correct. What we do have, as part of our ISAC program is an ability to monitor the travel on a bus around the country. And that is in its infancy. But, we are looking at how do we communicate with bus drivers, how do we provide some security value and training for them as part of our outreach efforts, and working in the consortium of the bus companies.

Mr. RODRIGUEZ. What I would be interested to know, if we have a strategy, how to deal with it and how to, you know. Especially, I guess, close to those states on the border, as well as the Canadian and the Mexican side, and see how we can help secure that.

Ms. ROSSIDES. Right.

Mr. RODRIGUEZ. Okay. Thank you very much. Thank you for being with us.

Mr. PRICE. Thank you. Ms. Roybal-Allard.

SECURING UNIFORMS AND BADGES

Ms. ROYBAL-ALLARD. Thank you, Mr. Chairman. First of all, I would like to express the same concerns that Ms. Lowey just did. With regards to the fact that 100 percent of airport employees are not being screened, especially in light of the fact that there has been a recent report of airport workers smuggling guns and narcotics onto commercial planes.

So I will be interested in your report, and also if those seven pilots actually reflect what could be done. Because there is about 300, or more than 300 airports. So I would be interested to see if those seven that you did pilots really are a reflection of all the airports.

Also, if you could include in that report, I would appreciate it if the conclusion is that it is not possible, for whatever reason, is what contingency plans, then, do you have in place to prevent a terrorist from becoming an airport employee in order to sabotage or, you know, hijack a plane?

Because certainly if you can get people smuggling guns and narcotics on planes, it is certainly possible that a terrorist also could get onto a plane, as an employee.

I would like to talk a little bit about the TSA badges and the uniforms. As you know, an investigation by DHS Inspector General of missing TSA badges and uniforms concluded that the Agency does not have adequate controls to track these items; and that this increases an airport's level of risk to a wide variety of terrorist and criminal acts.

In September 2008, the Inspector General recommended the TSA strengthen its policies and guidance related to securing a uniform and badges. Could you tell the Subcommittee what steps have been taken to implement the IG's recommendation?

Ms. ROSSIDES. Yes, ma'am. With respect to the uniforms and badges, we have provided training to our employees. We also have an accountability for the new badges that is required of every Federal Security Director to account for all of the badges. Any report of a missing or lost badge is investigated by our Office of Inspection.

We have had a very small number of badges lost since we have issued the new uniform in September, with the metal badge. The employees are required to conduct the training as part of their initial orientation, and annually, on the importance of safeguarding the badges, in particular.

SECURITY OF AIRPORT WORKERS

If I may, if I could go back for one moment to your comment about what assurances or confidences do we have with respect to

airport workers and people getting on aircraft, or putting prohibited things on an aircraft.

TSA, in 2006, began a program where we have our TSOs randomly go through the secured area of the airport, and do things, including gate-screening and patrolling the perimeter. We also require all airport workers to be vetted.

So there are a number of things that we have in place today that are fairly aggressive measures that provide for random screening inside the secured area, getting to the exact concern that you are describing as an insider threat.

Ms. ROYBAL-ALLARD. But still, there are some vulnerabilities there that could have been cited. So again, I would be interested in your report.

Also, TSA conducts covert tests of airport security, in which undercover inspectors attempt to pass through passenger checkpoints with weapons and other prohibited items.

And according to an August 2008 GAO report, TSA failed to systematically record the reasons for the airport failing the tests. And GAO has said that without this information, that you are very limited in your ability to correct inadequate security in airports.

How are you addressing this limitation? And are you implementing, again, GAO's recommendation to fully document a covert test failure?

Ms. ROSSIDES. Yes, ma'am. Since that GAO report, we do actually document the reasons. But, prior to that, even when the covert test teams went out to the airports, they did a number of things to advise the TSOs in the immediate aftermath of the testing, and the Federal Security Director, as to what they observed that they believed contributed to the failures, as well as what they observed that contributed to the passing of the testing.

And then after every trip that the covert team makes, they come back and brief everybody, from the Administrator through the executive staff, of not only what the test results were, but their observations. And, they have always issued recommendations for tightening up procedures, such as focusing on better training of supervisors to be vigilant as to the officer's performance on the checkpoint, on any number of measures.

So we have implemented the GAO recommendation. But, prior to that, we had a tremendous amount of dialogue on what were the things that the covert teams observed every time they went out and did these tests.

Ms. ROYBAL-ALLARD. Thank you, Mr. Chairman.

LARGE AIRCRAFT SECURITY PROGRAM

Mr. PRICE. Thank you. We are aware that the time is getting rather late. I would like to have a very efficient final round of questions. And I will begin, because I think it is important to focus on the general aviation matter that I mentioned in my opening statement.

Ms. Rossides, as you know, on October 30 of last year TSA announced a notice of proposed rulemaking that would strengthen the security of general aviation by further minimizing the vulnerability of aircraft being used as weapons or to transport dangerous people or materials. This so-called Large Aircraft Security Program Regu-

lation would require all U.S. operators of aircraft exceeding 12,500 pounds maximum takeoff weight to implement security programs that would be subject to compliance audits by TSA. The proposed regulation would also require operators to verify that passengers are not on the no-fly and/or selectee portions of the federal government consolidated terrorist watch list.

Airports, pilots, small businesses, and the general aviation community have expressed serious concerns, to put it mildly, over some of these proposed regulations, saying they are overly intrusive, would pose significant financial and resource impacts on general aviation airports across the country, and so forth.

And so this rulemaking does appear to be one of the more controversial issues from the waning days of the last Administration. TSA has been asked by numerous entities to delay its implementation until the new leadership at DHS can review it.

I know you are in the process now of weighing costs and benefits, that you are continuing to work with the affected stakeholders. So I want to ask you just a couple of things.

What is the current timeline and status of this rulemaking, first of all? And secondly, to what extent is it being rethought? Are you considering alternative security measures for general aviation aircraft?

Ms. ROSSIDES. Yes, Mr. Chairman. First of all, let me say that the rulemaking when it went out, it specifically addressed security vulnerabilities that we felt needed to be raised and addressed. Those vulnerabilities included things like who the pilot is, who is actually commandeering that aircraft, who are the other people on board that aircraft, and what is actually being transported on board that aircraft.

The initial interest was to address what we were concerned about in terms of security vulnerability.

It was also very much a risk-based decision to address it at the 12,500-pound-size aircraft, which really covers about 4 percent to 5 percent of the general aviation community. We received over 6,000 comments to that proposed rulemaking. We extended the comment period by 60 days from the initial deadline. We conducted public hearings around the country. Now, we have over 6,000 comments that we are looking at.

What we have decided to do is actually bring in representatives from the general aviation community. We have a meeting scheduled for April 6. We are going to have the members come in and help us look at what are the interests from the security standpoint, what are their concerns, and come up with the best options.

Once we have had that meeting, we intend to go out with a second proposed rulemaking period of time for comments from the community and from the general public.

Obviously, no final rule will be made until, no final decisions will be made, without bringing in the DHS leadership.

Mr. PRICE. Well, that second round is an unusual process for you.

Ms. ROSSIDES. Yes, it is. Yes. We have only done it one other time, and that was when we were implementing Secure Flight.

We believe that this, plus the in-person engagement, and the April 6 meeting should help address concerns and get some common understandings out there.

Mr. PRICE. Well, I think it is well-advised, and I appreciate your undertaking this additional layer of review. We know there are security vulnerabilities here, we know this needs to be dealt with. But I do believe, under the circumstances, this is warranted. And we will look forward to reviewing with you the results of this process.

Mr. Rogers.

Mr. ROGERS. Well, nothing further, except to echo the Chairman's remarks about general aviation. I have heard a lot from them. I am sure, obviously, you have.

But in the rural parts of the country, in which I live, general aviation is the way to get around. And a lot of these pilots, charter and/or personal, cannot understand that you do not know that they know every person that gets on that plane, and they know every nut, bolt, and screw in that plane, and they know everything that somebody brings on that plane. So they are quite upset.

Thank you for your service. You have been a long-time worker in that venue, the TSA, from its very inception, in fact. And worked most recently with Kip Hawley, who did, I think, a masterful job of bringing TSA around, along with all of your-all help. Give our regards to him if you talk to him.

Ms. ROSSIDES. I will.

Mr. ROGERS. Thank you.

Ms. ROSSIDES. Thank you.

Mr. PRICE. Thank you. We do appreciate your service and your testimony here today. I look forward to working together going forward.

With that, the Subcommittee is adjourned.

QUESTIONS FOR THE RECORD SUBMITTED BY

CHAIRMAN DAVID PRICE

**Gale Rossides, Acting Administrator,
Transportation Security Administration**
Improving the Efficiency of the Aviation Security System

Air Cargo Security

Question: The 9/11 Act requires DHS to establish a system to screen 50 percent of cargo transported on passenger aircraft by February 2009 and 100 percent by August 2010. TSA has told Subcommittee staff that it was able to easily meet the 50 percent deadline because of a variety of initiatives it undertook, including requiring its personnel to screen 100 percent of cargo carried on passenger aircraft at the nation's 250 smallest airports, removing almost all cargo screening exemptions, and mandating that all nonexempt cargo carried on narrow body aircraft be screened. Yet, GAO testified on March 18th that TSA cannot verify that 50 percent of all nonexempt air cargo carried on passenger aircraft is actually being screened. This stems from the fact that TSA does not have a system in place to provide verification and to collect data from screening entities. When and how will you be able to do this verification?

ANSWER: The Transportation Security Administration (TSA) does have a system in place for the collection and verification of data provided by air carriers. The data for each month is unavailable until the subsequent month due to the time that is required to compile and report the information. TSA can confirm that the 50 percent screening mandate was met for both February and March 2009.

Question: TSA is now piloting a voluntary program to permit cargo screening by certified entities at additional points along the supply chain. For the record, please elaborate on this pilot, including who is participating, the timing, and how it will work? When do you expect to see results from the pilot to decide how this screening should work in a longer context?

ANSWER: The Certified Cargo Screening Program (CCSP) is no longer in the "pilot" phase, having begun in December 2008. The CCSP allows screening of cargo at all points in the air cargo supply chain by a trusted, vetted, audited, federally regulated facility. CCSP establishes the integrity of a shipment through enhanced physical and personnel security standards at Certified Cargo Screening Facilities (CCSFs), of which 320 are currently in existence. The program also maintains the integrity of a shipment throughout the supply chain by utilizing stringent chain of custody methods. Program Participation in CCSP is voluntary, but once certified, CCSFs are subject to TSA compliance inspections.

The CCSP is a facility-based program. Entities that may become CCSFs include, but are not limited to, shippers, manufacturers, third party logistics providers, warehouses/Distribution Centers, Freight Forwarding Facilities, and Independent Cargo Screening Facilities.

The Certified Cargo Screening Facilities have already contributed significantly (20 percent) toward industry's attainment of the 50 percent milestone in February 2009.

Question: To date, how have the certified cargo screening pilots gone? What problems have you encountered? What was easier than expected?

ANSWER: TSA's outreach efforts have been received favorably by industry. TSA continues to receive applications and certifies entities throughout the air cargo supply chain.

Many Certified Cargo Screening Facilities are entities that were previously unregulated and required additional outreach efforts to familiarize them with TSA regulations and regulatory responsibilities. TSA also identified unique commodities and business models requiring additional consideration. Additionally, some delays are being encountered due to longer-than-expected screening equipment production lead times.

The industry's open collaboration and receptiveness to the flexibilities provided by the Certified Cargo Screening Program has been greatly appreciated and TSA has received very positive industry support from the airline and freight forwarding community.

Question: Assuming that the screening of air cargo, for the most part, will permanently move away from the airports and the airlines to certified off-site facilities (e.g. manufacturers, indirect air carriers and freight forwarders), detail who will screen packages before they are consolidated into pallets and what standards you will set to make sure that the same level of screening is applied everywhere.

ANSWER: TSA does not anticipate that all screening will move away from the airport. The Certified Cargo Screening Program (CCSP) provides industry the flexibility to screen cargo at the point most appropriate for a given supply chain participant. Air carriers will continue to screen a percentage of freight and retain the ultimate responsibility for ensuring that cargo is screened prior to uplift on passenger aircraft. Other screening will be performed at Certified Cargo Screening Facilities by vetted and trained individuals.

Screening standards in the Certified Cargo Screening Program are outlined in the appropriate security programs and are enforced by Transportation Security Administration compliance inspectors. These standards are the same as those utilized by air carriers.

Question: According to recent GAO testimony, TSA has not yet issued guidance on when and how to secure cargo with tamper-evident technology. The testimony notes that TSA plans to test and evaluate such technology and issue recommendations to the industry, but have not set any time frames for doing so. What is your time frame to issue guidance on how to secure air cargo for the various entities that handle and screen air cargo shipments prior to its loading onto an aircraft? Why has TSA not completed this step already?

ANSWER: TSA has already issued security measures through the appropriate security programs and other regulatory documents that outline supply chain security measures relative to the Certified Cargo Screening Program. These measures include the use of tamper-evident technology (TET) and other chain of custody processes. TSA continues to test and evaluate TET, and will issue further operational requirements as appropriate.

TSA has completed the issuance of standards for the performance segment of the requirement.

Question: The same GAO testimony notes that TSA plans to test and evaluate tamper-proof technology but has not done so yet. What is your time table to do so?

ANSWER: TSA has already issued security measures through the appropriate security programs and other regulatory documents that outline supply chain security measures relative to the Certified Cargo Screening

Program. These measures include the use of tamper-evident technology (TET) and other chain of custody processes. TSA continues to test and evaluate TET, and will issue further operational requirements as appropriate.

Question: Without this type of testing, evaluation and follow-on guidance, in the interim, how are we assured that the methods third party screeners are using once physical screening has been completed and the package/pallet is sealed, is adequate to prevent tampering of air cargo later on and that the cargo is effectively secured?

ANSWER: The Transportation Security Administration (TSA) continues to test and evaluate tamper-evident technology (TET), and further operational requirements will be issued as requirements are finalized.

Question: How will you handle this cargo carried on passenger aircraft coming from overseas into the United States? Will and where will it be screened? What percent of all air cargo does this represent?

ANSWER: TSA has revised its security programs to accomplish system-wide screening for international inbound cargo. TSA will continue to evaluate revisions to its security programs to improve the screening of cargo imported into the United States.

TSA has submitted a paper to the United Nation's International Civil Aviation Organization (ICAO) that proposes integrating supply chain security standards into ICAO's standards and recommended practices (SARPs). ICAO accepted the proposal in April 2009, and will be issuing amendments to the Annex 17 standards on securing air cargo that would introduce the supply chain security concepts. TSA is also working under bilateral and quadrilateral arrangements with a number of countries to introduce the supply chain approach to securing air cargo into their programs and regulations.

Additionally, TSA is actively exploring the use of the Customs and Border Protection's (CBP's) Automated Targeting System (ATS) to assess risk on inbound passenger air cargo based on information provided by aircraft operators. TSA is proposing an enhancement to the system to perform an evaluation of risk for explosives in cargo shipments. If the tool is found to be effective TSA will work with CBP to have the information supplied early enough to assure that risk evaluations could be done prior to a flight's departure.

The Transportation Security Administration is working towards 100 percent screening of passenger air cargo abroad before it is uploaded for transport to the United States. Efforts towards this goal include working with foreign partners to introduce air cargo screening and security concepts across the entire supply chain system. According to calendar year 2007 Bureau of Transportation Statistics data, international inbound passenger air cargo represents approximately 44 percent of the total U.S. air cargo received for passenger aircraft.

Question: Are other countries seeking reciprocal agreements to scan U.S. cargo being carried on passenger aircraft overseas?

ANSWER: Currently, no other countries are seeking reciprocal agreements to screen cargo originating in the United States.

Question: Reaching 100 percent screening requirements is a mandate that I believe TSA can meet but it will be a challenge within the timeframes that Congress has set, particularly as it relates to cargo coming from overseas.

Is the best way forward to screen cargo overseas or should we assume that most cargo heading to our shores will be screened here?

ANSWER: TSA's layered approach to securing inbound air cargo is focused on working with our foreign partners to implement security measures abroad before cargo travels to the United States. TSA is focused on keeping items off the aircraft before it departs.

Question: What are the biggest challenges to meeting the 100 percent screening requirement by August 2010?

ANSWER: Meeting the screening requirements with respect to inbound air cargo from foreign countries presents unique challenges. Sovereignty issues make it difficult to impose U.S. regulations on foreign nations with diverse air cargo security regimes without seriously impeding the flow of commerce. TSA's assessment of the risks associated with the international environment indicates that the risks vary by location and demography and are compounded by the fact that security practices vary with the foreign location.

TSA has the legal authority to require that a given percentage of inbound cargo be screened before it reaches the United States, but the physical space at foreign airports is often constrained. Moreover, screening is regulated by the almost 100 foreign countries that transport cargo into the United States and each country has its own screening requirements.

Question: What progress has TSA made in coordinating with the U.S. Customs and Border Protection (CBP) to enhance the security of air cargo transported into the United States?

ANSWER: TSA is actively exploring the use of Customs and Border Protection's (CBP) proven Automated Targeting System (ATS) to assess risk on inbound freight. ATS is a proven system for evaluating certain risks associated with inbound cargo based on information provided by aircraft operators. TSA is proposing an enhancement to the system to perform an evaluation of risk for explosives in cargo shipments before shipments are uplifted on passenger aircraft.

To date, CBP representatives have provided an initial briefing on CBP's air cargo targeting capabilities and the two agencies are engaged in a series of next steps to advance the pilot, including plans to maintain a TSA liaison at the National Targeting Center-Cargo.

Question: What is the status of TSA's efforts to develop and implement technology to inspect air cargo? As part of this response, please identify what technology is being used now to screen air cargo and what is under development that may be used to meet the 100 percent screening mandate.

ANSWER: Explosives Detection Systems (EDS), Explosives Trace Detection (ETD) and Advanced Technology X-ray Systems (ATs) are currently being used by air carriers and certified screening facilities to screen cargo. Advanced ETD, larger aperture higher speed metal detectors, and other detection and imaging technologies are among the additional technologies being developed or under evaluation. TSA published an approved technology list that includes seven EDS machines, six ETD machines, and eleven AT machines.

Question: Recent GAO testimony indicates that while TSA has done a preliminary assessment of air cargo screening technologies, it has not yet completed laboratory or operational testing of these technologies in the air cargo environment. Frankly, the lack of laboratory testing surprises me. Why was this not done prior to TSA

providing air cargo screening participants with a list of acceptable technologies that they could procure? When do you expect to complete laboratory testing?

ANSWER: The initial list of approved technology included equipment that was laboratory and field tested in air cargo sites and facilities over the past several years. TSA's Office of Security Technology (OST) and the DHS Science and Technology (S&T) Directorate have conducted lab testing of all equipment on the TSA Air Cargo Screening Technology List. This list was first published for industry in April 2008.

TSA's OST and the DHS S&T Directorate continue to conduct qualification and field testing. New technologies will be added to the approved technology list as they are tested and approved. In addition, based on further lab and field evaluations, these technologies will be added to a Qualified Technology List as quickly as possible.

Question: As I understand the current air cargo screening pilot program, TSA will be evaluating what technologies are effective in screening air cargo before finalizing the requirements. This evaluation must be completed well before TSA is required to meet the 100-percent mandate. What is your current timetable to evaluate these technologies and, at this time, when do you expect to have a finalized list that entities can use?

ANSWER: TSA's Office of Security Technology (OST) and the DHS S&T Directorate continue to conduct qualification and field testing. New technologies will continually be considered and added to the Qualified Technology List upon approval.

TSA published an initial Qualified Technology List in April 2008 and as more technologies are approved, these items will be added.

Question: When do you expect to have a technology that has been evaluated at the laboratory and tested in an operational setting that can screen larger sized air cargo pieces, such as pallets or skids?

ANSWER: There are three larger apertures, skid-level technologies to which TSA has given provisional approval until at least August 2010 and are being used for operational testing in the field. Seven skid-level screening systems from four vendors have been selected for laboratory and field qualification testing beginning in mid-July 2009.

Question: Does TSA have any plans to continue to use the San Francisco air cargo test facility that was utilized as part of a S&T cargo pilot? For example, could this facility be used as a test bed to evaluate new air cargo technologies or other advanced technologies to screen bags for explosives?

ANSWER: TSA does not currently have any plans to continue using the test facility in San Francisco. TSA is currently utilizing the new TSA System Integration Facility located at Reagan National Airport for the majority of qualification/laboratory testing and other designated labs as necessary. Operational testing will occur at designated field test sites based on predetermined criteria for site selection.

Question: How many air cargo inspectors do you have currently on-board? How many positions are vacant? What is your plan to fill the vacant positions?

ANSWER: As of May 20, 2009, there are 516 Air Cargo Inspectors on-board.

TSA is authorized 535 Cargo Inspector Full-Time Positions. As of May 20, 2009 TSA is in the process of filling 19 vacancies.

TSA anticipates filling the two Explosive Detection Canine Handler positions shortly. Candidates for these positions were interviewed in early April. TSA is currently working through the offer process.

TSA is working diligently to fill the remaining 17 traditional cargo inspector positions by posting job listings both internally and externally, as well as actively recruiting applicants from both the public and private sectors.

Question: TSA has stated it may not have enough transportation security inspectors to conduct compliance reviews once the air cargo mandate is fully implemented in August 2010. On average, how many reviews do you believe are necessary each year? How many inspectors will that take? Does your 2010 budget request sufficient staffing levels to get you there?

ANSWER: TSA believes that frequent, quality inspections, coupled with outreach and deliberate enforcement actions, are needed to properly execute our mission. We believe that, at a minimum, at least one comprehensive inspection a year for each regulated entity is needed to verify compliance with current security requirements. In addition we believe that regular targeted inspections of critical security areas and practical testing are vital in promoting compliance. Per national guidance, we encourage Cargo Inspectors to inspect a regulated entity at least once every six months.

The current staffing allocation of 535 Cargo Inspectors is sufficient to monitor current mandates.

TSA believes the current workforce is sufficient to monitor compliance with current air cargo mandates, therefore the FY 2010 Budget Request does not include additional inspectors above the current authorized amount.

Question: The DHS Inspector General recently issued a report on TSA's known shipper program that concluded that TSA's testing and inspection activities did not provide assurances that regulated entities were complying with the program's vetting requirements. While the report acknowledges that TSA has made progress in improving the known shipper program by developing a known shipper management system. The agency has not resolved technical problems and policy issues, which have hindered its use as the primary method for establishing and verifying known shippers. What is TSA doing to resolve these problems? As part of this answer, please include a proposed timeline to fix the problems and outline any associated costs.

ANSWER: The Known Shipper Management System (KSMS) has undergone significant improvements since the Inspector General audit. These improvements have resolved policy issues regarding response times and accuracy. KSMS full functionality is planned for September 2009 with an estimate of \$500,000 to complete the enhancements.

Question: The same IG report notes that the criteria and guidance used to make shippers "known" are unclear and subject to interpretation. This increases the risk that shippers may be improperly vetted and therefore, unknown. What is the agency doing to resolve this problem? Will this be completed prior to August 2010?

ANSWER: TSA issued new program guidance, effective February 2009, which clarified the known shipper vetting process using the manual and automated systems. The program clarifications issued by the TSA, effective February 2009, have resolved this issue.

Question: With TSA's new air cargo regulation, TSA will be doing 100,000 more background checks, specifically on cargo employees who screen cargo and/or have knowledge of how it is going to be transported or actually transport the cargo. The rule requires more robust checks and more visibility on the shipping companies and their employees. What type of background checks are you doing? Is it similar to the checks being done for transportation workers in the ports? How quickly does this check take?

ANSWER: TSA is currently conducting name-based checks for the Certified Cargo Screening Program (CCSP) pilots. When the Interim Final Rule for the CCSP is issued, TSA will conduct an estimated 540,000 background checks in the first year against federal terrorism, law enforcement and immigration databases.

Transportation Worker Identification Credential (TWIC) background checks are similar but more extensive than those performed for air cargo. TWIC security threat assessments also include a fingerprint-based criminal history records check against the Integrated Automated Fingerprint Identification System maintained by the Federal Bureau of Investigation and a more comprehensive immigration check through the Citizenship and Immigration Service's Systematic Alien Verification of Entitlements-Verification Identity System to verify that the applicant meets a specific eligible immigration category listed in the TWIC rule.

Results for the name-based security threat assessments for the air cargo program are typically returned within 72 hours.

Question: The budget blueprint includes \$64 million to modernize the infrastructure to vet travelers and workers. Is this funding necessary to handle vetting of employees that will handle air cargo under the certified cargo shipper program? If so, what specific improvements must you do to include this class of people?

ANSWER: The \$64 million that TSA requests in FY 2010 for infrastructure modernization will benefit air cargo; however, it does not include specific enhancements to support the Certified Cargo Screener Program (CCSP). CCSP-specific enhancements will be funded by a combination of air cargo appropriations and user fees.

TSA does not anticipate funding improvements for this specific program through the \$64 million requested for infrastructure modernization. The Certified Cargo Screener Program will benefit from an improved infrastructure for more robust and reliable vetting system performance, enhanced customer service technology and functions, and economies of scale through shared costs and person-centric vetting capabilities.

Checkpoint Technologies

Question: Congress has appropriated a significant amount of funding to DHS and TSA for the research, development, test and evaluation, and deployment of checkpoint screening technologies since 9/11. Yet, only a few new technologies have been deployed to airports during that time. What are the primary factors that have contributed to this limited progress in deploying new technologies and what can be done to expedite these efforts?

ANSWER: Prior to deployment of a new technology, TSA must ensure that the equipment actually operates and performs to TSA standards. TSA has been testing and deploying new technology to the checkpoints. To date, approximately 775 Advanced Technology X-ray systems (ATs) have been deployed. Deployment of the remaining systems is anticipated to be completed by the end of Summer 2009. Currently, there are ongoing acquisitions that will complete the replacement of legacy systems with ATs. Additionally, Whole Body Imager technologies are being evaluated for deployment.

TSA maintains ongoing communication with the security technology industry to exchange information on our developing and evolving requirements. While new threats cannot always be anticipated, enhanced effectiveness of current state-of-the-art technologies continues to be foremost among the layers of security that TSA has focused its time, attention and funding.

Question: Given the significant investments DHS and TSA have made in research, development, and deployment in new screening technologies to detect explosives and other threat items on passengers and their carry-on items, how effectively are the new technologies working in the airports?

ANSWER: Screening technologies are a valuable part of TSA's arsenal in conducting security screening at airports nationwide. When utilized in conjunction with operational processes and procedures that our Transportation Security Officers implement daily, these technologies increase the ability to ensure that threat items do not enter sterile areas in airports or onboard aircraft. TSA uses a variety of assessments to determine the effectiveness and focus resources on system-wide improvements.

Question: Last summer, Assistant Secretary Hawley announced that the public would soon be able to fly with liquids greater than 3 fluid ounces in their carry-on bags. The Europeans are clamoring for this change. However, the Subcommittee is hearing from the business community that TSA has recently decided that this problem cannot be easily resolved. What is the status of this initiative? Will this change be imminent, meaning will we be able to carry large liquids soon? When will TSA begin testing technologies that better detect threat liquids? What are the challenges and obstacles that you face to make this change?

ANSWER: The ability to do away with 3-1-1 rests with the successful implementation of Liquid Algorithm technology on Advanced Technology X-ray units. The two vendors are Rapiscan and Smiths. Rapiscan recently went through initial testing and those results are forthcoming. Smiths indicated its second round of testing began on or about May 4, 2009, for a period of 60 days.

Development and testing of this technology is ongoing. At the present time, it is unlikely this technology will be deployed before the first quarter of calendar year 2010.

TSA's liquid threat detection strategy is predicated upon a systems approach. To that end, TSA is currently testing Next Generation Bottled Liquid Scanners and Advanced Technology X-ray Systems to improve upon TSA's current liquid threat detection capabilities. This requirement is included in the solicitation for any vendor's technology that intends to be selected by TSA for deployment. TSA expects to retrofit existing equipment to the same standard.

At present, known technologies for liquid detection do not provide TSA with all of the required capabilities that would allow TSA to make changes to the current liquid restrictions (i.e. the 3-1-1 policy). TSA is working diligently with both Next Generation Bottled Liquid Scanners and Advanced Technology X-ray Systems

vendors to make the necessary improvements to current technologies to overcome this hurdle, thereby permitting TSA to relax, if not eliminate, the liquid carry-on restrictions.

Question: What is the status of the Advanced Checkpoint Technology system proposals that will contain additional enhanced detection capabilities? TSA had informed the Committee that it planned to award new contracts for these technologies in the summer of 2009. Is this still on track? If not, please explain the delay.

ANSWER: The new Advanced Technology X-ray Systems (ATs) Procurement Specification incorporates liquid threat detection of the ATs as a mandatory requirement. Vendors are in the process of submitting ATs to TSA to undergo testing of these requirements in a lab and operational environment. An award will be made based on TSA's established operational effectiveness and suitability requirements that all technologies will be evaluated against. Other factors, such as life-cycle cost and overall benefit to TSA's missions, will also be considered.

Contract awards for enhanced Advanced Checkpoint Technology equipment are dependent upon successful completion of laboratory and operational testing. This testing is expected to be completed by the end of June 2009 and will enable awards to be made as originally scheduled during Summer of 2009.

Question: Does TSA plan to deploy Advanced Checkpoint Technology systems nationwide? If so, how long will that take?

ANSWER: Yes, the Transportation Security Administration has a comprehensive national deployment plan for Advanced Technology X-ray Systems replacing legacy TRX systems

Full Advanced Technology X-ray Systems deployment is estimated to be complete by the end of calendar year 2010.

Question: TSA has been testing whole-body imagers at airports for quite a while now. Does this system continue to be controversial with passengers as the press suggests? On average, what percentage of travelers are opting for the full body imaging instead of the pat down when presented with two options?

ANSWER: There has always been some controversy with the Whole Body Imagers with some members of the traveling public. However, the majority of feedback that TSA has received has been positive due to the increase in security and the ability to screen passengers with pacemakers and other implanted medical devices without requiring a pat-down search.

During the initial deployment of Whole Body Imagers (WBI), TSA has experienced an average passenger acceptance rate of 93 percent in the Post Walk Through Metal Detector configuration (As a Secondary Screening Device). Based on the current deployment of Primary Screening WBI units, passenger acceptance rates are now above 99 percent (99.72 percent).

Question: Similarly, what is the current status of the Whole Body Imager program? Last year, TSA was testing a number of systems using difficult airport configurations (primary, secondary, etc). How do you plan on using WBIs now? Do you plan to buy from vendors that produce different types of WBIs? Will these systems be only installed at primary screening checkpoints?

ANSWER: Currently, Whole Body Imager (WBI) technology is being used for primary screening pilots at six airports and for secondary (that is, random) continuous screening protocol (as an alternative to a pat-down) at 13 airports. Overall, a total of 40 systems have been deployed. A solicitation for WBIs is currently underway. There are a variety of different vendors who have responded to the request for proposal with different technology solutions. Interested vendors have begun submitting the Qualification Data Packages (QDPs) to the Transportation Security Lab (TSL) to determine if their systems meet the Transportation Security Administration's specifications. Vendors with systems that pass the QDP evaluation will be requested to submit systems to the TSL to determine safety and field readiness.

The current strategy is to continue to evaluate Whole Body Imagers in a primary and secondary position at the checkpoint, as established in the most recent field assessments.

Under the current solicitation for Whole Body Imagers, those vendors that pass laboratory and field testing and satisfy privacy, operational feasibility, safety, and security requirements will be placed on a Qualified Products List. These vendors will then be able to compete for awards at the delivery order level, which may result in procurements from more than one vendor.

TSA is piloting Whole Body Imager technology in a primary configuration at six airports and will continue to consider operations, staffing, and passenger flow to optimize the use of the technology.

Question: Do you plan on using the Whole Body Imager as a primary screening tool in place of the walk through metal detector?

ANSWER: The current deployment strategy under evaluation is a Whole Body Imager unit co-located with a walk through metal detector in a primary position that allows for increased security without affecting overall passenger throughput. This provides a systems approach to screening, which is a facet of the Transportation Security Administration's layered security approach.

Question: Last fall, despite Subcommittee concerns, TSA stopped collecting wait time data at all airports. At that time, Mr. Hawley said that he would begin using a credentialing technology that could, among things, measure a passenger's wait time at security checkpoints. Is this credential authentication technology in use yet? If not, what is the planned deployment schedule?

ANSWER: The Credential Authentication System (CAT) is scheduled for deployment this summer and will be used to verify the validity of passenger IDs and boarding passes. However, further analysis required TSA to reassess the use of this technology to measure wait times. The length of passenger queues is dynamic and not always contained within the sanctioned off areas. Measuring wait times with stationary scanners would result in collecting inaccurate wait time data. Opting for a 'mobile' scanner to follow the end of the line as it varies in length would take Transportation Security Officers away from their 'critical mission' to handle administrative duties.

As a result, TSA is pursuing a fully automated system. TSA issued a Request for Proposal on March 23, 2009, and anticipates technical proposals by May 4, 2009. We will then begin evaluation of proposals to include laboratory and OT&E testing. It is our intention to conclude our evaluation of written technical proposals by June 22, 2009. We anticipate an award by September 2009. TSA has also collaborated with Customs and Border Protection and Transport Canada on the wait time effort. These latter two agencies have worked jointly as part of the Model Ports Initiative to automate wait time data collection along the border as well as within Immigration and Customs Enforcement facilities at the nation's airports. The demonstrations of the available

technologies as well as pilots at the Transportation Systems Integrated Facility will allow TSA to draft a Request for Procurement with the goal of having a fully automated system in place by the first half of 2010.

Question: The stimulus provided \$1 billion for aviation security technologies. TSA plans to spend \$300 million of this funding on next generation checkpoint technologies. How and when will TSA spend these funds?

ANSWER: TSA's Passenger Screening Program (PSP) will expend approximately \$300 million of the \$1 billion allocated to Aviation Security per the American Recovery and Reinvestment Act Spend Plan that was submitted to Congress on April 3, 2009. PSP will use the Recovery Act funding to accelerate its planned deployment schedule for new equipment by more than three years and strengthen the program's ability to meet its objectives and achieve the following benefits:

- Enhanced detection capability;
- Improved checkpoint efficiency; and
- Preserved passenger privacy and dignity.

Specifically, PSP will deploy the following enhanced checkpoint screening equipment: Advanced Technology X-ray Systems, Next Generation Bottled Liquid Scanners, Whole Body Imager technology, and Next-Generation Explosive Trace Detectors. Contract awards for these technologies are expected to proceed through the remaining months of fiscal year 2009.

Explosive Detection Systems (EDS)

Question: How are you going to prioritize the application of \$700 million in economic recovery funding? For example, how much of these funds will be devoted to upgrading airport baggage systems and how much will be spent on terminal modifications?

ANSWER: In accordance with its American Recovery and Reinvestment Act expenditure plan that was submitted to Congress on April 3, 2009, TSA is continuing the process from FY 2009 and carrying it forward for FY 2010. That process relies upon airports to apply for funding for their projects. The applications received are evaluated for completeness and compliance with the Planning Guidelines and Design Standards. A combination of threat, application scoring, and airport readiness continues to be used to prioritize airport projects funded with the economic recovery funding. TSA gives higher priority to airport projects that can commence quickly in order to meet the goals of the economic recovery program.

The economic recovery funding is being applied for the implementation of new baggage handling systems. Upgrades on current operational in-line systems are not being considered for this funding.

Approximately \$600 million will be allocated to fund the TSA share of terminal modification project costs for in-line baggage handling systems. The funding will facilitate the facility modification to install in-line systems, which will improve security and expedite the baggage handling process.

Question: Earlier this year, TSA informed the Subcommittee 24 percent of the top 82 airports had optimal screening systems throughout the entire airport (and another 41 percent have optimal screening systems in some part of the airport). With the large influx of funding in 2009, can you give us an estimate of how many of

the top 82 airports will have optimal baggage systems throughout the entire airport following our appropriation of almost \$1.25 billion?

ANSWER: With the 2009 and American Reinvestment and Recovery Act funding, the Transportation Security Administration will fund an additional 19 Projects at Category X and I airports. Upon completion of the projects, a total of 61 airports or 74 percent will have at least one optimal system. In addition, 27 airports or 33 percent will have the entire airport configured for optimal baggage systems.

Question: Time and time again, this Committee has been told that in-line baggage screening systems hold huge advantages in terms of increased efficiency and accuracy and dramatically reduce TSA personnel requirements. Unfortunately, cumbersome and inefficient in-lobby EDS systems remain in place, including at some of the busiest airports in the country. Of the largest airports (Category X and Is), how many have optimal systems in place now, assuming this figure has changed since the 24 was reported earlier? When do you plan on having optimal systems in place at all of the Category X and I airports?

ANSWER: By the end of FY 2009, we anticipate 54 CAT X and I airports will have optimal systems installed and operational at some screening areas.

Current Transportation Security Administration projections indicate completion of optimal solutions at CAT X through III will be completed no later than 2023. Please note that these projections are dependent upon funding levels and airport submittals of applications for funding.

Question: What plans to you have in place for getting in-line systems into those and other facilities across the country that lack an in-line solution?

ANSWER: TSA continues to employ its fiscal year request process to identify airports that are ready to accept and apply funding to in-line baggage projects. TSA is moving to a continuous, rolling application process that will enable us to identify airports as early as possible in the planning process. Furthermore, TSA continues to strengthen its outreach program with the aviation industry, particularly to high-priority airports that have yet to apply for program funding. The optimal solution is not always an in-line system, but it does always include the use of certified automated explosives detection systems.

Question: Consistent with the 9/11 Act, does TSA now plan to consistently request Letters of Intent? If so, will they be for more than a two year period? Or does TSA plan to continue to predominately utilize yearly other transactional agreements (OTAs)? In the long run, aren't OTAs more costly for airports that have large projects than an LOI?

ANSWER: Yes, the Transportation Security Administration intends to comply with the law.

With the economic recovery funding and the FY 2010 Budget Request, there is a substantial infusion of capital into airport projects. TSA expects a mix of two-year Letters of Intent and yearly Other Transaction Agreements to be an effective funding strategy.

TSA uses Other Transaction Agreements (OTAs) to fund useable segments of projects, typically individual terminal projects. The large influx of funding provided by the American Recovery and Reinvestment Act has

enabled TSA to fully fund large projects at airports minimizing the cost impact of delayed project execution. Therefore, Letters of Intent (LOIs) do not appear to provide a more cost-effective solution.

Question: In assessing the needs of airports throughout the country that receive the latest security technology I recognize that your decision-making process involves (1) a top-down approach using the Electronic Baggage Screening Program (EBSP) Strategic Plan, and (2) a reverse approach using requests from airport Federal Security Directors. Once prioritized, these requests are included in the EBSP Spending Plan by fiscal year, based on the availability of funds. How often does TSA reassess the Electronic Baggage Screening Program Spending Plan, and does one of these one of these approaches carry more weight than another?

ANSWER: As required by law, TSA reassesses and adjusts the Electronic Baggage Screening Program Expenditure Plan on a quarterly basis.

Airports that submit complete application packages in compliance with Planning Guidelines and Design Standards are scored higher for readiness to apply the funding. However, TSA uses both the top-down threat-based prioritization and funding application scoring on an approximately equal basis when prioritizing airport projects.

Question: How many airports still use ETD for primary screening of checked baggage?

ANSWER: In all airport size categories, there are currently 265 Explosives Trace Detection-only airports.

Maintenance and Utility Costs for Screening Technologies

Question: What is the status of the report requested in FY 2009 on maintenance and utility costs for screening technologies? As part of this report, TSA was to identify ways that these costs could be controlled in the future. When do you estimate we will receive this report? If it has been transmitted, please summarize your findings for the Committee.

ANSWER: A draft of the Screening Technology Maintenance and Utilities report was cleared by the Office of Management and Budget on May 19, 2009; it will be transmitted to Congress in the very near future.

TSA anticipates that a final report will be ready for delivery to Congress during the third quarter of fiscal year 2009.

Question: What is the average maintenance cost for each screening technology?

ANSWER: The FY 2010 average unit maintenance cost for each Security Screening Technology is provided below. Because of partial year maintenance requirements due to warranty coverage for new equipment, extension of unit prices and equipment counts will not equal estimates reflected in the FY 2010 Budget Request. "TBD" manufacturers represent unit cost estimates for equipment that has not been procured.

Equipment	Average Unit Maintenance Cost
EDS	
CTX-2500	\$80,204
CTX-5500	\$90,939
CTX-9000 Series	\$105,320
e6000 Series	\$112,575
Reduced Size	\$55,820
ETD	
IonScan 400B	\$11,393
Itemiser-W	\$10,496
Next Generation	\$2,279
EMD	
Ceia	\$651
Metorex	\$852
Garrett	\$746
EMD-2	\$247
TRX	
Rapiscan	\$13,059
Smiths	\$11,306
AT Systems	
Smiths/ Rapiscan	\$10,880
WBI	
L-3	\$7,915
Universal Conveyor Systems	
TBD	\$10,625
Bottle Liquid Scanners (BLS/ILD)	
TBD	\$754
Cast & Prosthesis Imagers	
Spectrum	\$10,350
Standoff Detection	
QinetiQ	\$12,974
Credential Authentication Technology	
TBD	\$1,387
Shoe Scanners	
TBD	\$3,213

Question: What is the average utility cost for each screening technology? How do the older EDS compare to the newer EDS?

ANSWER: Utility costs vary widely by region, and costs for each screening technology vary by number of hours the machine is used. The table below provides average kilowatt hour usage by equipment type, and uses the December 2008 Energy Information Administration average cost of 9.64 cents per kilowatt hour for all sectors and regions. The daily usage assumes an average 20 hour operating day.

The energy usage for older versus newer Explosive Detection Systems (EDS) does not vary significantly by age, as the technologies employed are similar. Differences in energy usage are largely dependent on the size and throughput volume of the machine.

	Equipment	Average Power (KW)	Hours per day of operation	KWH/Day	Cost per KWH (\$)	Cost per day (\$)
EDS	InVision CTX-2500	2.1	20	42	0.0964	4.05
	InVision CTX-5500	3	20	60	0.0964	5.78
	InVision CTX-9000 Series	9.7	20	194	0.0964	18.70
	L3 eXaminer	5.5	20	110	0.0964	10.60
	CT-80	2.1	20	42	0.0964	4.05
ETD	Smiths Detection Ionscan (Barringer)	0.3	20	6	0.0964	0.58
	Thermo Detection EGIS II	1.725	20	35	0.0964	3.33
	Ion Track Itemiser (GE)	0.345	20	7	0.0964	0.67
ETP	EntryScan3e (GE)	1.2	20	24	0.0964	2.31
	Smith	5.2	20	104	0.0964	10.03
X-Ray Equipment:	AT -Smiths 6040aTix	1.219	20	24	0.0964	2.35
	AT -Rapiscan 620DV	1	20	20	0.0964	1.93
	Smiths Series	0.575	20	12	0.0964	1.11
	Rapiscan Series	1.15	20	23	0.0964	2.22
WBI	L-3	0.3	20		0.0964	0.61
WTMD	CEIA 02PN20	0.04	20	1	0.0964	0.08
	Metorex 200D	0.04	20	1	0.0964	0.08
	Garrett 6500i EMD	0.035	20	1	0.0964	0.07

Transportation Security Officers

Question: Recently, TSA has brought back the random gate security checks implemented after September 11, 2001 that disappeared in 2003. This policy means that TSA officers will randomly select flights to re-screen passengers just before they board the aircraft. Airport travelers are mostly grumbling about TSA airport screeners adding another layer to their daily security routine. Why does TSA feel it is necessary to bring back this 2001 policy? Is it based on threat, intelligence, or the importance of unpredictability?

ANSWER: In 2001, gate screening activities focused on the identification and collection of prohibited items. Now, screening beyond the checkpoint is a critical layer in TSA's risk-based, flexible, and unpredictable model of security. Security activities at the gate add unpredictability to the screening process, making it more difficult for a terrorist to anticipate screening procedures and adapt to them. It also helps to reduce insider threat vulnerabilities. TSA identifies and targets flights for screening based on a risk model and includes a random component to ensure unpredictability.

Question: To date, all we have heard is that these specialized screeners have caught some convicts and immigration violators, which is not the primary responsibility of TSA. How do you measure the effectiveness of these costly positions and the tradeoffs from losing entry level screening positions?

ANSWER: While TSA uses Transportation Security Officers (TSOs) to perform multiple security functions such as gate screening, there are no specialized positions performing this function. TSOs, including entry-level officers, are trained in checkpoint screening procedures as well as screening functions away from the checkpoint and utilized to perform these screening activities. Furthermore, positions such as Behavioral Detection Officers are career progression positions and do not replace the need for entry-level screening positions. There is no requirement for a TSO to be "specialized" to perform these functions.

Question: How is TSA determining the effectiveness of the Behavioral Detection Officers program, Travel Document Checkers, the Aviation Direct Access Screening Program, and Visible Intermodal Protection and Response Teams?

ANSWER: TSA currently monitors the effectiveness of the Screening of Passengers by Observation Technique (SPOT) program through the SPOT database. The SPOT Program office also conducts regular assist and standardization visits at each airport with a SPOT Behavior Detection Officer (BDO) Trainer to evaluate its procedures, methodology, reporting, and training effectiveness. When necessary, the SPOT Program conducts site visits to review specific issues that have come to light during which the SPOT Program's procedures, methodology, reporting, training and effectiveness will be assessed.

The SPOT Program Office is working with DHS on an independent review with the American Institutes of Research to conduct 1) a controlled SPOT Base Rate Data Collection study which will allow TSA to compare BDO accuracy with a random screening protocol; 2) an operational analysis which will show correlations of behavior indicators to security outcomes and the statistical weights of those behaviors; and 3) a study in which BDOs observe videos of passengers to identify SPOT behaviors in order for TSA to assess the reliability of BDOs. The SPOT Program Office is also working with DHS to perform a BDO Effectiveness and Selection study.

The Travel Document Checker (TDC) is a screening function performed as part of the standard checkpoint screening procedures. The TDCs have both initial and recurrent training relating to fraudulent document identification and detection. TSA currently monitors the effectiveness of TDC procedures through the TDC database. The database records all Law Enforcement Officer referrals and arrests. As of April 2009, more than 5,000 TDC referrals have been made to Law Enforcement Officers, resulting in approximately 500 arrests, all resulting from the TDC process.

TSA is currently expanding its security operations beyond the checkpoint by incorporating Aviation Direct Access Screening Program (ADASP) operations with additional security measures that can be implemented by the Federal Security Director (FSD) at each airport. This new initiative, called Playbook, will allow each FSD to alter the placement and scheduling of security measures in unpredictable ways to address specific vulnerabilities and threats, including those posed by persons who seek access to non-public areas of the airport. The Playbook Program Manager tracks the metrics for this program to determine the frequency and unpredictability of security measures implemented nationwide.

TSA receives After Action Reports regarding every Visible Intermodal Prevention and Response (VIPR) deployment that are used to refine and improve future operations. These reports often include feedback from other federal, state and local security partners that provide useful information on the effectiveness of TSA collaboration in the planning and execution of VIPR operations, as well as our security partners' views of the

value of VIPR deployments. TSA believes that these assessments are an important component to assess the effectiveness of VIPR operations. These assessments also aid in developing strong interagency contacts that are helpful in coordinating future VIPR operations. TSA measures the success of the VIPR program by seeking feedback from federal, state and local security, law enforcement and transportation officials after each VIPR deployment.

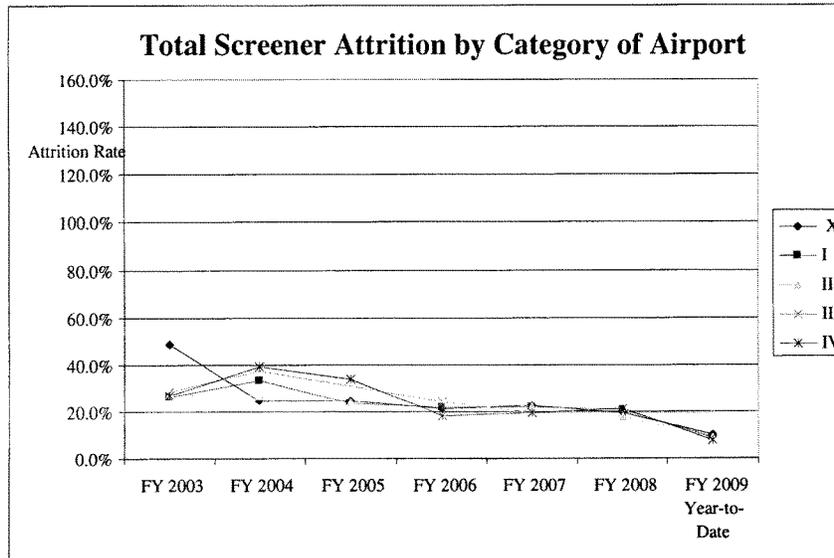
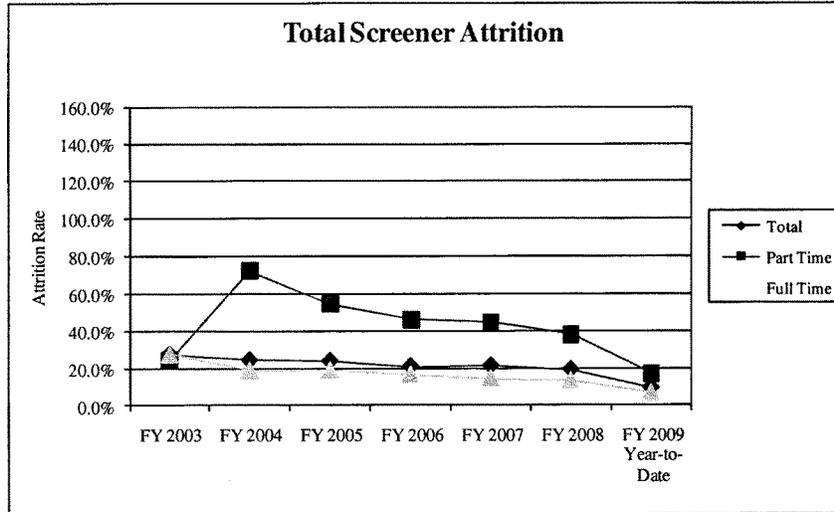
Question: Historically, TSA faced challenges in hiring TSOs to meet its staffing needs at passenger screening checkpoints and checked baggage screening stations. TSA implemented local hiring in 2006, which was supposed to make hiring easier. Has it? As part of this response, please compare your attrition rates for both full and part-time screeners on an annual basis from 2003 onwards. Also, please compare rates by airport categories (Cat X, I, II, III and IV).

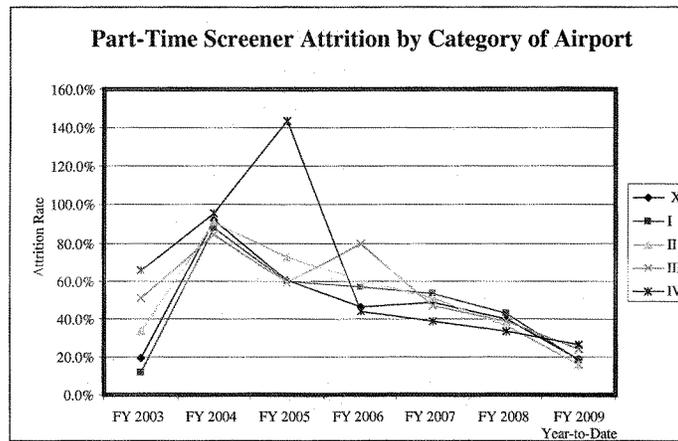
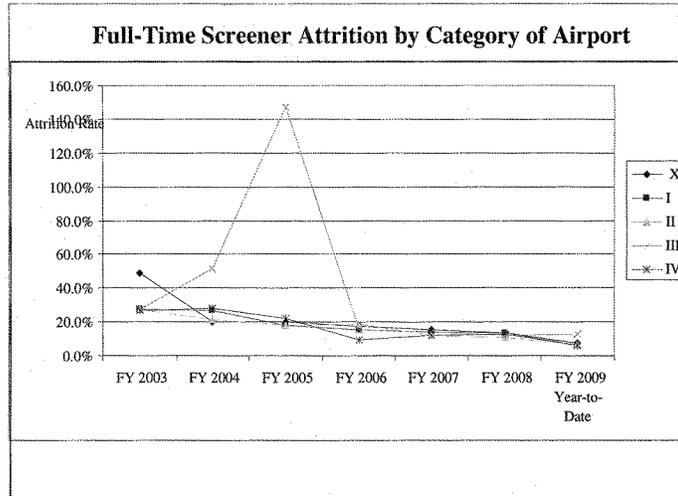
ANSWER: Yes. In March 2006, TSA instituted local hiring to ensure quicker hiring and closer alignment of candidate expectations with on-the-ground realities.

Prior to implementing local hiring, TSA hired approximately 180-200 Transportation Security Officers (TSOs) per pay period at approximately 20 airports nationwide. With the implementation of local hiring in 2006, new hires increased to 11,781 TSOs, an average of 452 per pay period. In calendar year 2007, TSA hired 12,730 TSOs, an average of 488 per pay period. Also, local hiring increased TSA's capacity to hire TSOs at more airports – 90 to 100 airports every pay period. In January 2008, TSA hired over 1,000 TSOs in one pay period.

In addition, with local hiring, TSA reduced the time it took to hire a TSO. Early in the local hiring process, the mean time to hire a TSO was 157 days. By early 2008, the mean time to hire dropped to 104 days.

As a result of these changes, TSA now maintains hiring levels within a few percentage points of the number required by the staffing allocation model. In addition, TSA's attrition rate for its screening workforce has steadily decreased.





Question: What impact, if any, do you believe the slowing economy has had on your ability to attract and retain screeners and other transportation security officers that specialize in certain areas (e.g bomb appraisal)?

ANSWER: No data is currently available to answer this question. Surveys indicate that employee satisfaction has improved over time.

Question: What is the current screener staffing FTE level? Do you expect to maintain this FTE through the end of FY 2009? What level of screener staffing do you project for FY 2010? For this response, please include separate and distinct figures for screeners, lead screeners, supervisory screeners, bomb appraisal officers, travel document checkers, behavior detection screeners, and ADASPs.

ANSWER: The current screener staffing level is 44,300 Full-Time Equivalents. Staffing levels are expected to remain flat through the end of FY 2009.

TSA is currently engaged in the FY 2010 staffing allocation model process and is analyzing the impact of industry changes, passenger travel projections, and advancements in technology to staffing requirements. FY 2010 staffing level estimates are as follows:

TSO Budgeted FTE by Job title

Job title	FY10 FTE
TSOs	31,192
Lead TSOs	5,490
Supervisory TSOs	4,360
BDOs	3,204
BAOs	352
Managers	1,100
TOTAL	45,698

TSO FTE Allocated to Security Duties

Job Duty	FY10 FTE
TDC	2,001
ADASP	1,654
BDOs	3,204
BAO	352
Checkpoint / Other	38,487
TOTAL	45,698

Aviation Regulation and Other Enforcement

Question: Please provide the number of inspectors on-board under aviation regulation and other enforcement for fiscal years 2005 through 2008, and planned for in 2009 and 2010.

ANSWER: Please see the following chart for a tabular explanation of Transportation Security Inspector (TSI) staffing levels and notations.

	Full Time Permanent Positions					
	On Board				Planned	
	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010
TSI - Aviation Domestic	776	681	657	778	778	755
TSI - Aviation Int'l	49	49	45	45	45	45
Total, Aviation Inspectors	825	730	702	823	823	800
TSI - Int'l Repair Stations	0	0	13	13	15	15

*Fiscal Year 2010 Full-Time Equivalent allocations have not yet been authorized by Congress. In FY 2009, the Transportation Security Administration converted 23 canine handlers to Federal Air Marshals.

Question: Please update the Committee on hiring of inspectors for foreign and domestic repair stations. How many are on-board now?

ANSWER: The Repair Station staffing levels are provided in the chart below.

	Domestic	Foreign
Repair Stations Authorized	2	15
Repair Stations On - Board	2	11

Security at Foreign Repair Stations

Question: The TSA and FAA are now over four years delinquent in establishing new security regulations for repair stations, and in conducting an audit of foreign repair stations, though the agencies were tasked with this under the Vision 100: Century of Aviation Reauthorization Act of 2003, and subsequently the 9/11 Commission Act of 2007. It appears that there is currently little collaboration between the TSA and FAA to ensure that repair stations are audited and are maintaining the highest level of security. What are the two agencies doing to correct this lapse in the oversight? When do you anticipate the new security regulation will be issued?

ANSWER: TSA has established the Aircraft Repair Station Program (ARSP) office to develop, execute and sustain an aircraft repair station regulatory program that will oversee implementation of security regulations and conduct security audits as required by the statute.

TSA continues to execute its domestic and foreign voluntary repair station outreach efforts. TSA is conducting voluntary outreach visits at foreign repair stations. The outreach visits have provided TSA with valuable information on current security conditions and best practices at repair stations. A total of 154 voluntary foreign repair station outreach actions have been completed. With respect to domestic locations, TSA continues its domestic outreach effort through its national Transportation Security Inspection workforce and completed a Special Emphasis Inspection of approximately 600 repair stations located on TSA-regulated airports in 2008.

As part of the outreach effort, TSA developed a "best practices" document to share with repair station owners and operators. The best practices document is provided as a tool to assist the repair station owner/operator in assessing security vulnerabilities. It is important to note that the document is used to provide a possible listing of effective and reasonable security enhancements at domestic and foreign repair stations and not as a preview of the pending security regulations.

TSA maintains a close working relationship with the Federal Aviation Administration (FAA) and monitors FAA repair station policy guidelines. TSA is continuing to strengthen its relationship with the FAA Flight Standards and International Field Offices and has established a partnership with the FAA to conduct joint TSA/FAA foreign repair station visits. Recently, the first TSA/FAA joint foreign repair station visit was conducted in Central America. In addition, TSA recently coordinated with the FAA to develop and disseminate "Information Paper – FAA Procedures for Certifying/Reviewing Part 145 Repair Stations Located outside the United States and Its Territories."

A Notice of Proposed Rulemaking (NPRM) is currently being reviewed within DHS. After publication of the NPRM in the Federal Register, there will be an opportunity for public comment. TSA will analyze and respond to the comments before issuing the final rule.

Question: Airlines continue to increase the volume of aircraft maintenance work being performed overseas. For the 11 years ending in 2007, U.S. airlines outsourcing-related maintenance expenses increased from 37 percent to 64 percent; the number of foreign FAA-certificated repair facilities has grown from 344 to 704 over a comparable period of time. In addition, the IG reported that the FAA has not maintained a list of non-certified repair stations both at home and abroad that U.S. airline and their code share and alliance partners continue to use. What are the TSA's plans for ensuring that those facilities are in compliance with U.S. standards in order to protect passengers? How is the TSA going to ensure the security of foreign repair stations that are not even certified by the FAA?

ANSWER: TSA's statutory mandate [USC 44924(f)] is to develop regulations for Federal Aviation Administration (FAA) Part 145 certified repair station facilities. It should be noted that non-FAA certificated facilities do not perform maintenance on US- registered aircraft or components. Since the statute does not address non-certificated FAA facilities, TSA has not included such facilities in its proposed regulations. U.S. registered aircraft are required to use FAA certificated repair stations.

Federal Flight Deck Officer and Flight Crew Training

Question: Please provide a table that breaks out the fiscal year 2010 budget request for federal flight deck officer and flight crew training by these two categories. As part of this response, please distinguish how much of the federal flight deck officer training is for new and how much is for recurring training. For comparison purposes, this table should show both fiscal year 2009 enacted and the fiscal year 2010 request.

ANSWER: Please see the chart that follows.

Federal Flight Deck Officer and Flight Crew Training PPA		
Summary		
Program	FY 2009 Enacted	FY 2010 Request
Federal Flight Deck Officer Program	\$21,784,114	\$21,936,462
Crew Member Self Defense Training Program	\$3,240,886	\$3,190,538
Total Funding	\$25,025,000	\$25,127,000
Federal Flight Deck Officer Program (FFDO)		

	FY 2009 Enacted*	FY 2010 Request**
Payroll	\$4,108,063	\$4,190,224
Program Administration Costs	\$6,408,117	\$6,141,786
Initial "New" Training	\$2,235,353	\$959,028
Recurring Training	\$10,032,581	\$12,145,424
Total Funding	\$22,784,114	\$23,436,462
Crew Member Self Defense Training Program (CMSD)		
	FY 2009 Enacted*	FY 2010 Request**
Payroll	\$0	\$0
Program Administration Costs	\$812,097	\$505,450
Crew Member Self Defense Training	\$1,428,789	\$1,185,088
Total Funding	\$2,240,886	\$1,690,538
* FY2009 Enacted amounts include the \$1M transfer of CMSD funds to FFDO, a one-time transfer of funds.		
**FY2010 Request amounts include the \$1.5M transfer of CMSD funds to FFDO, a permanent transfer of funds.		

Secure Flight

Question: It is my understanding that the Secure Flight is operational but to a limited degree. For the record, please highlight the status of the Secure Flight program. As part of the response, please indicate what carriers are currently participating in the program and when you believe the first large air carrier will begin participating.

ANSWER: Secure Flight is currently deployed to four airlines. For security reasons, the identity of those carriers is not being publicly released. The first large carrier is scheduled to begin participating in the program in August 2009.

Question: When will the system be fully operational for domestic watch list matching? For international watch list matching functions? Do you believe your schedule is realistic, given the program's past history?

ANSWER: It is anticipated that Secure Flight will be performing watch list matching for all covered domestic aircraft operators near the end of March 2010, and near the end of calendar year 2010 for all covered foreign aircraft operators.

The Secure Flight schedule is realistic. A number of carriers submitted comments on the proposed Secure Flight rule noting that they would need additional time to make system changes to support the integration of Secure Flight. As a result, when published in late October 2008, the final rule allowed this additional time, and the program developed a schedule that allowed initial capability for carriers to voluntarily implement Secure Flight as early as January 2009. The remaining carriers will implement the program throughout 2009, assuming their system changes are made in time to meet their scheduled implementation timeline.

Question: In a January 29, 2009 letter from the Government Accountability Office regarding its longstanding review of the Secure Flight program, GAO noted that while TSA has made significant progress in developing

the Secure Flight program, key activities needed to be completed to fully satisfy the statutory conditions and minimize operational risks. These key points included "executing performance and stress tests in accordance with recently developed plans and procedures and report any limitations in the scope of the test performed and shortfalls in meeting requirements to the DHS Investment Review Board; and completing all relevant security testing, update, and complete security documents, certify and accredit Release 3, ensure that U.S. Customs and Border Protection has implemented adequate security controls over its devices that interface with Secure Flight, and mitigate all open high- and moderate-risk vulnerabilities from Release 1 and any new high- and moderate-risk vulnerabilities from Release 3 of the Secure flight system. What are you doing to address these remaining concerns? Please provide an answer for each concern separately.

ANSWER: Between January 29, 2009, and April 10, 2009, TSA provided additional information and documentation to the Government Accountability Office (GAO) verifying that all performance and stress tests were accomplished in accordance with recently developed plans and procedures and appropriately reported the following: All relevant security testing was completed, Release 3 had been certified and accredited, and U.S. Customs and Border Protection had implemented adequate security controls over its devices that interface with Secure Flight; and all open high- and moderate-risk vulnerabilities from Release 1 and any new high and moderate-risk vulnerabilities from Release 3 of the Secure flight system had been mitigated. As a result, GAO advised TSA on April 13, 2009, that the Secure Flight program has generally achieved these statutory conditions and minimized operational risks. TSA concurred with this updated GAO assessment on April 23, 2009.

Question: TSA was in the process of hiring adjudicators to work on Secure Flight "hits" when a passengers name is run through the program. In total, how many adjudicators did you plan to hire tin 2009? What is the status of filling those positions? For fiscal year 2010, do you plan to hire additional adjudicators? If so, how many and at what cost?

ANSWER: Secure Flight plans to have the following staffing levels in 2009. Some of these positions have already been filled or are in the process of being filled.

Position	FTE Count	Amount (Millions)
Analysts and Analyst Managers (Government)	35	\$4.2
Analysis (Contractor)	50	\$6.5
TOTAL	88	\$10.7

All contractor position hiring is currently on schedule. Of the government positions, 18 of the 35 positions have been hired, and 11 are in the process of being filled. TSA has posted announcements for the remaining positions and applications are being processed.

No additional contractor or government adjudicator positions are anticipated in FY 2010.

Screening of Aviation Workers

Question: The fiscal year 2008 Act appropriated \$15 million for TSA to conduct airport employee screening pilots at seven airports for no less than 90 days. At three of the seven airports, all employees were to be screened. At the remaining four airports, TSA could use other more random screening methods (e.g. physical inspections, biometric access control, camera, and training) to enhance whatever level of airport employee screening was currently being utilized. TSA ran this pilot program from May until August 8, 2008. In October

2008, the Subcommittee staff was briefed on the pilots' preliminary results. At that briefing, TSA told us that there was no clear distinction between the number of inappropriate items found at 100 percent employee screening vs. random screening airports. Both forms of screening caused employees to modify their behavior by reducing the number of trips they made between secure and unsecured areas of the airport; additionally, they reported the 100 percent screening did not significantly disrupt daily operations. TSA was to complete a final report on this pilot to include the cost estimates for 100 percent employee screening and further analysis of this pilot. We have not received it yet. Why has it taken so long for TSA to finalize the report on the 100 percent airport employee screening pilot? When can we expect to see it?

ANSWER: The employee screening pilots ran from May-July 2008. Following the completion of the pilots, TSA hired the Homeland Security Institute (HSI) to begin a comprehensive analysis of the pilots. HSI was challenged by the amount of data that had to be analyzed and evaluated in order to determine the effectiveness of the two pilot types, and to provide a cost analysis for 100 percent employee screening at approximately 455 airports.

HSI provided a preliminary report to TSA in September 2008, and the final report with cost estimates and recommendations was provided in December 2008. TSA reviewed and analyzed the report in order to formulate the agency's position, opinion, and recommendations; taking into consideration the cost implications, effective use of resources, and overall security benefit. TSA completed its analysis of the HSI report in late January 2009.

A draft of the Airport Employee Screening Pilot Program Study report is currently undergoing edits by TSA to clarify the document following comments by the Office of Management and Budget (OMB) as a part of the Administration level clearance. After OMB approval of the draft report, it will be transmitted to Congress. The Transportation Security Administration anticipates that a final report will be ready for delivery to Congress during the third quarter of FY 2009.

Question: Does TSA continue to oppose the 100 percent physical screening of airport employees? What are your concerns with mandated physical screening of airport workers?

ANSWER: TSA believes that physical screening of employees is a critical component of the airport security solution. TSA is focused on security solutions that address all of the vulnerabilities associated with airport operations. Security solutions are created by significantly enhancing layers of security which complement each other. A draft report on this issue is currently undergoing Administration-level review and should be delivered to the Appropriations Committee in the near future. However, an independent analysis of TSA's airport worker screening pilot verified that 100 percent worker screening did not yield statistically significant detection of prohibited items and, from a risk and cost perspective, would not be an effective use of resources.

While physical employee screening plays an important role in airport security, it is one element of the larger layered security strategy. TSA recommends comprehensive security solutions that offer greater operational flexibility and increased deterrence/detection capability.

Question: Just last week at a major airports conference, I was told that 100 percent screening of airport employees would significantly disrupt airport operations even though preliminary results from the pilot found differently. Do you agree?

ANSWER: While the 100 percent screening pilots may not have demonstrated any significant disruptions during their short tenure, it is important to note that those pilots were conducted at three airports for a period of

90 days. The impact would likely be quite different across the network due to physical layout and environmental conditions.

Question: Beyond this pilot program, what are you doing to proactively address the “inside threat” at airports? Are you working collaboratively with airports to address this issue?

ANSWER: TSA continues to work proactively in collaboration with airports and the airline industry. TSA’s current activities focus on designing means and methods to implement biometric identification credentials in the commercial airport environment, identify and implement improved technologies and methods of screening for the presence of prohibited items, and conducting security threat assessments on airport workers. Background checks enable TSA to distinguish those who have previously disclosed an intent to do harm from those who have not, and screening enables TSA to detect and neutralize means of doing harm. Collectively, these three layers of security significantly mitigate the risk associated with possible insider threats in commercial aviation.

In 2008, TSA introduced strategies to vary where, when, and how security resources and energies are used to apply unpredictability to the layers of security and thereby prevent terrorists from identifying patterns in an effort to circumvent the system. TSA has continued making risk-based security adjustments at commercial airports through the use of Visible Intermodal Prevention and Response teams and the Screening of Passengers by Observation Techniques program.

TSA continues to work collaboratively with airports and other aviation security partners, such as airlines, the airport consulting community, law enforcement, and others, to address security risks that may be posed by insiders and others that may affect transportation security by acting at or upon commercial airports.

Air Crew Screening

Question: The 9/11 Act required TSA to move expeditiously on a security screening process for flight crews. TSA completed a report to Congress on the status of efforts to “institute a sterile area access system” last year and planned to pilot test this screening process. Please update the Committee on your efforts. What is the status of the expedited screening system to check the identity of airline crew members as required by the 9/11 Act?

ANSWER: TSA has met with our industry security partners on a number of occasions and continues to support the existing pilot programs based on the Crew Personnel Advanced Screening System (CrewPASS) concept with its real time employment verification through a live link to airline employee databases. CrewPASS involves 82 aircraft operators evaluated at three airports - Baltimore/Washington International Thurgood Marshall Airport (BWI), Pittsburgh International Airport, and Columbia Metropolitan Airport.

The original pilot program included flight deck crew who were part of the Cockpit Access Security System (CASS) and ran from July 17, 2008, to September 17, 2008. TSA approved a 180-day extension that ended March 17, 2009, and upon receipt of a request from the Air Line Pilots Association for an additional extension, TSA extended the pilot program, which is now scheduled to end on July 17, 2009. The CrewPASS pilot program has been authorized by TSA to incorporate a biometric at the three locations during the extension period and also allowed the inclusion of a technical solution to add flight attendants.

TSA authorized a second pilot to test the biometric technology of an expedited access system called SecureScreen. The pilot program was tested at BWI and all participants were Southwest Airlines flight deck crewmembers. The pilot ended on November 24, 2008, since the biometric technology that was being tested worked as designed.

As a result of the two pilots, TSA has concluded that it would authorize a pilot program expansion if the pilot proponent(s) incorporate further specifications into any expedited crew access system to address remaining security vulnerabilities identified by TSA. The program standards are in the final phase of clearance at TSA and will be released to interested security partners.

9/11 Act Expenditure Plan:

Question: The expenditure plan to implement recommendations of the 9/11 Act includes funding for general aviation security. Does any of this funding relate to the pending rule on the large aircraft security program? If not, please detail how these funds will be used.

ANSWER: None of the 9/11 Act funding supports the Large Aircraft Security Program (LASP). Once the regulation is final, LASP will be largely supported by fees. The FY 2009 DHS Appropriations Act (P.L. 110-329) included \$20 million for TSA to continue to implement recommendations of the Implementing Recommendations of the 9/11 Commission Act of 2007. The money was allocated to support general aviation (GA) security initiatives, and the upgrade of the Automatic Detection and Processing Terminal (ADAPT) system. TSA will also focus on enhancing rail and transit security through expanded vulnerability and threat assessments, additional security exercises with rail and transit providers, hiring additional surface transportation security inspectors, and reimbursing costs of the existing public transit Information Sharing and Analysis Center. Additionally, TSA will expand its Intermodal Security Training and Exercise Program.

Question: Please explain to the Committee what the ADAPT system is that you are using 9/11 funding for. My understanding is that this is an FAA system that is being transferred to TSA. What is the system's purpose? Why is TSA taking over this system instead of retaining it in FAA?

ANSWER: The Automatic Detection and Processing Terminal (ADAPT) program, developed by the Federal Aviation Administration (FAA), correlates information from Air Traffic Control radar feeds, security-related databases, and other relevant sources. ADAPT provides advance warning to security personnel by allowing individuals to validate the identity, movement, and potential threat of aircraft operating to, from, within, and transiting the National Airspace System. The FAA has enhanced the ADAPT program to meet TSA requirements for a cost significantly less than needed for full program development.

The Automatic Detection and Processing Terminal (ADAPT) program is not being transferred to the Transportation Security Administration (TSA), but is being enhanced to meet TSA's needs. ADAPT has the capability to correlate large amounts of information to graphically display and track all aviation traffic in "real time." This feature dramatically increases TSA's ability to identify potential aircraft tracks of interest and subsequently improves the ability to respond and mitigate security concerns. ADAPT has the ability to capture "returns" from a variety of targets which are typically filtered out by existing Federal Aviation Administration (FAA) Air Traffic Control systems and the majority of Commercial Off The Shelf products.

Although TSA is not taking over the program, TSA has funded program modifications to enhance security situational awareness. This joint effort with the FAA has been codified using an Interagency Agreement and a Memorandum of Agreement. Under this agreement, FAA retains program management of the Automatic Detection and Processing Terminal and will continue to provide enhancements, modification, upgrades, routine maintenance and sustainment, while TSA will oversee policy decisions with respect to security enhancements of the program.

School Bus Security Assessments

Question: Public and private sector school transportation organizations have indicated an interest in working together with TSA on a security assessment, but little progress has been made to date. What is the status of TSA's plans to conduct a professional threat assessment of the school bus industry?

ANSWER: The Implementing Recommendations of the 9/11 Commission Act of 2007 required the Department of Homeland Security to provide Congress with "a comprehensive assessment of the risk of a terrorist attack on the nation's school bus transportation system." A draft report of the School Bus Security Risk Assessment has been completed and is currently undergoing executive level clearance within TSA. TSA continues to assess the risk of terrorist attacks on school buses, including the nature of that risk in the context of risks to other modes of transportation.

Transportation Security Support

Question: Please provide a chart showing the FTEs and amounts requested for each office within Transportation Security Support, including Administrator, Internal Affairs, Chief Counsel, Finance and Administration, Legislative Affairs, Acquisition, Special Counselor, Communications, Human Capital, and Operational Processes and Technology. This chart should include actual funding levels and FTEs in both fiscal year 2007 through 2009, as well as planned for in 2010. Also, as part of this response, please provide a brief mission statement for each office.

ANSWER: The TSA Headquarters Administration Program Project Activity (PPA) in the Transportation Security Support Appropriation provides funding for Headquarters offices as depicted in the following table.

Office	FY 2007 (Actual)			FY 2008 (Actual)			FY 2009 (Enacted)			FY 2010 (President's Request)		
	FTE	PC&B	Non-PC&B	FTE	PC&B	Non-PC&B	FTE	PC&B	Non-PC&B	FTE	PC&B	Non-PC&B
Assistant Secretary	13	1.9	0.8	18	1.8	1.0	12	1.7	0.9	13	1.7	0.1
Deputy Assistant	18	2.6	4.8	32	3.2	2.4	32	2.3	1.5	23	3.1	1.5
Inspection	177	28.2	4.4	173	29.9	4.6	199	33.2	5.1	202	35.2	5.3
Chief Counsel	194	29.3	2.2	187	32.0	2.3	197	33.9	0.8	202	32.6	2.5
Finance &	162	21.4	70.7	175	21.4	52.9	176	23.2	51.5	186	24.0	58.6
Legislative Affairs	8	0.9	0.3	8	1.0	0.1	8	0.9	0.1	9	1.0	0.1
Acquisition	117	13.8	4.1	124	13.6	7.9	125	14.8	8.0	134	14.0	9.1
Special Counselor	92	10.8	12.5	92	11.0	10.3	95	11.7	11.3	123	15.2	9.2
Strategic												
Communications &	26	3.5	0.3	28	4.1	2.5	28	4.4	1.7	29	3.8	1.7
Human Capital	166	24.2	11.8	171	23.3	8.9	204	27.1	186.0	208	27.9	194.5
Security Operations	49	5.8	1.6	52	6.5	1.0	-	-	-	-	-	-
Operational Process & Technology	190	27.4	1.3	191	27.1	1.1	-	-	-	-	-	-
Office of Law Enforcement (for background)	1	0.1	20.9	1	0.2	21.5	6	0.8	26.7	14	1.7	28.2
Total	1,213	169.9	135.7	1,252	175.10	116.50	1,082	154.0	293.6	1,143	160.2	310.8
												471.0

Note: Funding for Security Operations, and Operational Process & Technology were realigned to other PPAs in the Aviation Security Appropriation. Funding for the Office of Human Capital was realigned from Aviation Security to the Transportation Security Support Appropriation.

Mission Statements are as follows:

- **Assistant Secretary**

The Assistant Secretary's Office provides strategic direction, policy guidance, and external representation of the Transportation Security Administration.

- **Deputy Assistant Secretary**

The Office of the Deputy Assistant Secretary manages the day to day operations of the agency.

- **Inspection**

The Office of Inspection identifies vulnerabilities in security systems through operational testing; ensures the effectiveness and efficiency of the TSA's operations and administrative activities through inspections and internal reviews; and ensures the integrity of TSA's workforce through impartial and comprehensive special investigations.

- **Chief Counsel**

The Office of Chief Counsel provides legal advice and services to all TSA mission areas and operational components. The Office of the Chief Counsel is comprised of attorneys and staff at the Headquarters and at our Nation's airports.

- **Finance & Administration**

The Office of Finance and Administration is responsible for providing TSA with essential administrative, revenue, budget, and financial services to support the program responsibilities of TSA.

- **Legislative Affairs**

The Office of Legislative Affairs (OLA) develops and implements strategies within the agency to achieve congressional approval or authorization of the agency's programs and policies, furthering the agency's mission of protecting the nation's transportation network. OLA acts as the principal liaison between the agency and Congress, with the primary responsibility of providing timely, accurate information about the agency, its programs, and its policies. Through professionalism and customer service, OLA seeks to cultivate relationships thereby developing trust, confidence, and friendship with our colleagues in Congress, enabling the free flow of information between the two bodies.

- **Acquisition**

The Office of Acquisition provides mission-focused acquisition and contract services to support TSA. The Office of Acquisition primarily functions as the business advisor and consultant for the planning, award and management of TSA's acquisition program. As such, the Office of Acquisition partners with program offices to provide TSA with critical services and technology through contracts and other business agreements. The Office of Acquisition builds sound business judgment into mission solutions, and ensures the wise stewardship of taxpayer dollars while securing public trust.

- **Special Counselor**

The Office of the Special Counselor is dedicated to delivering quality information to TSA's stakeholders, both internal and external, and ensures that employees and the traveling public are treated in a fair and lawful manner, consistent with federal laws and regulations governing privacy, information sharing, redress, civil rights and civil liberties.

- **Strategic Communications and Public Affairs**

The Office of Strategic Communications and Public Affairs serves as the Agency's buttress in protecting the Nation's transportation systems by providing full and appropriate information about the implementation of policies and security measures. The office also fosters broad public understanding of the methods and impact of transportation security to promote effectiveness and contribute to TSA's commitment to customer service.

- **Human Capital**

The Office of Human Capital (OHC) develops and manages best practice, results-oriented programs that ensure that TSA's human capital strategy and services support TSA's mission, goals and objectives, achieves alignment with the DHS Chief Human Capital Officer (CHCO) goals, and facilitates the management and improvement of employee and organizational performance. Additionally, OHC develops the human capital policy agenda, establishes priorities, monitors progress, and coordinates and evaluates results related to all policy development for senior leadership approval. OHC also serves as TSA's representative on DHS CHCO Council and coordinates TSA membership on Departmental working groups.

- **Office of Law Enforcement**

The Office of Law Enforcement administers the funds for background investigations and physical security. Personnel Security schedules and adjudicates background investigations and grants security clearances to TSA employees and contractors. Physical security ensures the safety of all TSA employees and guests at all TSA facilities, including the Headquarters buildings.

Reception and Representation

Question: How does TSA plans to utilize its reception and representation expenses in 2010? To date, how much has been spent in 2009 and what is the plan for the remainder of the fiscal year?

ANSWER: TSA plans to use the Reception and Representation funds for meals and entertainment to host foreign dignitaries and senior officials, and international industry representatives. TSA will also host several conferences with our international partners such as the QUAD (U.S., Canada, Australian, and the European Union), International Civil Aviation Association, International Working Group on Land Transportation Security, and New and Emerging Threats Working Group.

As of April 22, 2009, TSA has spent \$8,296. The balance of the funds will be used for the meeting of the International Working Group on Land Transportation Security to be hosted by the Transportation Security Administration.

Bonuses:

Question: Please provide a table showing how much is requested in the 2010 budget for bonuses for TSA political employees, TSA SES employees, and TSA non-SES employees.

ANSWER: The Transportation Security Administration does not predetermine the budget for bonuses. Bonuses are provided to employees based on their performance and the availability of funds.

Travel

Question: Please provide for the record a table that shows all funds expended by TSA political employees travel in 2008. Include name of individual traveling, purpose of travel, location(s) visited, and total cost.

ANSWER: Please see the following table.

Traveler Name	Purpose of Travel	Location visited	Trip Cost
Edmund Hawley	CONFERENCE ATTENDANCE	MONTERREY, CA	1,621.76
	CONFERENCE ATTENDANCE	BRUSSELS, BEL	3,178.61
	SITE VISIT	HOUSTON, TX	990.01
		SALT LAKE CITY, UT;	
	CONFERENCE ATTENDANCE	DENVER, CO	1,803.39
	CONFERENCE ATTENDANCE	NEW YORK, NY	466.63
	CONFERENCE ATTENDANCE	OTTAWA, CAN	1,214.79
	CONFERENCE ATTENDANCE	ST LOUIS, MO	717.88
		BRUSSELS, BEL; PARIS, FRA	
	CONFERENCE ATTENDANCE		3,040.02
		DALLAX, TX; SAN ANTONIO, NM	
	CONFERENCE ATTENDANCE		971.17
		LONDON, ENG; GLASGOW, SCO	
	CONFERENCE ATTENDANCE		3,693.76
	CONFERENCE ATTENDANCE	ATLANTA, GA	600.38
		AMMAN, JOR; BERLIN, FRG; ROME, ITA; TEL AVIV, ISR; VIENNA, AUT; WARSAW, POL	
	CONFERENCE ATTENDANCE		9,110.89
		BOSTON, MA; DENVER, CO; SEATTLE, WA	
	CONFERENCE ATTENDANCE		2,344.75
	CONFERENCE ATTENDANCE	ST. LOUIS, MO	976.88
	OTTAWA, CAN; NEW YORK, NY; PITTSBURGH, PA		
CONFERENCE ATTENDANCE		3,054.20	
	BALTIMORE, MD; PHILADELPHIA, PA		
CONFERENCE ATTENDANCE		703.13	
	LOS ANGELES, CA; SAN FRANCISCO, CA		
CONFERENCE ATTENDANCE		1,942.75	
OFF-SITE	CAMBRIDGE, MD	567.09	
CONFERENCE ATTENDANCE	ORLANDO, FL	389.00	
	SAN FRANCISCO, CA; NEW YORK, NY		
CONFERENCE ATTENDANCE		2,345.86	
	TOTAL		39,732.95

Traveler Name	Purpose of Travel	Location visited	Trip Cost
Ellen Howe	SITE VISIT	DALLAS, TX	3,196.78
	SITE VISIT	SAN ANTONIO, TX	1,598.39
	SITE VISIT	SAN FRANCISCO, CA	1,507.43
	INFORMATION MEETING	MANHATTAN, NY	1,300.13
	TRAINING	MANHATTAN, NY	760.00
	SPEECH OR PRESENTATION	MANHATTAN, NY	694.99
	SITE VISIT	BOSTON, MA	653.63
	CONFERENCE ATTENDANCE	OTTAWA, CAN	1,799.97
	INTERNATIONAL TRAVEL	LONDON,GBR	3,931.39
	SITE VISIT	MANHATTAN,NY	390.63
	SPEECH OR PRESENTATION	NEW ORLEANS,LA	1,143.70
	SPEECH OR PRESENTATION	MANHATTAN, NY	701.68
	SPECIAL MISSION TRAVEL	CHICAGO, IL; DENVER, CO; SEATTLE, WA	2,039.65
	SPEECH OR PRESENTATION	MANHATTAN,NY	539.91
	TOTAL	20,258.28	
Rebekah Williams	CONFERENCE ATTENDANCE	LONDON, ENG; GLASGOW, SCO	5,188.11
	CONFERENCE ATTENDANCE	PHOENIX, AZ	761.50
	CONFERENCE ATTENDANCE	BIRMINGHAM, AL	770.54
	CONFERENCE ATTENDANCE	BRUSSELS, BEL	3,333.26
	CONFERENCE ATTENDANCE	BRUSSELS, BEL; PARIS, FRA	2,876.24
	CONFERENCE ATTENDANCE	CHARLSTON, SC	1,174.03
	CONFERENCE ATTENDANCE	AMMAN, JOR; BERLIN, FRG; ROME, ITA; TEL AVIV, ISR; VIENNA, AUT; WARSAW, POL	8,825.97
	CONFERENCE ATTENDANCE	LONDON, ENG; GLASGOW, SCO	5,174.11
	OFF-SITE	CAMBRIDGE, MD	436.54
	CONFERENCE ATTENDANCE	OTTAWA,CAN	1,199.29
	CONFERENCE ATTENDANCE	SAN FRANCISCO, CA	2,578.87
	CONFERENCE ATTENDANCE	SALT LAKE CITY, UT; DENVER, CO	2,199.44
	CONFERENCE ATTENDANCE	TEL AVIV, ISR	3,574.90
	CONFERENCE ATTENDANCE	MANHATTAN, NY	1,379.30
	CONFERENCE ATTENDANCE	MEMPHIS, TN	296.55
	CONFERENCE ATTENDANCE	DALLAS, TX	987.58
	TOTAL	40,756.23	

Unobligated Balances

Question: Please provide unobligated balances within TSA, by appropriation account, and when you anticipate that they will be expended.

ANSWER: As of January 31, 2009, TSA's unobligated funds for all appropriations, including fee accounts, is as follows:

Appropriation	\$M
Aviation Security ¹	3,951.2
Surface Transportation Security	57.2
Transportation Threat Assessment & Credentialing	150.8
Transportation Security Support	702.5
Federal Air Marshals	542.7
Research and Development	6.7

¹ Aviation Security includes \$250 million in mandatory fees for Aviation Security Capital Fund and payroll for over 45,000 Transportation Security Officer FTE. The amount above does not include the \$1 billion received in the American Recovery and Reinvestment Act in February 2009.

TSA expects to obligate most of these funds in FY 2009.

QUESTIONS FOR THE RECORD SUBMITTED BY

THE HONORABLE HAROLD ROGERS

**Gale Rossides, Acting Administrator,
Transportation Security Administration**
Improving the Efficiency of the Aviation Security System

Secure Flight

Question: As noted within the TSA Acting Administrator's testimony, the Secure Flight system is currently only working with smaller airlines as it ramps up operations, but expects to begin working with one of the larger airlines in May. Does TSA expect to face any technical challenges as it begins incorporating the large amounts of data from the larger airlines? Please also address all of the challenges that could possibly impede TSA from fully deploying the system to all carriers, domestic and international, by the end of 2010.

ANSWER: Recent stress testing of the Secure Flight system showed that it can properly and robustly handle the forecast volume of traffic even if one of the two Secure Flight data centers is offline. Additionally, the Secure Flight system design allows for easy addition of capacity should our analysis or experiences indicate that it is warranted. Otherwise, current and future technical challenges include: (1) potential delay in DHS Router upgrades that are a prerequisite for future airline deployments, and (2) potential delays with aircraft operators or their technology service providers to make necessary programming changes for Secure Flight. The Secure Flight program is working aggressively in these two areas to mitigate any potential impact, and is generally experiencing good cooperation from those parties involved.

Large Aircraft Security Program

Question: Many general aviation groups and Members of Congress have raised serious concerns about the Large Aircraft Security Program (LASP), noting that TSA is not recognizing the inherent differences that exist between private and commercial aviation. They claim that LASP is an unreasonably expansive response to an undocumented and unproven security threat and argue that TSA selected the 12,500 lb weight threshold without providing a data-driven, risk-based analysis. Please address what methods TSA relied upon for the selection of the weight threshold.

ANSWER: TSA analyzed risk factors such as range, carrying capabilities, and fuel loads of General Aviation (GA) aircraft. Due to these increased capabilities, risk factors and the greater level of sophistication of large aircraft operators, TSA determined in the Notice of Proposed Rulemaking (NPRM) that aircraft with a Maximum Takeoff Weight (MTOW) of over 12,500 pounds is the appropriate balance between security and burden to the industry. Additionally, the Federal Aviation Administration's long-standing definition of "large aircraft" is an aircraft with a MTOW of over 12,500 pounds.

In addition, TSA is analyzing comments received from the public and working with our security partners to reassess various elements of the NPRM, including the weight threshold, to ensure that the most appropriate weight was selected.

QUESTIONS FOR THE RECORD SUBMITTED BY

THE HONORABLE JOHN ABNEY CULBERSON

Gale Rossides, Acting Administrator,
Transportation Security Administration
Improving the Efficiency of the Aviation Security System

Canadian Bag Rescreening

Question: I want to raise an issue as a placeholder for further discussion and possible action -- rescreening of bags from Canada. As I understand it, an airline passenger and their luggage can depart a Canadian airport after having been screened. When that passenger gets to a connecting U.S. city, like Houston, they can proceed to their next gate, but their bags must be rescreened. This rescreening appears to be a waste of government resources since TSA inspectors are used for the rescreening. Additionally, it is a waste of airline resources because the number of misconnected bags -- and costs associated with misconnected bags -- is high. Furthermore, passengers whose bags do not make it to their final destination because of this requirement are unhappy with the service provided. If the TSA does not think the bags can be flown safely from the connecting airport to the final destination without rescreening here in the U.S., why are they safe enough to fly from Canada across the U.S. to their first destination? Will the TSA look into this issue and to find a better process without compromising security?

ANSWER: TSA screens checked baggage coming from Canada and transferring to a connecting domestic flight because 49 U.S.C. §44901 of the Aviation and Transportation Security Act, P.L. 107-71 (2001), requires the use of explosives detection systems (EDS) to screen all checked baggage at U.S. airports. By contrast, Canada uses Advanced Technology (AT) equipment as its primary means of screening checked bags. Canadian airports do have EDS equipment, but this equipment is used primarily to screen bags that alarm when screened with AT equipment. Because not all checked baggage in Canada is screened by an EDS machine, TSA rescreens the bags of passengers coming from Canada.

This situation is not unique to flights arriving from Canada. At many foreign airports from which flights into the U.S. depart, checked bags are not screened by EDS equipment.

Yes. Currently, TSA's Office of Security Technology and Office of Global Strategies are working with their counterparts at Transport Canada on this issue. The TSA technology team has a Cooperative Activity Agreement with Transport Canada that facilitates the exchange of technical and testing information. TSA is also exploring the possibility of developing software upgrades for Canada's Advanced Technology equipment which is used in Canada to screen checked baggage. These upgrades would potentially improve the detection capability of this equipment. It should be noted that even with these upgrades, it is not clear at this time whether the Advanced Technology equipment would be the equivalent of the EDS equipment that TSA is required to use. Additional laboratory and operational testing will be performed to determine the comparability of the upgraded Canadian systems with EDS detection capabilities.

QUESTIONS FOR THE RECORD SUBMITTED BY

THE HONORABLE KEN CALVERT

Gale Rossides Acting Administrator, TSA
Improving the Efficiency of the Aviation Security System

ARRA Funding for John Wayne Airport

Comment: As you may know, John Wayne Airport in Orange County, California, located about 20 miles from my congressional district, is one of the facilities that received a "conditional letter" indicating that their new Explosive Detection System project is being considered for TSA funding under the American Recovery and Reinvestment Act. John Wayne Airport is scheduled to meet with TSA staff next week to refine the scope of work for this important project and is very appreciative of TSA's support. Thank you for your assistance on this project.

Biometric Access Controls

Question: TSA and the aviation industry have been discussing the value and viability of biometric access controls for years. A number of airports have been following this discussion closely and are anxious to learn more about when and what biometric regulations TSA will ultimately issue. Can you comment on when airports can expect to know when biometric access controls will be required, what technical specifications will be established and whether TSA will provide funding to support the acquisition, installation and operation of such systems?

ANSWER: TSA encourages the implementation and use of airport biometric access control systems consistent with the Federal Information Processing Standards 201 standards. TSA has encouraged airports to explore biometric access control systems and identity verification technologies that will enhance their ability to reduce unauthorized access and verify user identity. To further this end, TSA posted three documents, the Aviation Credential Interoperability Solution (ACIS) Technical Specifications, ACIS-Biometric Airport Security Identification Consortium Comparison Matrix and the Biometric Definition and Terminology Document for review and comment by the airports and biometric industry. In addition, TSA encouraged airport operators to refer to the RTCA DO 230-B Integrated Security Standards for Airport Access Control document, which was posted on June 25, 2008. This document aggregates industry best practices for use of perimeter security measures, including biometric smart card control points.

Due to the complexity and potential cost of biometric access controls, a rulemaking would likely be required to mandate biometric access control standards. A rulemaking of this nature generally takes at least two years to complete.

Note that TSA normally does not provide funding for access control systems, but airports can apply with the Federal Aviation Administration for Airport Improvement Program grants.

Installation of New Technology at Airports

Question: On the topic of new technology, I was pleased to see that TSA recently installed four new AT X-ray machines at John Wayne Airport. I understand that the transition was smooth, in large measure because the new machines roughly mirrored the old machines in size. Your testimony refers to new technology on the horizon – whole body image scanners, bottled liquid scanners, etc. Would you please comment on how TSA plans to work with airports to facilitate the installation of new technology – particularly in terminals with space-constrained checkpoints – where such installation may require substantial construction and capital?

ANSWER: TSA works directly with security partners to develop designs that are satisfactory to all parties. While the goal is for all the security technologies to be placed in a checkpoint, the reality is that the facility housing the security checkpoint may be very constrained. TSA works closely with airports to determine which combination of equipment is best suited for each checkpoint environment.

Redundancy in TSA Regulatory System

Question: Your testimony refers to Secretary Napolitano's request for a review of security programs and strategies for aviation, surface and maritime modes of transportation. A number of airport operators, like John Wayne Airport, have found some overlap and redundancy between older security programs and directives with those issued more recently. I welcome the Secretary's request for a comprehensive review and hope that the results will be shared, when and where possible, with airport operators and will help to streamline TSA's regulatory system.

ANSWER: While TSA cannot comment on any plans the Secretary may undertake as a result of the review, TSA does anticipate that the Secretary will set security priorities and make decisions based on a thorough evaluation of several factors and priorities, as defined by the Secretary, all of which will drive security program development and allocation of resources.

THURSDAY, MARCH 19, 2009.

BIOMETRIC IDENTIFICATION

WITNESSES

**KATHLEEN KRANINGER, DEPUTY ASSISTANT SECRETARY OF POLICY,
DHS SCREENING COORDINATION OFFICE
BOB MOCNY, DIRECTOR, UNITED STATES VISITOR AND IMMIGRANT
STATUS INDICATOR TECHNOLOGY**

OPENING STATEMENT OF CHAIRMAN PRICE

Mr. PRICE. The Subcommittee will come to order. Good morning. We are going to be discussing this morning biometrics identity management more broadly, continuing our hearings on policy questions and topics of great interest as we look toward writing the Department of Homeland Security's budget.

One of the advantages of this transition period that we are in—there are some disadvantages in terms of not having precise numbers and not having a detailed request of the sort we usually have at this point in the cycle, but one of the advantages is that we can step back a bit and consider some of these broader issues which very definitely have budget implications. So we welcome you this morning for your part in that series.

Recognizing and authenticating a person's identity is part of daily life in business and in government. Recording a person's physical features to authenticate their identity has been done for millennia, beginning with the use of fingerprints, so we are told, in ancient Assyria.

This recording has evolved in modern times to the high-technology of biometrics, automating the collection, management, and authentication of data about personal physical characteristics and storing that information in databases that can be used to identify people.

Supporters of these practices see them as a solution to identify security challenges. Critics view them as a threat to individual privacy.

Our governments use identity databases in several ways. US-VISIT relies on IDENT, one of the largest identity databases in the world, to track foreign individuals as they deal with our immigration services. We have watch lists that identify people for special screening at airports or that bar people from flying altogether.

Several databases are outside of DHS, including the Consolidated Consular Database System at the State Department and the Interstate Data Sharing Network, which we have required states to establish for their driver's license files, under the Real ID program.

Effective use of these databases to confirm or discover personal identities is critical in maintaining our national security, but there are many signs that we are not where we need to be in this regard.

For example, on March 16th, GAO released a report that showed fundamental vulnerabilities in the way our government issues passports. A single investigator obtained four U.S. passports using fraudulent identity documents and was able to travel on those identities.

While weaknesses identified in the report are in the State Department and Postal Service, not DHS, nonetheless, the example is broadly relevant, I think. It proves we need to build vigilance into our system to catch bogus documents and that watch lists and databases must be constantly scrubbed for accuracy.

Now, inclusion of biometrics can be part of the solution, but just bolting it onto our current system and our current practices will no more solve this problem than reroofing a house will solve a termite problem.

Since the 9/11 attacks, the federal government has intensified the use of biometrics in databases to identify terrorists or other individuals of concern. We have also used this practice to confirm the rights and privileges of those who pose no security risk or who may be entitled to special credentials.

The Department of Homeland Security has a principal role in collecting and managing biometric and biographic information on millions of foreign nationals, residents, and citizens in programs used for border and travel security, counterterrorism, immigration control, law enforcement, and infrastructure protection.

DHS incorporates biometrics in a variety of identification documents, particularly for immigration. DHS has at least nine other systems or databases that collect and maintain biometric and biographic records and links to at least five others in other departments.

Identification data, for example, is collected for Trusted Traveler and Safe Shipper programs. It is collected to credential transportation workers and for critical infrastructure protection.

Now, such broadened use of biometrics may seem justified in the post-9/11 world, but that begs the question we expect to discuss here today. We are not trying to give absolute answers here because that is not where we are or where we need to be. We need to use this technology well and responsibly and effectively.

How is the Department using biometric technology today? We need to know, and how can we best use it to secure the homeland while protecting individual privacy rights? We must do both things.

Under this theme, how is DHS working with other agencies to develop standards for biometric and contextual data and to coordinate the collection and management and sharing and control of such records?

Why are there so many different databases? What is DHS doing to ensure that the use of biometric technology improves security in law enforcement or program effectiveness with a minimum duplication of effort?

And, finally, how does DHS protect personal information in its custody and keep this powerful tool from being abused?

The most prominent DHS biometric program is US-VISIT, which collects and verifies fingerprint and facial images for almost all non-U.S. travelers entering this country and, in theory, will someday do the same for their departure.

US-VISIT has evolved into a provider of identity management services for other agencies, for U.S. Immigration and Customs Enforcement, for the Coast Guard, for U.S. Citizenship and Immigration Services, as well as other U.S. Government agencies. In that role, it is working to link its records with those of the Departments of Justice and State and is developing information-sharing agreements with the Department of Defense.

We expect to hear today how US-VISIT is undertaking its mission as custodian for one of the world's largest databases of biometric information. We also expect to hear about plans for the air traveler exit tracking pilots mandated in the Fiscal Year 2009 appropriations bill, as well as any plans for a comprehensive exit strategy.

Clearly, widespread use of biometric technologies to confirm or discover people's identities is here to stay. It is critical, then, that we understand the full range of policy implications, management challenges, and funding issues that such programs entail.

We welcome today, for the first time before this Subcommittee, Kathleen Kraninger, the deputy assistant secretary for screening, and we welcome back Mr. Robert Moczny, the director of US-VISIT.

We have, as I understand, a combined written statement from the two of you, which we will enter in the hearing record, and then we will ask, as we usually do, for each of you to begin with five-minute oral statements, and then we will turn to questions.

Before we do that, let me turn to my colleague, our distinguished Ranking Member, for his comments.

[The information follows:]



COMMITTEE ON APPROPRIATIONS

David Price (D-NC), Chairman, Subcommittee on Homeland Security

FOR RELEASE UPON DELIVERY
Thursday, March 19, 2009

Media Contact: Phil Feagan
202-225-1784

OPENING STATEMENT OF CHAIRMAN DAVID PRICE *Biometrics and Identity Management* *March 19, 2009 / 10:00 am*

Recognizing and authenticating a person's identity is part of daily life in business and in government. Recording a person's physical features to authenticate their identity has been done for millennia, beginning with use of fingerprints in ancient Assyria. This recording has evolved in modern times to the high technology of biometrics – automating collection, management, and authentication of data about personal physical characteristics – and storing that information in databases that can be used to identify people. Supporters of these practices see them as a solution to identity security challenges; critics view them as a threat to individual privacy.

Our governments use identity databases in several ways. US-VISIT relies on IDENT, one of the largest identity databases in the world, to track foreign individuals as they deal with our immigration services. We have watchlists that identify people for special screening at airports, or bar people from flying altogether. Several of these databases are outside of DHS, including the Consolidated Consular Database system at the State Department and the interstate data-sharing network we have required states to establish for their drivers' license files under REAL ID. Effective use of these databases to confirm or discover personal identities is critical

in maintaining our national security, but there are many signs that we are not where we need to be.

For example, on March 16th GAO released a report that showed fundamental vulnerabilities in the way our government issues passports. A single investigator obtained four U.S. passports using fraudulent identity documents and was able to travel on those identities. While weaknesses identified in the report are in the State Department and Postal Service, not DHS, it proves we need to build vigilance into our system to catch bogus documents, and that watch lists and databases must be constantly scrubbed for accuracy. Inclusion of biometrics can be a part of this solution, but just bolting it to our current system and practices will no more solve this problem than re-roofing a house will solve a termite problem.

Since the 9/11 attacks, the federal government has intensified the use of biometrics in databases to identify terrorists or other individuals of concern. We have also used this practice to confirm the rights and privileges of those who pose no security risk or who may be entitled to special credentials. The Department of Homeland Security has a principal role in collecting and managing biometric and biographic information on millions of foreign nationals, residents, and citizens in programs used for border and travel security, counterterrorism, immigration control, law enforcement, and infrastructure protection.

DHS incorporates biometrics in a variety of identification documents, particularly for immigration. DHS has at least nine other systems or databases that collect and maintain biometric and biographic records, and links to at least five others in other Departments. Identification data is collected for “trusted traveler” and “safe shipper” programs, to credential transportation workers, and for critical infrastructure protection.

Such broadened use of biometrics may seem justified in the post-9/11 world, but that begs the questions we expect to discuss today. How is the Department using biometric technology today, and how can we best use it to secure the homeland while protecting individual privacy rights? Under this theme, how is DHS working with other agencies to develop standards for biometric and contextual data and to coordinate the collection, management, sharing and control of such records? Why are there so many different databases? What is DHS doing to ensure the use of biometric technology improves security, law enforcement, or program effectiveness, with a minimum duplication of effort? Lastly, how does DHS protect personal information in its custody, and keep this powerful tool from being abused?

The most prominent DHS biometric program is US-VISIT, which collects and verifies fingerprint and facial images for almost all non-US travelers entering this country, and in theory, will someday do the same for their departure. US-VISIT has evolved into a provider of "identity management services" for U.S. Immigration and Customs Enforcement, Coast Guard, and U.S. Citizenship and Immigration Services, as well as other U.S. government agencies. In that role, it is working to link its records to those of the Departments of Justice and State, and is developing information sharing agreements with the Department of Defense. We expect to hear today how US-VISIT is undertaking its mission as custodian for one of the world's largest databases of biometric information. We also expect to hear about plans for the air traveler exit tracking pilots mandated in the fiscal 2009 appropriations, as well as any plans for a comprehensive exit strategy.

Clearly, widespread use of biometric technologies to confirm or discover people's identities is here to stay. It is critical, then, that we understand the full range of policy implications, management challenges, and funding issues such programs entail.

We welcome today for the first time before this Subcommittee Kathleen Kraninger, the Deputy Assistant Secretary for Screening, and welcome back Mr. Robert Mocny, the Director of US-VISIT. Your written statements will be entered in the record, and I ask that you provide brief oral statements. Before you begin, let me turn to my distinguished Ranking Member, Mr. Rogers, for his comments.

###

OPENING STATEMENT OF RANKING MEMBER ROGERS

Mr. ROGERS. Thank you, Mr. Chairman. Welcome, ma'am and sir.

From IDENT to WHTI to TWIC, REAL ID to US-VISIT, a seemingly endless list of acronyms and abbreviations that represent DHS's efforts to verify identity and provide real integrity for the screening and credentialing of both travelers to and from the country and key personnel. At the heart of this acronym soup is the biometric data that allows DHS to distinguish between the legitimate and those who wish to inflict harm.

In recognition of the multitude of programs with similar reliance upon biometric data for their enrollment and vetting processes, DHS did what any good government agency does: It created yet another new acronym to coordinate and harmonize these activities, known as the—I think I am pronouncing it right—the SCO. Is that right: SCI or SCO?

Ms. KRANINGER. SCO.

Mr. ROGERS. SCO—pardon me—SCO, the Screening Coordination Office. This office has made some real progress in unifying these programs across the Department through what is known as the Credentialing Framework Initiative, an effort that, for the first time, comprehensively inventoried all of the DHS's screening and credentialing programs in terms of capabilities, technology relationships, and investment needs, thereby identifying opportunities for improved efficiency and economies of scale.

But these programs, and perhaps, more importantly, our terrorist, selectee, and no-fly watch lists are only as good as the data they contain. DHS's efforts to unify the vetting process for its credentialing programs will serve little benefit if the data they are checking against is lacking in its breadth or authenticity.

To this point, GAO recently identified gaps in the Department of Defense's processes for the collection and sharing of biometric data of known and suspected terrorists with DHS. In a separate investigation, GAO found it relatively easy to obtain genuine U.S. passports, the so-called "gold standard of identification," using fraudulent identification.

These two reports, combined with the fact that we continue to lack an effective exit solution for US-VISIT, tell me there are some serious gaps in our identity security efforts across the government, gaps in the quality of the known and suspected terrorist data we are checking against, gaps in our immigration controls, gaps in identity verification. These are gaps we simply cannot tolerate in the post-9/11 era.

So, with the help of our witnesses, Mr. Chairman, I hope to learn more about how we are addressing these gaps, like you. While I certainly appreciate how far DHS has come in coordinating its identity security efforts, all of that work will be for naught if we are not applying rigor to the foundations of these programs and managing them with real accountability, sentiments which echo the findings of the 9/11 Commission, as well as the priorities of this Subcommittee.

So welcome to the room. Mr. Chairman, and thank you for the time.
[The information follows:]

OPENING STATEMENT

CONGRESSMAN
Hal Rogers



FIFTH DISTRICT • KENTUCKY

Offices in
Washington, D.C.
Somerset, Prestonsburg,
Hazard

Contact: Stefani Zimmerman

202.225.4601

Opening Statement
Subcommittee on Homeland Security Appropriations

Biometrics / Identity Programs

Witnesses:

Miss Kathleen Kraninger, Deputy Assistant Secretary for Policy
Mr. Robert Mocny, Director, US-VISIT

10:00 AM | Thursday | March 19, 2009 | 2362-B

Thank you, Mr. Chairman, and welcome to our distinguished guests.

From IDENT to WHTI to TWIC to REAL ID to US-VISIT, there is a seemingly endless list of acronyms and abbreviations that represent DHS's efforts to verify identity and provide real integrity for the screening and credentialing of both travelers and key personnel. At the heart of this acronym soup is the biometric data that allows DHS to distinguish between the legitimate, and those who wish to inflict harm.

In recognition of the multitude of programs with similar reliance upon biometric data for their enrollment and vetting processes, DHS did what any good government agency does: it created yet another, new acronym to coordinate and harmonize these activities known as the "SCO," or Screening Coordination Office.

This office has made some real progress in unifying these programs across the Department through what is known as the Credentialing Framework Initiative—an effort that, for the first time, comprehensively inventoried all of the DHS's screening and credentialing programs in terms of capabilities, technology relationships, and investment needs; thereby, identifying opportunities for improved efficiency and economies of scale.

But, these programs, and, perhaps more importantly our terrorist, selectee, and no-fly watchlists, are only as good as the data they contain. DHS's efforts to unify the vetting process for its credentialing programs will serve little benefit if the data they are checking against is lacking in its breadth or authenticity.

To this point, GAO recently identified gaps in the Department of Defense's processes for the collection and sharing of biometric data of known and suspected terrorists with DHS. In a separate investigation, GAO found it relatively easy to obtain genuine U.S. passports – the so-called "gold standard of identification" – using fraudulent identification.

These two reports, combined with the fact that we continue to lack an effective exit solution for US-VISIT, tell me there are some serious gaps in our identity security efforts across the government—gaps in the quality of the known and suspected terrorist data we are checking against, gaps in our immigration controls, and gaps in identity verification.

These are gaps we simply cannot tolerate in the post-9/11 era.

So, with the help of our witnesses, I hope to learn more about how we are addressing these gaps. While I certainly appreciate how far DHS has come in coordinating its identity security efforts, all of that work will be for naught if we are not applying rigor to the foundations of these programs and managing them with real accountability—sentiments which echo the findings of the 9/11 Commission as well as the priorities of this Subcommittee.

Thank you, Mr. Chairman. I look forward to today's discussion.

###

Mr. PRICE. Thank you. Ms. Kraninger, please begin.

OPENING STATEMENT OF KATHLEEN KRANINGER

Ms. KRANINGER. Mr. Chairman, Ranking Member Rogers, and other distinguished Members, I am pleased to appear before you today with my colleague, Bob Moczny, to discuss the use of biometrics and identity management programs across DHS that enhance our nation's security.

In its short history, the Department of Homeland Security has truly been at the forefront in implementing large-scale, high-visibility programs utilizing biometrics technology. It is clear that biometrics and identity management programs provide a key capability, furthering our mission to keep bad people and dangerous goods out of the United States and to protect critical infrastructure.

Our mission is critical, tangible, and highly complex. It requires a split-second decision by a CBP officer at the port of entry or a U.S. CIS adjudicator reviewing a naturalization case or a Coast Guard officer on the high seas.

To support those decisions, we need to provide the right information to the right person at the right time, and, Mr. Rogers, as you said, that is, obviously, a very difficult thing to do, and it is relying on the underlying information that we have available to us. But we have to ensure that that right decision can be made in that limited period of time, and we have to be right every time.

Bob will provide some key examples of some of the success stories, but we recognize that much work has to be done.

As the Department continues to mature, we are focusing on not just those individual mission environments but how they fit together, how the investments we make in one component can support another, how the business processes we use in one component compare to the ones used in another in a similar process, and we are beginning to realize the capabilities and vision with the creation of the Department.

Let me take a moment to speak specifically about what the Screening Coordination Office is doing in this area. Over the past two years, the SCO has led a DHS-wide effort to establish a framework for our people-screening programs. We have looked at how we can enhance our screening processes to achieve better security, efficiency, and facilitation, and we have found that the screening programs face the same challenges and essentially follow the same process.

Every process involves enrollment or collection of certain personal information, whether it is fingerprints or a photograph, name and date of birth, extensive biographic information, or all of the above, depending on the program, yet how is each program collecting that information? How did they determine what information was appropriate to collect?

After enrollment, the agency must conduct vetting, or validating that information, and ensuring eligibility and accuracy. Is the terrorist watch list checked? Is immigration status checked? Is a criminal history records check conducted? Which systems facilitate these checks, and how do adjudicators receive results back and make appropriate determinations?

Enrollment and vetting are just two of the key parts of the screening business process, but they account for a significant portion of the investment.

That takes me to the most critical part of our framework effort. Working with the screening programs, the Department's CIO, CFO, chief procurement officer, and privacy officer, we are rationalizing and prioritizing these investments in the screening technologies and systems to provide a consistent, security-risk-based framework across DHS programs to improve our processes, eliminate redundant activities, utilize existing information in a more effective manner, and improve the experience for the travelers and the public who seek DHS services.

While this exercise is certainly about good management, it also supports our ability to accomplish our mission. Establishing standards and ensuring interoperability enables us to better share information across programs, as appropriate. It creates a common language so that the different layers of security, key interdependencies, and inherent vulnerabilities are better understood across the Department. This all facilitates a stronger integration of effort to improve how we achieve our mission.

I focused primarily on internal DHS integration, though, as the Committee appropriately recognized, this is an effort across the interagency, as well as across the globe. We have a longstanding relationship with the Departments of State and Justice in furthering biometric technology standards and interoperability to enable information sharing.

We have established a strong cooperative effort with the Department of Defense and the intelligence community, and both of those efforts continue to mature. DHS is working closely with allies and interested nations to shut down terrorist travel routes through these same principles: establishing standards and interoperability and sharing information, as appropriate.

We realize the responsibility we have to protect this country and the opportunities for meeting that mission through a coordinated effort.

Thank you again for the opportunity to testify and for your continued support of these efforts.

I would be happy to take any questions that you have at an appropriate time.

Mr. PRICE. Thank you very much. Mr. Mocny.

OPENING STATEMENT OF BOB MOCNY

Mr. MOCNY. Chairman Price, Ranking Member Rogers, and distinguished Members of this Committee, I am pleased to appear before you today with Kathy Kraninger of DHS's Screening Coordination Office to discuss the critical role that biometric identity management plays in today's homeland security efforts.

In the five years since DHS embarked on the world's first large-scale, biometric identification program, our biometric services have revolutionized the way decision-makers across the government verify identity and determine whether someone poses a threat to the United States.

When we began, the U.S. was relying on travel documents that could be easily forged to verify international travelers' identities.

ICE inconsistently knew when local police arrested an immigration violator, and the U.S. Immigration and Border Management System had disparate information systems that lacked coordination.

The use of biometrics has changed all of this. Today, we verify international travelers identities with biometrics, which makes fraud almost impossible. Thanks to biometrics, DHS and the State Department have stopped thousands of criminals and immigration violators from traveling to or entering the United States. Information about criminals and immigration violators is more seamlessly shared between ICE and law enforcement authorities as we make the DOJ and DHS biometric systems interoperable.

And DHS is moving from disparate systems toward a single source for biometrics-based information about criminals, immigration violators, and known or suspected terrorists. Our IDENT biometric system helps almost every single agency whose mission affects homeland security, from CBP officers at ports of entry to the U.S. Coast Guard on the high seas of the Caribbean to local law enforcement agencies booking criminals.

To give you some sense of the scale of these services, government agencies relied on biometrics to help accurately identify people and assess their risk 48 million times in Fiscal Year 2008 that is more than 130,000 identification transactions every day. These encounters were people applying for visas, arriving at ports of entry, applying for immigration benefits, people caught trying to illegally sneak into the U.S., and people arrested by local law enforcement.

DHS's Biometric Support Center also helps law enforcement and the military identify criminals and terror suspects through the analysis of latent fingerprints left behind at crime scenes or on the battlefield.

Biometrics are also helping where other forms of identification cannot. Last year, a man arrived at New York's JFK Airport and presented a valid passport and a valid visa. When his fingerprints were checked through US-VISIT, they revealed that he was trying to use the visa belonging to his twin brother, who had no history of criminal or immigration violations.

By matching his biometrics, CBP officers learned that this man had been apprehended for taking photos of a U.S. military base and had overstayed the terms of admission on a previous visit to the U.S. He was refused admission.

Although the use of biometric identification and analysis services has grown rapidly across DHS and other agencies in the last few years, we still have much to do to stay ahead of the increasing sophistication of terrorists and criminals. The work ahead requires collaboration across the government and with the international community.

Internally at DHS, US-VISIT is working to strategically align its biometric services with the needs of the agencies it supports through an Executive Stakeholder Board. This board will significantly improve planning and coordination for future biometric initiatives.

In addition to continuing to collaborate internally, DHS is working on three areas that will enhance our biometric services.

Number one: As I mentioned earlier, DHS is working to make our biometric system interoperable with that of the FBI. The im-

proved interoperability of our system is already helping ICE identify and remove criminal aliens arrested by state and local law enforcement through the Secure Communities program.

Number two: We continue to stay on the leading edge of biometric technology to ensure that the solutions we develop are more advanced than the threats we face. We are closely working with DHS's Science and Technology Directorate to research multimodal biometric technologies like iris scans and facial recognition, that will help us more accurately identify people, increase efficiency, and make the technology easier to use.

Number three: We are working with other countries who are adopting similar biometrics programs to share lessons learned and develop compatible systems. As countries develop compatible systems, we can share biometric information about criminals and known or suspected terrorists, dramatically improving our ability to prevent those people from moving across our borders undetected.

For example, United Kingdom immigration officials recently requested that the United States check one of its asylum applicant's fingerprints against DHS's data. The result revealed that the man had previously traveled to the U.S. using a different name, confirming for U.K. officials that the asylum applicant was lying about his identity. Upon further investigation, the U.K. learned that the man was wanted on rape charges in Australia, and he was returned.

A case like this illustrates that sharing biometric information with our allies holds great promise for making all of our countries safer.

Mr. Chairman, thank you for the opportunity to update you on how biometrics are improving DHS's identity management efforts. Your Committee's leadership in funding this work has helped the United States lead the way in biometrics screening. I look forward to working with this Committee as we continue to improve the biometric identification services our frontline decision-makers rely on to identify and deter human threats. Thank you very much.

[The information follows:]

**Statement for the Record
of
Kathleen Kraninger
Deputy Assistant Secretary for Policy, Screening Coordination
Department of Homeland Security
and
Robert A. Mocny
Director
US-VISIT Program
National Protection and Programs Directorate
Department of Homeland Security**

**Before the
United States House of Representatives
Appropriations Committee, Subcommittee on Homeland Security
Washington, DC**

March 19, 2009

Chairman Price, Ranking Member Rogers, and other distinguished Members, we are pleased to appear before you today to discuss how the use of biometrics and identity management programs enhances our Nation's security. The Department of Homeland Security (DHS) continues to refine our capabilities to identify accurately and more efficiently process individuals at the border, in airports, and across our screening programs. The Screening Coordination Office (SCO) within the DHS Office of Policy was established to integrate, where appropriate, the wide range of DHS screening and credentialing activities to enhance our missions of keeping dangerous people and things out of the U.S. and securing critical infrastructure. US-VISIT provides the Department's biometrics identification and analysis services to agencies throughout the immigration and border management, law enforcement and intelligence communities. US-VISIT supports the Department's mission by providing biometric identification services to Federal, State and local government decision-makers to help them accurately identify people and assess risk.

Access to our nation is critical for a terrorist to plan and carry out attacks on our homeland. As the 9/11 Commission's Final Report states, "Terrorists must travel clandestinely to meet, train, plan, case targets, and gain access to attack. To them, international travel presents great danger because they must surface to pass through regulated channels to present themselves to border security officials, or attempt to circumvent inspection points." As the Department continues to implement and integrate key screening programs, the establishment of an integrated immigration and border screening system represents a significant achievement that has improved national security.

The Value of Biometrics

The Department began to collect digital fingerprints and photographs from international visitors applying for visas or arriving at U.S. ports of entry (POE) in 2004 to help immigration officials make visa-issuance and admission decisions. With biographic screening capabilities already

well established, biometrics became the next logical step in the evolution of identity management. Unlike names and dates of birth, biometrics are unique and extremely difficult to forge. They provide a reliable, convenient, and accurate way to establish and verify visitors' identities. Moreover, biometrics are a scalable technology and can be upgraded to stay one step ahead of terrorists and criminals. Biometrics help us meet the challenge of making travel difficult for those who want to do us harm, while making it convenient and efficient for legitimate visitors.

Through its use of biometrics, the Department's US-VISIT program collects, stores, and shares digital fingerscans and digital photographs for subsequent verification. This biometric information is paired with biographic information pertaining to an individual and used to establish and verify that individual's identity.

We want to reinforce the critical progress we have made by discussing key capabilities that biometrics provide: greater security, increased efficiency, and a new level of identity assurance.

The Department's implementation of biometrics capabilities has laid the foundation for the rapid expansion of biometric identification to other agencies. Today, this biometric coordination across the Government is making our screening more collaborative, more streamlined, and more effective than ever before.

Five years ago, our immigration and border management system had disparate information systems that lacked coordination. Today, the Department is unifying these systems to promote a centralized source for biometric-based information on criminals, immigration violators, and known or suspected terrorists.

Five years ago, U.S. Immigration and Customs Enforcement (ICE) lacked timely and accurate information about visitors who overstay their visas. Today, US-VISIT provides more than 250 credible leads weekly to ICE, enabling that organization to better enforce our immigration laws. Through ICE's Secure Communities Program, we are also helping to identify immigration violators arrested by State and local law enforcement.

Five years ago, the United States was alone in applying biometrics to the immigration and border management communities. Today, the United Kingdom and Japan already have robust programs using biometrics. The European Union, Canada, Mexico, Australia, Argentina, Peru and many other countries are in various stages of applying biometrics to immigration control.

Five years ago, we were relying on visual inspection of travel documents to try to identify those that were fraudulent. Today, because of increased information sharing within DHS and with the Department of State (DOS), along with the use of biometrics and machine-readable travel documents, we are able to more quickly identify fraudulent documents. As an example, DHS and DOS partnered in developing the e-passport, which set a new international standard for the security features of a travel document, and the passport card, providing U.S. citizens a secure, limited-use travel document in a more convenient format.

As you know, DHS is preparing for the June 1, 2009, implementation of the Western Hemisphere Travel Initiative (WHTI), which will require U.S. and Canadian citizens to present standardized, secure documentation denoting identity and citizenship for entry at the U.S. land and sea ports of entry. WHTI addresses the vulnerabilities inherent when travelers can present a wide range of documents that are highly susceptible to fraud and cannot be verified. WHTI-

compliant documents available to U.S. citizens (the passport book, passport card, Trusted Traveler Program cards, and Enhanced Driver's Licenses) are issued in a secure manner and include a biometric (digital photograph) on the face of the card. The WHTI solution is transforming the border by moving away from a vehicle-centric system to a person-centric one.

Radio-frequency identification technology embedded in most WHTI-compliant travel documents, with the appropriate privacy protections and infrastructure, allow DHS the ability to verify an individual's identity and perform real-time queries against lookout databases even before the traveler pulls up to the inspection booth. The trained DHS officer can compare the digital photograph and biographic information on the document to the traveler in front of them, as well as to the photograph and information on the DHS border officer's screen that is provided by the document's issuer—all of which assist the officer in making better decisions about an individual's admissibility to our country.

While implementing the screening programs across the Department, DHS has maintained focus on the four guiding principles first established for US-VISIT, which are to:

- Enhance the security of our citizens and visitors;
- Facilitate legitimate travel and trade;
- Ensure the integrity of our immigration system; and
- Protect the privacy of our visitors.

Screening and Credentialing Programs

DHS continues to identify opportunities to harmonize and enhance screening processes for both security and efficiency reasons across DHS programs. In doing so, we must rationalize and prioritize investments in screening technologies and systems while recognizing that each program faces individual challenges, operates in different environments, and adheres to its respective legal authorities.

In July 2008, DHS finalized the DHS Credentialing Framework Initiative (CFI) to guide the selection and coordination of credentialing activities and investments throughout DHS. In developing the CFI, the SCO led a DHS-wide effort to analyze and compare key programs across the credentialing lifecycle of registration and enrollment, eligibility vetting and risk assessment, issuance, and expiration and revocation; identify the relationships between the credentialing processes and business capabilities and the Information Technology services related to screening and credentialing across the DHS enterprise; and outline the projects needed to actualize a robust, cohesive environment across DHS programs.

While one size does not fit all, every program does not have to reinvent the wheel. The CFI aims to provide a consistent, security risk-based framework across all DHS credentials, improve credentialing processes to eliminate redundant activities, utilize existing information more effectively and improve the experience for individuals applying for DHS credentials. The guidance directs the following:

- Design credentials to support multiple licenses, privileges, or status, based on the risks associated with the environments in which they will be used.
- Vetting, associated with like uses and like risks, should be the same.
- Immigration status determinations by DHS components should be verified electronically.
- Eligibility for a license, privilege, or status should be verified using technology.

- Design enrollment platforms and data collection investments so that they can be reused by other DHS programs – establishing a preference for “enroll once, use many” environment, where appropriate.
- Ensure opportunities for redress – individuals should be able to correct information held about them.

Integrating a Streamlined Transportation Screening Platform

The Transportation Security Administration’s (TSA) Transportation Threat Assessment and Credentialing (TTAC) entity is in the initial stages of an enterprise modernization that is being designed to meet the mission of TSA in line with the CFI requirements. The TTAC Enterprise Modernization Program supports TSA’s mission by significantly improving the vetting management and adjudication platform currently used for conducting security threat assessments on various transportation populations through the use of software applications and a common information technology infrastructure. The current TTAC vetting and credentialing enterprise architecture was created to support 2.5 million individuals per year. Today, the populations supported by TTAC have almost tripled.

It is anticipated that after five years, existing stove-piped business processes and information systems will either be reengineered or replaced by a new integrated business enterprise architecture that will: consolidate multiple enrollment methods, implement identity management services across programs, standardize the approach for customer relationship management, standardize the physical and virtual credentialing processes, standardize threat assessment processes, and consolidate operations, integrating program-specific IT systems and business processes into a common secure enterprise vetting and credentialing architecture. The TTAC Enterprise Modernization program presents an opportunity to eliminate redundant business practices, processes, and subsequent IT investments to achieve significant economies of scale benefits associated with a unifying business integration effort.

In line with the CFI, the TTAC Enterprise Modernization program provides for a unified, modular, and maintainable architecture that will reduce the cost, risk, and time associated with implementing new capabilities, on-boarding new populations, improving the robust nature of the architecture, and on-going operations and maintenance. The Department expects that TTAC modernization will support not only TSA needs but also other special population vetting programs that may support the security of critical infrastructure sectors. Further, TTAC modernization is being coordinated with the Department’s other ongoing information technology modernization efforts.

Biometric Screening and Identification

In another effort to streamline DHS processes, DHS has designated US-VISIT’s Automated Biometric Identification System (IDENT) as the biometric storage and matching service for the Department, providing biometric identification and analysis services to agencies throughout the immigration and border management, law enforcement, and intelligence communities. US-VISIT supplies the technology for collecting and storing biometric data, provides analysis of the data to decision-makers, and ensures the integrity of the data.

IDENT plays an important role in the biometric screening and identity verification of non-U.S. citizens for ICE, CBP, U.S. Citizenship and Immigration Services (USCIS), and U.S. Coast

Guard. US-VISIT also supports the Department of State's (DOS) BioVisa Program and shares information with the Federal Bureau of Investigation (FBI).

Here is how it works:

- With each encounter, US-VISIT checks a person's biometrics against a watchlist of more than 5.2 million known or suspected terrorists, criminals, and immigration violators identified by U.S. authorities and Interpol.
- When an identification document is presented, a person's biometrics are also checked against those DHS has on file as associated with the document to ensure that the document belongs to the person presenting it and not to someone else.
- US-VISIT provides the results of these checks to decision-makers when and where they need them.

Biometric Services for DHS and Other Agencies

To give you an idea of the breadth of our services, every day US-VISIT provides access to biometric data for 30,000 authorized Federal, State, and local government agency users to help them identify, mitigate, and eliminate security risks. Let us give you a few examples.

- USCIS uses biometrics to screen applicants for immigration benefits.
- Border Patrol and U.S. Coast Guard use biometrics as part of their efforts to apprehend illegal migrants.
- Department of Defense (DOD) and the intelligence community provide biometrics, including latent fingerprints, they collect from locations where terrorists have been, such as safe houses or training camps to DHS in order to determine whether we've previously encountered individuals they suspect to be terrorists and terror suspects.
- And finally, State, local and other federal agencies submit biometrics to DHS to support their investigations. Our Biometric Support Center (BSC) verifies almost 50,000 fingerprints each week—helping to solve crimes, identify John or Jane Does, and support terrorist investigations.

Additionally, the US-VISIT Program Office is working with a number of other DHS components, such as the TSA, on future and planned credentialing and identity management programs.

10-Fingerprint Transition

DHS's transition from collecting 2 digital fingerprints to collecting 10 digital fingerprints at ports of entry from visitors to the United States is nearly complete. DHS deployed new 10-fingerprint scanners at U.S. POEs in 2008, providing the capability to capture 10 fingerprints from 97 percent of in-scope travelers. The transition to 10-fingerprint collection increases DHS's ability to keep dangerous people out of the United States, while making legitimate travel more efficient. Today, the new fingerprint scanning devices are in place at all major POEs, so international visitors can expect to use the upgraded technology when they enter the United States.

The use of 10 fingerprints for biometric verification offers many enhancements. In 2007, DOS began collecting 10 fingerprints from visa applicants at all of our embassies and consulates to

enhance the ability to establish and verify applicants' identities. 10-fingerprint readers improve the accuracy of identification; improve interoperability with the FBI and DOS, local, and tribal governments; and will mean fewer travelers will be referred to CBP secondary inspection. DHS will now also be able to conduct full searches against the FBI Unsolved Latent File, which, for example, allows DHS to match against prints lifted from crime scenes and those collected in Afghanistan and Iraq.

Interoperability with the Departments of Justice and State

DHS's 10-fingerprint collection standard makes our system more compatible with the FBI's biometric system, the Integrated Automated Fingerprint Identification System (IAFIS). We have been working with the FBI for the last several years to make our two databases fully interoperable to more seamlessly match biometric information so we can better identify people who pose a threat to our country.

DHS, the Department of Justice (DOJ), and DOS signed a memorandum of understanding on interoperability on August 1, 2008. The first-phase capabilities for the initial operational capability were deployed in October 2008.

This integrated system will allow authorized users access to all relevant information in a timely manner so they can make the right decisions about the individuals they encounter. IDENT/IAFIS interoperability increases the ability of DHS and DOS to screen individuals; and it benefits the FBI and other law enforcement organizations by providing them with increased access to immigration information about high-risk individuals to whom DOS has refused visas and those whom DHS has expeditiously removed.

Secure Communities

The Department's Secure Communities initiative will change immigration enforcement by using technology to automate sharing with law enforcement agencies and by applying risk-based methodologies to focus resources on assisting all local communities to remove high-risk criminal aliens.

In 2008, DHS and DOJ began an information-sharing program with local law enforcement counties in North Carolina by providing them access to immigration violation information on their criminal arrests. This capability is part of DHS and DOJ efforts to distribute integration technology that will link local law enforcement agencies to both FBI and DHS biometric databases.

US-VISIT and the FBI Criminal Justice Information Services Division continue to work with ICE in preparation for further deployment of Secure Communities.

Developing Interoperability with the Department of Defense

DHS and DOD have begun identifying ways the two departments can exchange information in a more systematic manner to further each other's missions consistent with legal authorities and privacy. Central to this effort is an automated exchange of biometric data on individuals' DOD encounters overseas. Such information would greatly enhance the ability of DOS and DHS to effectively screen who is admitted into the United States. DHS information is useful to DOD for credentialing and access control vetting, among other uses. As with interoperability with DOJ

and DOS, some of the most complex issues concerning data sharing are not technical, but rather those dealing with policy and business processes. DHS and DOD are working diligently to explore potential opportunities and to identify technical and process solutions.

Air/Sea Biometric Exit

DHS has performed significant planning and testing over the past three years examining possible solutions for integrating US-VISIT biometric exit requirements into the international air departure process. The options of deployment at airline ticket counters, TSA checkpoints, airline boarding gates, and in airport terminals are being considered. For more than two years, US-VISIT ran biometric exit pilots at 14 air and sea locations. These pilots evaluated the use of both automated kiosks and mobile devices in port terminals. The pilots ended in May 2007 and demonstrated that the technology works, but also that compliance by travelers was low.

On April 24, 2008, DHS published a notice of proposed rulemaking (NPRM) on the collection of biometrics from aliens departing from air and sea ports. The NPRM proposed that commercial air carriers and vessel carriers collect and transmit international visitors' biometric information to DHS within 24 hours of their departure from the United States. Development and publication of a final rule is pending the completion of pilots as required by the Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009 (Pub. Law 110-329). The 2009 Appropriations Act restricts US-VISIT from spending any money to create an air exit solution, until the pilots are completed and a report on the pilot test is submitted to the Committees on Appropriations of the Senate and the House of Representatives and reviewed by GAO. DHS is assessing methods for conducting air exit pilots consistent with the FY 2009 appropriation. The results of the pilot evaluation, combined with the review of public comments submitted in response to the NPRM, will inform the decision on the option to be selected for publication in the final rule.

When a long-term exit solution is deployed, it will also be deployed to commercial seaports to provide an integrated biometric exit capture for vessel carriers passengers. However, the scope for biometric exit at sea will be considerably smaller than for air.

International Cooperation and Collaboration

When DHS began the US-VISIT program to collect biometrics as part of port of entry screening, the world watched skeptically to see if the benefits of biometrics would work on a large scale. Although a handful of nations were testing biometrics, DHS was the first to launch a comprehensive biometric-based identity management system for immigration and border management. Five years later, more and more countries are approaching us to discuss our lessons learned as they develop their own similar systems. We want other countries to benefit from our experience, and in turn, we can learn from them.

Some countries have already begun operations or are nearing deployment. For example:

- In November 2007, Japan implemented a two-fingerprint biometric entry system that is similar to US-VISIT's initial implementation.
- The United Kingdom is collecting 10 fingerprints from visa applicants and is testing fingerprint collection at ports of entry.

- The European Union is building a 10-fingerprint visa-issuance program based on the very successful Eurodac.
- We are working closely with Australia, which has been a pioneer in facial recognition, as it advances its identity management program.
- The United Arab Emirates has been using iris scans as part of its immigration and border control processes for some time now.

Other countries are actively pursuing biometrics:

- In August 2008, Peru announced it is working to implement biometric technology in its migration control systems to guarantee the authenticity of personal identification documents and to speed visitor control.
- Mexico is planning to modify its currently successful biographic-based system to incorporate biometrics, which is similar to what we did in 2004.
- Canada recently approved the budget for a 10-fingerprint visa-issuance program.

As the use of biometrics increases worldwide, the importance of international standards and best practices cannot be overstated. Consistent international standards for biometrics are essential to developing compatible systems, and compatible systems are essential to crippling international criminal enterprises as well as terrorists' ability to travel. Appropriate data sharing can only be accomplished with consistent standards.

The Future of Biometric Screening

Biometrics offer real opportunities to dramatically increase the efficiency of identifying people. The Department is researching emerging technologies to expand our screening and identification capabilities. We recognize that future identity management systems will require increased assurance, efficiency, ease of use, and flexibility.

As DHS implements biometric exit procedures, both at airports and land border POEs, we are looking for more efficient, less invasive technologies to verify visitors' departures. Particularly at the land border, we are looking for technologies that might meet our needs better than requiring visitors to have their fingerprints scanned while driving at speed through a POE.

In some cases, the key to expanding biometric screening is to bring the technology to remote locations where decision-makers need it.

- For example, Coast Guard is using mobile biometric collection and analysis capabilities on the high seas off the coasts of Puerto Rico and Florida. This project has helped the Coast Guard identify and refer for prosecution and/or administrative immigration proceedings hundreds of repeat illegal migrants who are ineligible to enter the United States, including some wanted for human smuggling and murder.
- In addition, CBP's Air and Marine Operations is examining opportunities to use mobile biometrics to its areas of operation.

Success Stories

Our biometric entry procedures have made a tremendous difference in efforts to improve the integrity of our immigration and border management system. Some of our many success stories include stopping more than 2,400 criminals or immigration violators at the POEs based on

biometrics alone, and identifying thousands who are ineligible to receive visas to travel to the United States. There is no doubt that we have deterred countless more.

DHS's use of biometrics is helping eliminate the ability to use fraudulent or altered travel documents. Now when travelers arrive in the United States, we are able to quickly verify their identity and identify those who are known to have committed immigration violations. Here is an example:

- On March 16, 2008, a subject arrived at the John F. Kennedy International Airport in New York and applied for admission with a valid Turkish passport and an unexpired B1/B2 visa. The subject was referred to secondary inspection as a match to the IDENT biometric watchlist for a previous voluntary departure.
- During secondary inspection, queries revealed that on November 10, 2003, the subject had been apprehended taking pictures of the Ft. Leonard Wood Missouri Military Base. While in custody, it was discovered then that he had overstayed his period of admission in the United States.
- This subject had been admitted into the United States on June 9, 1997, and was granted voluntary departure by an immigration judge on May 13, 2005, to remove himself by September 13, 2005.
- On March 16, 2008, the subject attempted to enter the United States using the identity of his twin brother through his brother's travel documents. The subject was denied access. The subject is inadmissible to the United States for willful misrepresentation and not being in possession of valid travel documents.

Biometrics are helping enforce our borders away from ports of entry, too.

- In December 2007, the U.S. Coast Guard interdicted 10 migrants attempting to illegally enter Puerto Rico by sea. When the migrants' biometrics were checked against IDENT, it was revealed that two of the migrants had illegally entered the United States before, had been subsequently removed from the United States, and were suspected of being part of a human trafficking organization. The two suspected traffickers were brought ashore for referral for prosecution along with two witnesses who would testify against them. Since the Coast Guard began using mobile biometric services to identify illegal migrants at sea, prosecutions of repeat offenders have increased dramatically and illegal migration has dropped by 60 percent in the area where the technology is being used.

US-VISIT Privacy

DHS is committed to adhering to the strictest privacy standards. DHS only collects information needed to achieve the program objectives and mission and only uses this information in a manner consistent with the purpose for which it was collected. DHS also conducts periodic audits of its systems to ensure appropriate use within the limitations of the Privacy Act.

Ultimately, the success of the US-VISIT program will be measured by not only our ability to identify those who may present a threat, but also our ability to protect against identity theft and fraud. We are acutely aware that our success depends on how well we are able to protect the privacy of those whose biometrics we hold. A breach of this most personal data would undermine the public's trust. We have a dedicated privacy officer responsible for ensuring compliance with privacy laws and procedures and for creating a culture of privacy protection

within the US-VISIT Program. Furthermore, we are transparent. From the beginning, we made clear that the information gathered by DHS or State will be used only for the purposes for which it was collected, consistent with those uses authorized or mandated by law. Our policy extends to non-U.S. citizens most of the same privacy protections we give by law to U.S. citizens. We regularly publish privacy impact assessments and system of records notices to provide people with a clear view of the information we collect, how we store it, and our policies and practices to ensure it is not abused.

Conclusion

To ensure we can shut down terrorist networks before they ever get to the United States, we must also take the lead in driving international biometric standards. By developing compatible systems, we will be able to securely share terrorist information internationally to bolster our defenses. Just as we are improving the way we collaborate within the U.S. Government to identify and weed out terrorists and other dangerous people, we have the same obligation to work with our partners abroad to prevent terrorists from making any move undetected. Biometrics provide a new way to bring terrorists' true identities to light, stripping them of their greatest advantage—remaining unknown.

Biometrics have increased our Nation's security and the security of nations around the world to a level that simply did not exist before. Biometrics are affording us greater efficiencies, making travel more convenient, predictable, and secure for legitimate travelers. Biometrics are enabling people to have greater confidence that their identities are protected, and in turn decision-makers are more certain that the people they encounter are who they say they are.

So what is next? We need to aggressively pursue innovation. Those who want to do us harm continue to contemplate ways to exploit our weaknesses, so we cannot afford to slow down. We too must contemplate ways to create even more efficient and affordable identification technologies. We have to continue to explore mobile biometrics and biometrics captured at speed, and we must do so safely.

We must also continue to advocate abroad. We recognize that with the power of biometrics and a foundation of international cooperation, we can transform and enhance the way the people travel the world and the way we protect our nations from those who would do us harm.

Chairman Price, Ranking Member Rogers, and other distinguished Members, we have outlined our current efforts that, with your assistance, will help DHS continue to protect America. The Department's use of biometrics plays a critical role in supporting many programs and initiatives within DHS and other Federal agencies.

Thank you for again for this opportunity to testify. We will be happy to answer any of your questions.

PASSPORTS ISSUED TO GAO INVESTIGATORS

Mr. PRICE. Thanks to the both of you. Now, we will proceed with questions.

I want to ask you to reflect on a case that has been very prominent in the news lately. Even though it is outside your immediate area of responsibility, I am sure you have not only heard about it but thought about it, and I think it would be a good way to get us started today, to understand some of the potential, and maybe some of the limits, of biometric technology.

As you know, the State Department recently issued four U.S. passports to GAO investigators, and they were based on Social Security numbers issued to a fictitious five-year-old child, a dead man, and bogus identity documents, including forged drivers' licenses and birth certificates. All applications had pictures of the same individual.

Could biometrics have solved this, or to what extent could biometrics have solved this, or is it a case of underlying processes being so flawed that it is not simply a question of more sophisticated and more fool-proof technology?

Ms. KRANINGER. Biometrics are certainly an important aspect of being able to establish and verify an identity, but they certainly are not the end-all/be-all.

At the beginning of the process, you are looking at how to issue a passport or any document. As I said, we have really taken that business process apart and looked at what information should be collected and how should it be checked, and there is certainly a lot of system improvements that have happened in recent years but many more that still need to happen.

We have been working very closely, for example, with the Social Security Administration. They do provide a capability to actually check Social Security numbers for appropriate agency use. The State Department has been using that system. We use that system in different cases, but the next part of the process here is looking at birth and death records. Certainly, that would be an appropriate way to verify that an individual is no longer alive and, therefore, is not applying for a passport.

That system actually is underway as well, and will likely, with the desire to get to electronic health records, get a little boost as well in that area. This is something that we are very interested in, and the State Department is very interested in, because the opportunity to check with the vital records agencies across this country, of which there are many, and their ability to collect that information and verify is varied, but some [vital records agencies] are fairly sophisticated. And so the opportunity to check those records is, again, another useful step in the process.

The third point is just to look at the biometrics question you asked. In part, it becomes, when is the identity actually established, and then against what are you verifying? Certainly, the theory, as we have moved forward with US-VISIT, is, yes, it is very possible that someone who is not who they say they are is coming before us and presenting a false identification, but they will not get to do it again.

It is not ideal, but it is what we have done with the system. By collecting fingerprints, we are then freezing, so to speak, that identity in our system. For example, the twin brother case is a perfect example of how that action and that threat can be countered.

The State Department is looking to use facial recognition technology more broadly. It help to do a similar check as fingerprints, although the facial recognition technology is not as far along as we would like it to be. We are encouraging the State Department to continue to use that. As they noted in their response to the report, they do use it for visa applications, and are looking to do that for passport issuance as well.

So it is not one single solution to this problem, but it is something that we are looking at, the underlying documents that we are relying on for identity presentation, how we verify those, and certainly what information we collect, whether it is biographic or biometric.

Mr. PRICE. The inclusion of biometric data, whether it is a standardized facial image or fingerprints or whatever; the use of that in the successive documents that we are relying on obviously would tighten up the process of personal identification when you are doing something like issuing a passport.

Ms. KRANINGER. Yes.

DATABASES MANAGED BY DHS

Mr. PRICE. It does not answer the question, how feasible, or how desirable, for that matter, that that is, but there is no question that biometrics, at whatever stage, add a degree of precision that we have not heretofore had.

Well, let me just move into the databases that you are working with at DHS.

When the Department was put together, you inherited databases containing personally identifiable information and biometrics. It has taken time, of course, to bring these together into a cohesive unit, and duplications, new efficiencies, you are still working on.

We need a clear picture of databases managed by DHS, the biometric data they use and the relationship of those databases to non-DHS databases, and I do not expect you to do all of that here orally this morning. But I wonder if you could just give us an overall picture.

When DHS was set up, how many databases containing biometric and biographical and contextual data did it control? How many are there today? How many records are in these databases? Are there still overlaps that you are looking to eliminate, or is there perhaps some justification for keeping some of these databases discreet and not fully integrated?

Ms. KRANINGER. Well, at the beginning of the Department, of course, we had 22 agencies, so there were dozens of databases, again, associated with different programs that may have had personally identifiable information in them. We do have documentation on that, but, as you noted, going through that would be rather extensive.

Primarily, where we are going is setting up service providers within the Department so that we do not have stovepipe systems being set up for each new screening program as we go along the

way. The best example of that really is IDENT, that Mr. Mocny and US-VISIT actually manage and run for the Department.

Biometrics is, obviously, highly complex, highly technical. It is to our benefit, from a management standpoint and also from a security standpoint, to put our expertise in one place with respect to biometric storage, capture, and management of that information, and so that is what we have done. We have designated IDENT as the service provider.

We are on migration paths for the agencies that are not currently using IDENT because many of them are, certainly in the immigration context. Of those that are not, the biggest is TSA. That is something that we are working with them to migrate to. For example, the TWIC fingerprints. We are also looking at aviation worker process and how that works and making sure that we again create that center of excellence.

Probably the other big systems to note are the other modernization efforts that you are very familiar with. TECS is the back end, really, of CBP's operations but is also a major database for law enforcement across the board and contains all of the biographic derogatory information associated with agriculture violations and customs violations. There is ATF and DEA information in TECS. That information is all used for cross-border purposes. CIS uses that information appropriate to their decisions. And so, looking at that modernization effort to really improve our ability to get the right derogatory information to that end user, so they can actually appropriately make a decision, is why the TECS modernization is so important to us.

The other thing is really transforming the way TSA works. There is a modernization effort, actually, in Fiscal Year 2010, that increases their ability to bring their programs together that were very much created in different fee-funded structures with different systems.

US-VISIT IDENTITY MANAGEMENT SERVICES

Mr. PRICE. Perhaps you could supply, in graphic form, the answer to the broad question I asked about the number of databases you inherited, the degree of consolidation that has taken place, the number of records they contain, just so we have in one place an indication of exactly how far this consolidation has proceeded.

I want to move on to other questioners, but I do want to pick up, Mr. Mocny, and we will come back to this, I want to pick up on what Ms. Kraninger just said about the service function of US-VISIT. As we hear about that, it almost seems that this is becoming the core US-VISIT mission because you have so many other agencies and other programs now dependent on you. Of course, your basic entry/exit program; we want to look at the status of that as well.

But you are providing identity management services for CBP, for ICE, for CIS, for the Coast Guard, for FEMA, for TSA. Correct?

Mr. MOCNY. Yes.

Mr. PRICE. You are collecting biometric information on immigration violators and criminals because all of these agencies are collecting information, as well as utilizing it. So is this becoming your core mission, or, at least, a core mission?

Mr. MOCNY. It is. We are kind of transitioning away from what we were initially stood up as a project office, to deploying the equipment out there to begin collecting the information. But as we have done that. Our database is now at 98 million and we are almost at 100 million records of individuals who have come into the United States. We service about 30,000 users every single day, 24/7.

As you mentioned, most of DHS, those components that you mentioned, but also the Department of State. In some respects, that is a good news story because they use our system. They did not have to build a separate biometric system to satisfy the visa in-person biometric requirements; they use the IDENT system as well. So the State Department writes to the IDENT database all of the biometrics that they capture worldwide.

So it is providing a service that people do rely on. We have protocols in place to make sure that the system is as up as it possibly can be. It has to be ready and available for the decision-makers, as Ms. Kraninger talked about, but it is a service that is relied upon now for the current operations across DHS, State Department, and is also, as I said earlier in my opening statement, now helping state and local law enforcement.

So when a police officer in Houston, Harris County, or Boston, Dallas and in several other counties that are beginning to deploy Secure Communities, arrest a subject, in the past, that person would be run against the FBI's IAFIS system and stopped right there. Now, in these communities, more and more, they also run against the IDENT system, and these people will lie to the police officers that they are a U.S. citizen or a legal permanent resident. But now we are able to tell that police officer that this person is in fact, an illegal alien has been deported so many times. ICE can then put a detainer on that individual and then remove that person from the U.S.

So, from the federal to the state and local across the board we are assisting with biometric identification services.

SECURE COMMUNITIES

Mr. PRICE. And the local agencies that would access these records would do it through participation in Secure Communities or some such program.

Mr. MOCNY. That is correct.

Mr. PRICE. It is not generally the case across the country.

Mr. MOCNY. Through the Secure Communities program.

Mr. PRICE. Through a special designation as part of that program.

Mr. Rogers.

US-VISIT IMMIGRATION CONTROL OR INVENTORY

Mr. ROGERS. Well, to follow up on the Chairman's line of questioning on US-VISIT, of course, at the outset it was conceived that US-VISIT would be an agency that would pick up a chore that INS had failed for all of its years, and that was to find a way to learn who was in the country and who had overstayed their allotment of time, an inventory, if you will, of people here illegally. But since we cannot seem to get an exit piece of US-VISIT working, it is not

an inventory anymore of those here illegally, obviously, and it is really essentially a terrorist-screening system, not an immigration-control system. Right or wrong?

Mr. MOCNY. It is an immigration-control system. We do rely on biographic information in a big way. We have a unit dedicated to looking at the information that we glean from another system called ADIS, which is tied to IDENT—ADIS, the Arrival/Departure Information System—and every 180 days we get an exception record of those individuals who are potentially in the country, having overstayed their visa.

We have a unit that looks at that and culls that information, looking at priority countries and individuals and gives that information to ICE.

In Fiscal Year 2008, we sent thousands of records to ICE, Immigration and Customs Enforcement. They made approximately 750 arrests based on that information. That is a functionality we did not have before.

I will grant you, we do not have exit in place. We are working diligently on that. A biometric exit will be in place soon, but the biographic side of the house is being looked at. We are able to work with ICE and are able to take people out of the country to, who have overstayed their visas.

EXIT SOLUTION

Mr. ROGERS. Have we given up on an exit solution?

Mr. MOCNY. Absolutely not, sir. Let me speak to that issue because we have been talking about that, and I was here two years ago talking about that as well. We have made tremendous progress.

It is challenging. I will grant you that. We do not have exit in the U.S. When you leave from France or Australia or Japan, you go through an exit-control process. They have had that up for years.

We do not have that here in the U.S., and so where we did have an entry process which we modified through the US-VISIT program, we have yet to stand up the exit program. We have run some pilots, where we know the technology works. We are going to conduct the two pilots that were in the Fiscal Year 2009 DHS Appropriations Act.

We have the places identified where we are going to run those pilots: one in Detroit and one in Chicago. We will run that pilot for 35 days. We are going to analyze the information from that, and we are going to make recommendations, obviously, to the Secretary and to the Administration, to have a roll-out plan for how we implement biometric exit at the air and seaports of entry.

So I realize we are not where we need to be, or perhaps where we should be. But we are very close, and I am committed, and we are all committed, to getting it up and running.

Mr. ROGERS. Well, it has been a while. We spent \$2.1 billion on US-VISIT, and a big part of the chore that we assigned to US-VISIT was exit, and, without the exit capability, it severely cripples what we have conceived to be the mission of US-VISIT in the first place.

You know, are we just to continue pouring money in this bucket with all the holes in it, or can you give us some hope, just a thread of hope, that, one of these days, we will have an exit part of US-VISIT?

Mr. MOCNY. I can. I can tell you that we have all of the pieces in place.

Certainly, from a legal standpoint, we put a proposed rule out there. We looked at six different scenarios and we costed those out. We went through a very rigorous process. We are now going to conduct the two pilots that were mandated in the 2009 appropriations law. We can then conduct a final rule and have an exit system up and running within the year or so.

Obviously, it is a policy decision for the new Administration to look at. I have not had the opportunity to speak directly to this issue with the Secretary. I see my colleague over here nodding her head. She is aware of this issue within the Secretary's office.

So I can give you a thread of hope, absolutely. We are certainly poised to move forward, and I do not want you to think that the \$2.1 billion is not money well spent. The Chairman has provided this money over the years and we have gotten value for our dollars. We have stopped thousands of individuals from entering this country. We have identified people at the Mona Past, where I know you have seen it personally, sir, and been able to stop people who were coming into this country.

So the money has been well spent. It is not complete yet, but we are moving in that direction.

DOD BIOMETRICS

Mr. ROGERS. Let me switch gears real quickly here, then. DoD has got to be one of the most important sources of information. Right?

Mr. MOCNY. Absolutely.

Mr. ROGERS. GAO, in their October 2008 findings, says that DoD immediately shares biometric data related to terrorism that it collects on non-U.S. personnel. When asked, they share that information. But according to GAO, updates on certain types of DoD biometrics are not being regularly received by DHS, and, when received, are inconsistent in format and usefulness.

For example, if data collected in Afghanistan on a particular individual is only a two-print format, it is often impossible to go back and obtain the other eight prints in order for the information to be logged into our ten-print system.

Tell us about the DoD sharing, whether it is adequate, spotty, or complete.

Mr. MOCNY. Let me start, and I think that Kathy will want to say something as well. Let me start by saying, this is a work in progress. Yes, we are five years old, but, in many ways, the coordination of the biometrics is still something that we are working on.

That being said, we have made tremendous progress on this issue. We receive DoD prints on a daily basis through the FBI, so we have a direct connect from IDENT to Clarksburg, West Virginia, to the IAFIS system. Every day, the FBI will also collect information from ADIS, the DoD system, and will route that information to us in the form that we call "known suspected terrorists," or

KSTs. We get that information daily from the FBI to update our records.

Do we have every single print taken by every single warfighter on the battlefield? Again, a work in progress, and it is something that we need to look at, from a governance standpoint, to make sure that the collection processes are standardized, that we, in fact, do get that information. But I will say this daily, we get this information, as I said before. That which the FBI cannot send to us, we can get in another direct feed from ADIS via a CD, oftentimes, but we have already identified individuals who the DoD was holding.

We have latent print examiners in our office. They were able to identify an individual by a fingerprint on the back of a piece of electrical tape that was used for an IED that was linked to an individual that DoD was holding. They were able to increase the security, based on that information.

So it is working. Does it need to improve? Absolutely, and that is something that Kathy is working very strongly on. Do you want to add to that?

Ms. KRANINGER. Yes. DoD, just on their side, has, obviously, had a lot of progress to make, in terms of their collection and standardization, and, certainly, without speaking for them, they have made a lot of progress on that end, so the data that was collected earlier in both theaters is being cleaned up, and, from a point forward, they have been very good about standardizing and making sure that the collection is what the screening community would need.

So that has been one-half of the effort. The other half of the effort, as Bob noted, is that there is certain information that the FBI actually cannot take, or will not take, for legal reasons. Admissibility is a much broader category, and we have access to, and authority to look at the other information that DoD has. So we have been working very closely with them to ensure that we can get the right populations from them and be able to use that for screening, but it is a work in progress.

Mr. ROGERS. Well, finally, the compatibility of the data that you get from DoD and your system; are you fully compatible with DoD?

Mr. MOCNY. We are. We are.

Mr. ROGERS. No problem with format.

Mr. MOCNY. They collect through FBI standards. There is a standard collection process. If they collect only two fingerprints, our system can accept that. The FBI can accept that as the latent print, but we can accept two, one; it does not really matter. But the format is very compatible. As I said, we get them daily, we run them daily, and we get hits on a regular basis.

Mr. ROGERS. And they are fully cooperative?

Mr. MOCNY. Absolutely.

Mr. ROGERS. Thank you, Mr. Chairman.

Mr. PRICE. Ms. Roybal-Allard.

EXIT SYSTEM

Ms. ROYBAL-ALLARD. Thank you, Mr. Chairman. I just wanted to do a little bit of a follow-up on the exit system because you said you have been moving forward, and you are ready to implement it, yet there was a GAO report in 2008 that stated that "DHS still lacks the crucial capability," and the report states that "the De-

partment's poor planning risks repeating failed and costly past exit efforts," and it went on to recommend that DHS conduct an analysis of costs, benefits, and risks for proposed exit solutions before committing even more money to the development of such a system.

My question is, have you gone through that process, in terms of the planning, before you started to move forward on what you are doing now?

Mr. MOCNY. Yes. As part of the proposed rule that we published last year, we did do a cost-benefit analysis of six different scenarios. We looked at ways the government might do it, ways the airlines might do it, various ways that the government might do it. And so, looking at those various scenarios, and costing those scenarios out, we went with part of the proposed rule.

So that does, I believe, satisfy the GAO's recommendation that we do an analysis first before we actually move forward. Having done that, and in addition to the two pilots that we are going to be running this year—that is why I am saying, from a technical perspective and from a legal perspective—we are poised to move forward on the exit system.

TWO-PRINT AND TEN-PRINT DATA COLLECTION

Ms. ROYBAL-ALLARD. Okay. Then also, with regard to the fact that you are now capturing all 10 fingerprints, my question is, what is going to happen to all of the data collection, over the years, of the two prints? Is that still usable, or does it get destroyed?

Mr. MOCNY. It is an amazing challenge, but yes, it is usable. We do have to ten-print those individuals who we have two-printed in the past, so if we have not seen that person for a while, they would go through the new ten-print process, but the two prints are used today. There are many individuals who only come infrequently to the U.S., so we would use that information.

We have almost completed the ten-print deployment, we have a few places they go. So, in fact, some ports of entry are still using the two-print before the ten-prints get out there. The system accepts that. People can use that. It is just a more accurate way of doing it, and when we get to full deployment, by the end of this year, then everybody will go through a ten-print process when they come in for the first time and then, oftentimes, they will only need a slap of one hand in subsequent visits to the U.S. So it is a more efficient system and a more accurate system.

BIOMETRIC STORAGE SYSTEM

Ms. ROYBAL-ALLARD. Okay. Finally, the U.S. Citizenship and Immigration Service is required to submit the fingerprints of applicants for immigration benefits to the FBI for criminal history checks, and, unfortunately, as often happens, an immigrant's case is not adjudicated within the 15-month window, and his or her fingerprints must be taken again.

This practice, according to the CIS ombudsman, is very costly for the agency and also very inconvenient for the applicants.

To address the problem, DHS, I understand, is rolling out the Biometric Storage System, which is a repository of biometric information which enables the Department to save and re-send images of applicant fingerprints.

My question is, if you could just give us an update on how this is working and if you have encountered any problems with it.

Ms. KRANINGER. That particular program and that particular system were actually stopped, but the issue that you raise is one that is very much on the forefront of our attention.

Certainly, we want to make sure that we are improving USCIS processing time so that they are able to efficiently operate and that this is not an issue. So that is certainly the goal of the modernization of USCIS's transformation process, and we are looking at the ways to improve that.

The second half of this, though, is also an FBI policy issue with respect to the recapture of fingerprints and then resubmission. So we have had conversations with them to see what can be done about that policy over time. There are really two halves to this. One is certainly getting our better processes in place and transformation and then also working with the FBI closely to make sure we can make this a little easier.

Ms. ROYBAL-ALLARD. Okay. Thank you.

Mr. PRICE. Mr. Carter.

PILOT PROJECTS

Mr. CARTER. Thank you, Mr. Chairman.

You mentioned that you have two pilot projects that you are working on right now on exit.

Mr. MOCNY. Correct.

Mr. CARTER. How many pilot projects have you already worked on on exit and decided that they did not work?

Mr. MOCNY. Starting in 2004, actually, through 2006, where we looked at a couple of different ways of capturing biometrics, using a mobile device and using kiosks as well, and then a combination of kiosks and what we call a "verifier," but it was a mobile device as well. We ran those for about two years or so.

What we found is the technology worked quite well. We could take the fingerprint in the middle of the airport, transmit that fingerprint, and even get a response back, should we desire that.

The issue was the process. Working with the airports, as you well know, going through airports today, it is a mall now, so they want to save the retail space for the profit angle of it. So we put it in areas that were not easy to find. So people, where they could find it, did use it. It worked, but it was difficult for the traveler to find it.

So what we concluded from that was that the exit process is going to have to be part of the traveler's continuum, either at the check-in counter, at TSA, or at the gate itself, and it is the TSA pilot and the CBP, Customs Border Protection at the gate; those are the two pilots that we are going to run in the May-June timeframe.

BORDER CROSSING BY CAR AND ON FOOT

Mr. CARTER. I was at the border in Laredo about 18 months, 2 years ago. I stood there on the bridge and watched them bring people across. My memory sort of fails me, I guess, but, as I recall, they had people who were frequent crossers of the border, and they had had the fingerprints and all of that stuff done.

Some of them, they would stop in a car, see their card, and I do not know whether they had a print thing that took their fingerprint as they went across, or what the situation was, but they moved pretty rapidly across the bridge, much more rapidly than I would pass through at the airport.

Mr. MOCNY. Uh-huh.

Mr. CARTER. Then I stood and watched the walking people that were supposedly frequent visitors that made more than a few crossings. They had a fingerprint pad, electronic, and a card.

Now, I do not recall, and maybe you can answer this, whether those people walked through a magnetometer, whether they had their bags that they were carrying inspected or run through an x-ray unit, but I do not think they did. Can you tell me whether or not they do?

Mr. MOCNY. What I believe you are referring to, in the first instance, is the SENTRI program, which is across many ports of entry on the southern border. These people are prescreened, so they go for an actual interview with a CBP officer. They have their fingerprints taken, they go through a vetting process, and they get a card that is then used in special lanes in Laredo, El Paso, Otay Mesa, San Jacinto, and a couple of other places.

That is a very effective program for frequent travelers because, again, they are prevetted, and the Customs officer has a better sense of who that person is. What happens is it uses radio frequency technology, much like the Western Hemisphere Travel Initiative is going to be using. So it prepopulates the screen. The officer knows who is in the car—they have been vetted, they are green, they are good to go—and lets them through. That makes for a quicker inspection.

On the second scenario, what I believe you are referring to is probably just a regular US-VISIT person coming through the process, where they go through a fingerprinting process as part of the policy where, again, anybody coming under a visa or coming using a border-crossing card for more than 30 days or more than 25 miles.

So that is the standard US-VISIT process, and, frankly, while they may not go through a magnetometer in every instance, they are certainly screened by a Customs and Border Protection officer. They can have their bags looked at, at any given point, if the officer believes that to be the case. So there is a rigorous screening program on the southern border for anyone going into the United States.

Mr. CARTER. I asked the guy that was with me. I said, "Where do you think this person is going?" and they said, "Well, probably just right across the border here to do shopping and so forth."

I said, "How do you know?" He said, "We do not know."

I said, "How do you know when he comes back?" "We do not know when he comes back."

"Could he go all the way to Canada?" "Yeah, he could go all the way to Canada. It would not be a problem."

And what really struck me was, I went through the mess at the Houston Airport, although that is not my port of getting on the airplane normally—I get on the airplane in Austin—but I had the iris scan, I had the fingerprints done, and all that stuff.

It is supposed to speed along the process, but it does not. You still get your bags searched. You still have to stand in line to go through the magnetometer and all that stuff, and yet people are crossing the southern border in a wave almost. I mean, I find that curious. Do you have any comments?

Ms. KRANINGER. The distinction, just in terms of domestic screening processes by TSA and border entry, are real. One certainly is just the statutory responsibility we have to screen every individual and every bag that is actually going to get on a commercial aircraft. So that is the distinction that we would make. Not to say, though, that CBP cannot. CBP actually does do physical screening where they feel it is necessary. They are trained law enforcement who are conducting an inspection. They do generally ask someone where they are going. But we appreciate the point, that is absolutely the case that once someone enters, we can only rely on what they told us.

But there is a separate regime when it comes to domestic and international air travel, when someone is leaving the country from—

Mr. CARTER. I understand that. It just seemed like one was very particular, and one was very lax. In other words, you could have been carrying a suitcase full of plastic explosives across the border, and nobody was doing anything about it, it looked like to me, because I sat there for about an hour and watched them go by, and nobody's bag got looked at while I was there, and some of them were carrying lots of big things across the border. I just sort of found it curious, as we look at national security, that that is the way it would operate. I think you need an exit policy. Thank you.

Mr. ROGERS. Would the gentleman yield?

Mr. CARTER. Yes, I yield.

BORDER CROSSING BAGGAGE CHECK

Mr. ROGERS. Well, the fact that 90 percent of the cocaine entering this country comes through Mexico, obviously, across the border; some of those bags are containing substances that we do not want here, the bags you are talking about that go unchecked.

Mr. CARTER. It could be.

Mr. ROGERS. Right or wrong?

Mr. MOCNY. That is always possible. I do know that CBP every day encounters individuals, and they will confiscate cocaine, marijuana, and others. Border Patrol does the same thing in between the ports of entry.

It is a problem, no doubt. Is it universally appropriate to every single case? Obviously not.

Mr. ROGERS. Well, with the drugs coming into the U.S. and the guns going out of the U.S. to Mexico, it is an open sieve, open.

Mr. PRICE. Mr. Farr.

VISA WAIVER PROGRAM

Mr. FARR. I find these discussions fascinating because I think I have just felt, ever since 9/11, that having to go through this harassment at the airport is so un-American and so contrary to our right to freedom of travel, that it seems to me that once all of that

screening was put up, it was our government saying, "We do not trust you, as an individual."

I have hoped that maybe this all moves to some technology that we do not have to have the human interaction, but it is interesting that TSA now, their whole point is about human interaction. It is the interview, when they look at your eyes and look at you, that they really get back to this being able to determine by interviewing people whether there is something suspicious, more so than all of the equipment that is out there.

I had a couple of questions. How many countries now are in the visa waiver program?

Mr. MOCNY. Twenty-seven.

Mr. FARR. And how many of those 27 countries require for Americans coming into their countries, they have to do the same thing that we are requiring here?

Mr. MOCNY. Some of those, Japan and the U.K.—

Mr. FARR. Two out of 27?

Mr. MOCNY. Pardon?

Mr. FARR. Two out of 27?

Mr. MOCNY. Two right now, but the European Union is moving to a biometric visa issuance process, too, so all of the European Union countries—many of whom are in the Visa Waiver Program—in fact, the bulk of them are from Europe—will be implementing a biometric screening program for anybody required to have a visa to go to the EU.

EXIT STRATEGY

Mr. FARR. And will they have an exit strategy as well?

Mr. MOCNY. They are working on one. Japan already has one, and the EU has some, in various stages, in various countries, but the concept is to move to a biometric entry and exit process.

Mr. FARR. It is very hard to drive and walk in Japan. It is an island. They have this program that the other Members were talking about and bifurcated. We have this border where most of the people coming into the United States do come by land, from Canada and Mexico, far greater than all of the air travel.

Is there a plan to do an exit strategy for all of the people leaving California going into Mexico?

Mr. MOCNY. As part of the comprehensive exit process, yes. It is a concept that we have put forward. We have not gotten it fully developed yet, but we do have a report that talks about how you would implement a land-border exit for pedestrians, for vehicles, for trains and buses. So there is a process in place to actually implement that.

Mr. FARR. You would have traffic lines backed up to Los Angeles.

Mr. MOCNY. It is certainly not an easy challenge, but there are many locations where people walk across the border, and so you can capture their information, and there are many ports of entry which are one, two, and three-lane ports of entry, which makes it easier to capture the information.

Mr. FARR. There are 27 lanes in San Jacinto.

Mr. MOCNY. Absolutely. So that is something we are going to have to—

Mr. FARR. They are all backed up.

Mr. MOCNY. There is no easy solution. I will grant you that.

Mr. FARR. It is a two-and-a-half-hour wait coming into California, on a daily basis, even when you are in a fast track, to get through that. So if you had to do that going out, I think you would create something that people—when the enforcement is worse than the problem, you create a nightmare.

I am just interested. Why do we need an exit strategy?

Mr. MOCNY. We need an exit strategy; because number one, the Congress has mandated that in several statutes.

Mr. FARR. But why do we need it? Not just Congress mandates—

Mr. MOCNY. I understand. We need to know who is in our country and who has left the country. We need to be able to rationalize the 12 million people who are here in the country illegally, as estimated, how they got here, many of whom came under the visa waiver program and never left; many of whom came with a visa and never left.

Mr. FARR. When you discover that they are CEOs of high-tech firms and leading university professors and perhaps leading citizens in our community, and they came here on a visa, went to the university, got a degree, and stayed, what are we going to do about it?

Mr. MOCNY. Again, we need to know who is in the country and who has left. Once we know who has not left, then we can have our Immigration and Customs Enforcement take the appropriate action. Again, there is not a universal panacea, but it is a way of building integrity into the immigration system.

People have come to the U.S., exploited our immigration laws, and, therefore, we have to build some integrity into the process to make sure that we have some control over our immigration.

Mr. FARR. For 200 years, we never did this, and we know we have 11 million people. We do not even know how many people are staying. I do not see why we need an exit strategy. There are just so many loopholes in it and exceptions to it that it seems to me a waste of money. This is a job you have been doing since its inception, right?

Mr. MOCNY. That is right.

Mr. FARR. How long does it take to work yourself out of a job? No further questions.

Mr. PRICE. All right, Mr. Calvert.

INTERACTION WITH E-VERIFY PROGRAM

Mr. CALVERT. Thank you, Mr. Chairman. I think I will take a different tack on this, Mr. Chairman.

I understand why we need an exit policy. I was at Disneyland a few years ago in Florida, and I entered there, and you put a finger in, and, you know, I was wondering what the heck that technology was at the time—this was five years ago. And when I left, I put my finger in, and later on I talked to an executive at Disney Corporation, and he said, that is right, we know who you are when you come in, and we know when you left. And I do not know how many people go to Disney World every day, but it is significant amount of people.

In Japan, as you know, their exit strategy is primarily eye scan. It takes approximately one second as you walk through the turnstile, the Japanese can know who came in and who left. It is a very efficient system, and the systems are getting better every day.

And in respect to Mr. Farr's line of questioning, you know, the United States has changed over the last 200 years. We now get 90 percent of the methamphetamine that come into the United States comes across the border. We have a significant crime problem along the border, both people leaving the United States, as Chairman Rogers mentioned, and smuggling weapons into Mexico, and the other way around, smuggling these illicit drugs into the United States, and right now we have hundreds of thousands of people that, unfortunately, are out of work in the United States because of the economic situation in this country, and some of those people who are here illegally are taking jobs away from people who would love to have those jobs.

So I believe that we need to have a system that works, and I congratulate you on the progress you have made, though we would like to see more progress. And in that I was the original author of the program that is now being implemented as a volunteer program called "e-verify", and I wonder what your interaction with that program is, if any.

Mr. MOCNY. We do not have any within US-VISIT. There is no biometric involved with either other than a photograph.

Mr. CALVERT. I see, so the so-called photo tool that is now attached to that system?

Mr. MOCNY. Correct.

BIOMETRIC IDENTIFIER ATTACHED TO SOCIAL SECURITY CARD

Mr. CALVERT. Do you think it would be useful at some point in the future as this technology continues that a biometric identifier be attached to Social Security cards?

Mr. MOCNY. You are asking my opinion? I think, as stated earlier, you know, biometrics does add integrity to any identification process, and at the same time it is not a silver bullet. So you have to weigh the costs and benefits of it, and the ability for the various companies to utilize this information. But as you well pointed out, if Disneyland can do it, if we can do it worldwide, if the Brits can do it, it is probably something that is doable. It is, of course, a policy question as to how we implement that with respect to Social Security cards.

NUMBER OF INDIVIDUALS PROCESSED EACH YEAR

Mr. CALVERT. How many individuals does US-VISIT process each year, approximately?

Mr. MOCNY. Each year?

Mr. CALVERT. Each year.

Mr. MOCNY. In the range of about 25 million, I think, a year.

Mr. CALVERT. Twenty-five million people. So the problem right now you are identifying the 25 million that are coming up, but we do not really know how many are leaving. That is an accurate statement?

Mr. MOCNY. From a biometric side, you are right. Again, we work with the biographic side so that we do capture enough infor-

mation to give us a pretty good sense of who has not left the country. Again, we get that acceptance report every day, but the biometric would add significantly to the certainty of that.

NEXT EXIT PILOT PROGRAM

Mr. CALVERT. You mentioned these pilot programs and some discussions about that. Now, where is the next pilot program going to take place?

Mr. MOCNY. For the exit?

Mr. CALVERT. Yes.

Mr. MOCNY. We are going to have one in Chicago and one in Detroit.

Mr. CALVERT. One in Chicago and one in Detroit. Around the Windsor Bridge area, that type of?

Mr. MOCNY. No. This is for air exit so it is going to be at O'Hare for Chicago and the Detroit Airport for—

Mr. CALVERT. What port of entry into the United States receives the highest traffic?

Mr. MOCNY. Which port of entry receives the highest traffic? Probably San Diego and/or El Paso.

Mr. CALVERT. Depending on you—

Mr. MOCNY. Yes, right.

EYE SCAN TECHNOLOGY

Mr. CALVERT. Is there other technologies other than, and I know there is a 10-fingerprint scanner, which is quicker to use, is the eye scan the quickest to use or is the—what technology out there or what technology do you perceive in the future that may be utilized to move this process quicker?

Mr. MOCNY. We are actually looking at iris scans and facial recognition as well. Iris scans really is a promising biometric for us because it is hands off. It is highly accurate, and it is very quick, and you can do it on the move. You do not have to touch anything. The only issue with that obviously is we want to keep the fingerprint as the base biometric because that verifies criminality. So once we have established, and we are looking at a process which would include all 10 fingerprints, the face, and then the two irises and then process that as appropriate.

In some cases, it is better to use the iris given the scenario we have, possibly using that for exit control even at the airports because people do line up and walk through queues and tunnels where they can be easily captured. So we are looking at multi-modal, not only from a facilitation standpoint, but from a security standpoint because, again, they are going to try to thwart the fingerprint process. So we have to kind of mix it up; use what we call multi-modal—face, fingerprint, iris, and the next biometric—to make sure we are verifying their identities.

Mr. CALVERT. A final point, Mr. Chairman. I have always said to my friends since I live near the border as many of us do, that we can either be proactive about solutions to this problem as we are doing, or something is going to occur along the border, not with Mexican nationals, I do not think that is the problem, but with someone else that enters the United States, and then we will react,

and the government, when it reacts, tends to overreact, and then we will have a more difficult problem that we have to deal with.

So with that, I commend you on the job you are doing, and look forward to more progress. Thank you.

Mr. PRICE. Thank you. Mr. Culberson.

POTENTIAL IMPACTS ON RFID ENABLED DOCUMENTS

Mr. CULBERSON. Thank you, Mr. Chairman. This is really timely and important, and really appreciate what you are doing. I think that about two years ago the FBI director went to the office in San Antonio and congratulated them on their work in breaking up a smuggling ring that had actually snuck Hamas terrorists into the United States, and I think we have also documented that there has been Hezbollah terrorists have come in, and speculation—no absolute confirmation about al-Qaeda, but there is no question they are using the southern border, the ports of entry, the northern border to sneak into the United States, and that we as a country have absolutely got to use this technology, and good law enforcement techniques, just good old-fashioned boots on the ground that is working so well in the Del Rio and the Laredo sectors in securing those sectors using a very successful and very popular program called Operation Streamline, a zero tolerance policy.

But I wanted to ask in particular about the—zero in on the subject of the hearing today, that since we have already got—Congress has given hundreds of millions of dollars to DHS to build the physical and IT structure to read the travel documents under the Western Hemisphere Travel Initiative, and we have got travelers who have—a million travelers who have paid for the RFID-equipped cards in 13 ports of entries that have gone through the trouble and expense of installing the equipment to read them.

Could you talk about what could be the impact on the Department and the traveling public if there were any major changes to the program at this stage?

Ms. KRANINGER. Well, the biggest change will be coming, actually, June first of this year with the actual compliance date for having a secure document when you are entering the United States for U.S. and Canadian citizens, who this primarily affects. We are actually very excited about this because we really see it as a huge facilitation gain. As was noted before, the Senti Program has done a lot, and the NEXUS program on the northern border, to really move through individuals who are already identified to present to the CBP officer the information about that person on the screen, including a photograph. So there is a biometric component to this, including the photograph. They can have done quick checks done against wants and warrants, and the terrorist watch list, just as the car is pulling up, and actually know who is going to be in that vehicle and process them quickly and efficiently.

So we do expect and actually have seen gains in exactly that way, and the more individuals who have RFID-enabled documents the better it is going to get.

Mr. CULBERSON. So on June 1, how many ports of entry do you expect to have that in place?

Ms. KRANINGER. We have the top 39 ports of entry targeted to actually outfit the RFID readers in every lane in-bound and that will be completed before that point.

Mr. CULBERSON. So by June 1 you are going to have 39 ports of entry up and running—

Ms. KRANINGER. Yes, sir.

Mr. CULBERSON [continuing]. With read the RFIDs. Terrific. I know U.S. Visit was originally seeking competition for the U.S. entry program and getting the biometric equipment because you did not want to be held hostage to one supplier. Can you talk to us about your future plans for seeking additional sources for the biometric equipment and for other similar programs?

Mr. MOCNY. Absolutely. There is a limited number of companies out there that have this type of equipment. Before biometrics, it was about fingerprints and it was law enforcement-related. And you have basically four companies in the world, two of which are foreign, and so what we need to do is work with industry, which we have on a regular basis. We provided you some pictures up there, and the fingerprint device that we demonstrated to you, that did not exist three years ago. We had industry in our building, and told them that the flat fingerprint devices were too slow, too non-user friendly, and too large actually to put on a CBD officer's desk. And so we gave them a challenge to come up with something not bigger than 6" × 6" × 6"—and in about eight months we had the first prototype, and shortly thereafter, we had a couple more.

So working with industry, we need to encourage them in this field, not only the capture devices, but in the biometric processing in and of itself.

We talked about iris scans a little while ago. That was a very nascent program just a few years ago where the UAE has been using it very robustly for awhile now. It still had its issues as far as patent controls and all. That patent has now expired, and we are seeing more and more companies moving in that direction.

So I am very encouraged with what we are seeing from an industry standpoint. I think more needs to be done. I think, as more and more countries move to a biometrically-controlled border management system, as we talked about, we need to encourage that competition because we cannot rely on one or two companies, again, who have foreign ties to be managing our biometrics on a day-to-day basis.

PASS CARD FOR THE MEXICAN BORDER

Mr. CULBERSON. Now forgive me if this has already been asked earlier, but I also wanted to ask about them, again with the Western Hemisphere Travel Initiative, is DHS planning to use a card form for the PASS card for the Mexican border crossing card? And if so, what happens to the fingerprints that are on the current card? Is DHS planning to ignore the statutory requirements that the fingerprints be on the card?

Ms. KRANINGER. Well, with respect to the border crossing card, actually the State Department has issued 125,000 of the new cards already. They are RFID-enabled, and again provide the same benefits that I discussed with respect to secure documents, which is a major gain.

The collection of fingerprints is still very much a part of the border crossing card issuance process. We do actually use and currently check through US-VISIT IDENT to see if there are any law enforcement-related hits against those fingerprints, and again, the results of that are shown to the CBD officer when they process somebody who is entering with a border crossing card. So fingerprints are still very much part of the process.

From a security standpoint, we have not wanted to put the fingerprints actually on the card itself, and I am not sure—that has changed. Yes, that has changed. So the border crossing card does not actually have them on the card itself.

Mr. CULBERSON. Right.

Ms. KRANINGER. But they are associated in the file, and I do not want to speak for the State Department.

Mr. CULBERSON. A RFID tag will trigger it?

Ms. KRANINGER. Yes, sir.

Mr. CULBERSON. Thank you, Mr. Chairman.

ACCURACY ISSUES

Mr. PRICE. Thank you. Let me turn to the question of accuracy because, as you well know, these systems can have very dire consequences for individuals if they are caught up in an inaccurate match. They can also have dire consequences for security if the matches do not show up. There are two kinds of common errors as I understand it with biometric ID systems: the false match errors where an individual is matched with another's biometric, and the false non-match errors where an individual whose identity is recorded in the system is not matched with their biometric data. I know you worked to minimize or to maybe balance those two kinds of errors.

Ms. Kraninger, I wonder if you could tell us how the Department works to minimize such errors? What kind of ongoing efforts do you have underway?

Some of this is a matter of readings changing over time. As faces age and as fingerprints get worn away by labor or chemicals or injuries, whatever, so it is partly, I guess, a matter of ensuring that the biometric data is up to date. It is also a matter of continuing to refine the accuracy of the system.

Finally, what if an individual does get caught up in this? What kind of opportunities does that individual have to understand the problem, first of all, to be informed about it, and to take efforts to take action to correct their biometric data in the system?

In an unrelated area, we hear the stories of the watch lists at the airport where people simply cannot get themselves off that watch list, and they get pulled aside for special screening week after week after week, and it is very slow in getting fixed. What about this situation? If an individual is caught up in a false match or false identification, does that individual have any resource if the problem is not quickly fixed?

Ms. KRANINGER. Mr. Chairman, you went exactly where I did when you mentioned the watch list because the truth about the biometric situation, frankly, is that it helps us significantly in the area where we have a harder time actually matching the [biographic] information. When all you have about a person is a name, and you are matching that against a watch list, the opportunity for

more matches is there, and then, of course, you have to actually adjudicate those matches and determine if it is the real person.

Mr. PRICE. No, I understand. I understand that your system is far more accurate and, of course, that is the point of having the biometrics. However, we have background from GAO that you are not without error rates of both of the kinds that I mentioned.

Ms. KRANINGER. Yes.

Mr. PRICE. And presumably individuals are caught up in that.

Ms. KRANINGER. Absolutely. So with respect to redress opportunities, we did establish, I guess now two years ago, the DHS TRIP process, so that any traveler who is affected by a misidentification, or otherwise believes that they were improperly processed, whether it was by CBP in the US-VISIT process, or CBP in general, or TSA, or USCIS even in an immigration benefits process, where they think they have an issue related to watch list, they can submit that request to the DHS TRIP office. It's the central office managed by TSA on behalf of the Department. Those requests are then adjudicated in a uniform way across the Department so that we can make a determination whether the information is related to the watch list definitely or in another place, so that we can address that individual's issues and either correct their records or provide them some redress.

There are limitations on the biographic side. That is certainly why we are setting up Secure Flight and why we want to collect more than just a name, and therefore have required full name, date of birth, and gender as part of that process.

You brought up a very valid point though about biometrics too, no system is perfect. So we do have the situation where, as you noted, fingerprints that deteriorated or facial images that are not to quality. We are certainly doing things on that front as well that I would defer really to Bob in detail.

Mr. MOCNY. Yes, it is something that we take very seriously. We want to make sure we do not miss the bad guys but that we do not inconvenience the good guys. And so it is a matter, as you indicated, kind of setting up thresholds within the system to do just that. We work every single day to make sure that we have an accurate system. The 10-prints will help us get there, but other biometrics will even help us get there with higher accuracy, if we are adding iris scans to the process.

You should know that if there is a false match, we do have fingerprint examiners 24/7 who look at that information. So if a person provides fingerprints to the State Department, consulate overseas or port of entry—and there is “a hit”, within a couple of minutes we have a fingerprint examiner looking at the candidate print and the one on file, and making a determination of whether or not that is a true hit or not, again what we call gray area hits with those very, very few who are sent back into secondary to resolve that.

So we take that seriously because we want to make sure that we are moving people through the process and not inconveniencing them and not falsely identifying them. And to date, we have not had such an issue. Again, we have humans who do actually look at this on a daily basis, about 50,000 a week actually.

Mr. PRICE. Is there any way of tracking improvements in error rates of those sorts?

Mr. MOCNY. Absolutely.

Mr. PRICE. Do you have information you can provide us?

Mr. MOCNY. We can. We can give you good detailed information, you know, technical fixes that bring that false match right down to something that is very, very manageable. But again, people are looking at this on a day-to-day basis very, very bright people—much brighter than me—who are looking at algorithms and ways in which we can do this better and better, so we can actually provide that to you.

Mr. PRICE. Thank you. Mr. Rogers.

EXIT SYSTEM ADD TO US-VISIT

Mr. ROGERS. Thank you. To follow up on Mr. Farr's line of questioning about whether or not we need an exit system to the US-VISIT Program. If we do not have an exit system, there really is no way to know whether or not a person has overstayed his or her visa, right or wrong?

Mr. MOCNY. That is correct. If we do not have an exit, you are right.

Mr. ROGERS. And as a result of that, 40 percent of the 12 million illegals in the country now, I am told, 40 percent are here because they simply overstayed a legal visa, right?

Mr. MOCNY. That is correct.

Mr. ROGERS. Came here legally, overstayed the visa, and you have not caught them. So if you assume that the country needs a border and citizenship, then you have to say that we have to have a system of allowing visitors in for a limited time and then knowing when they leave. Is that right or wrong?

Mr. MOCNY. That is correct.

Mr. ROGERS. As a matter of fact, one of the big reasons why we have hopefully secure borders and checking people who come and go is to be sure that we keep out people that want to do us harm, right or wrong?

Mr. MOCNY. Right.

Mr. ROGERS. And I would remind you that four of the 9/11 hijackers were visa overstays, and that two of the World Trade Center bombers were visa overstays. So it matters whether or not we know a person is here on an overstay or not. But, you know, I think one of the big reasons why the efforts at exit control have not worked, like the kiosks in airports and the like, is that the exitor has no real incentive to let us know he has left; right?

What if we changed the rules so that if a person who is in the country on a visa, when they leave the country if they do not let us know that they have left, when they try to come back a second time they are not allowed? Would that not be an incentive?

Mr. MOCNY. That would be, and in fact, that is the case again from a biographic side is how we capture information. If someone leaves the country and they either have not reported it say at a land border, we would have a record of that biographically in the system to say that they potentially overstayed the visa.

The problem is it is difficult to enforce because people may have left the country, and we may not have known about it because we

do not have an exit system. So from one side of the standpoint, it is a facilitative measure to make sure that that person who legitimately left the country and checked out can come back into the country and be able to prove I left the country. Right now we think people may not have left the country, and that can become an issue for the traveler. So by having an exit system, it does help on the enforcement side, but it also helps the traveler to confirm the fact that they left legitimately, and it lets us know with more definition that that person did not leave on time.

Mr. ROGERS. Well, I am just trying to figure out what kind of an incentive we can put on the person who is coming and going to let us know when they have left the country. But as you say, if there is no mechanism by which they can let us know that, then it is not a good answer.

Mr. MOCNY. Well, it is certainly something we are looking at as far as, again, when we get to the land border because it is much more difficult to do so. So we want to provide a process by which someone can tell the officer, I have left the country and I have left on time, but we also want to know that that person left and did not leave on time, and because there is no way to watch those people leaving the country, there is no way to enforce that fairly and legitimately.

Mr. ROGERS. Well, if we could follow Disneyland's example that Mr. Calvert told us about, if here was a way that you can construct an exit system that is built on that simple procedure of putting your thumb in a box before the let opens to let you out, then we will have achieved the magic exit system.

Mr. MOCNY. And that is a challenge and that is why we need to work with industry. Again, I can probably paint you a scenario for people who walk across the border, and people who drive through one or two lane-ports of entry on the northern border. But to handle the people leaving through San Diego, El Paso, Detroit—some of the larger places, and some places where they drive 45 miles an hour across the border, to have that person place a thumb-print or whatever else and do it safely, that is our challenge. So we need to work with industry to either change the paradigm, or have them report back when they get to the other side of the border. There are different ways for looking at how to handle that, but I do believe we can put something in place.

Mr. ROGERS. Well, I charge you and challenge you again to come up with a system that—surely in this modern technological age in which we live you can do that, and I have been to that San Ysidro border. Is it 12 lanes each way?

Mr. MOCNY. It is 24 in and four out, four or five out.

Mr. ROGERS. It is amazing.

Mr. MOCNY. Yes.

Mr. ROGERS. And the traffic was backed up two or three miles, and they are going through it at 30–40 miles an hour through the check-out point, so I understand the complexity and the volume and the size of the flow that you are trying to carry. Thank you.

Mr. PRICE. Thank you. We obviously have votes on the House floor, so we will plan to close out with Mr. Farr.

GLOBAL ENTRY PROGRAM

Mr. FARR. Thank you, Mr. Chairman.

Mr. Rogers is right. We need to make sure that the bad people who snuck into this country or gotten in, I think that is what law enforcement is all about. My concern is that we have set up a separate department just on exit when we have the border customs and border patrol to do entry when it seems to me they ought to all be combined.

It also seems to me that there is a priority here. We did grandfather people in who came in here undocumented in the eighties who came through the amnesty program for farmworkers and it worked very well. What I am concerned about in a global strategy. We have also got to be a country that is not looked at and hated by the rest of the world because the business community, the traveling community of those countries want—you know, want to come here, want to be treated like we would want to be treated in their country, and I think we end up, just like this agricultural war that we have, we are trying to keep things out if they are threatening, and it is just that we have got to be smart about this. That is my point. I think there are ways of doing it.

Let me just ask this one question about the Global Entry Program. Can you provide me a timeframe when DHS will allow the international visitor from The Netherlands, Germany, and the U.K. to use the Global Entry Program?

Ms. KRANINGER. Actually, the Dutch pilot will be the first one, and we are looking to launch that very soon, in the spring, and the others will follow soon thereafter.

Mr. FARR. Well, does the pilot mean then that all of them from The Netherlands can come or is it just a few, or what is it—the question is really when is the timeframe when they will be in place for all those countries?

Ms. KRANINGER. The Netherlands are starting first and it is their similar program that will actually allow those members of that program to come in through Global Entry. So what we have to do actually is share information on the individuals in Global Entry, the individuals in, I think it is called Privium. So that is going to take a little bit of time to do quick checks on those individuals, share that information, allow them to enter. But the first person can enter in the spring when we get that moving. We only say pilot because it is the first of the international phases, so the U.K. and Germany will come soon thereafter. We will have to finalize agreements with them, but this should all work very well, and will happen this year.

Mr. FARR. This year. Okay, thank you.

INTERNATIONAL REGISTERED TRAVEL PROGRAM

Of the International Registered Travel Program, which we have for Canada, why do we not have it for Mexico?

Ms. KRANINGER. We actually do with SENTRI, and so Mexican nationals actually can participate in SENTRI. What we are doing with CBP as well is saying, NEXUS, SENTRI, Global Entry, when they were all established, have very similar requirements for the background check that we conduct, the information that is pro-

vided, and how we process those people. So what we are doing as well is letting them begin to use that same benefit through air that they use today on land. So we are actually in some respects—

Mr. FARR. So it is in place for Mexico as well as Canada?

Ms. KRANINGER. Yes. Mexico through the SENTRI Program, Mexican nationals, and the Canadians have the NEXUS Program.

Mr. FARR. Okay, thank you.

Mr. PRICE. Thank you, and with that we will draw this hearing to a conclusion. We do have more questions I feel certain, and we will submit them to you for answers then for the record.

In the meantime, thank you for the good work both of you do, and for being here today and helping us prepare for writing next year's bill.

Mr. MOCNY. Thank you, Mr. Chairman.

Ms. KRANINGER. Thank you.

Mr. PRICE. The Subcommittee is adjourned.

QUESTIONS FOR THE RECORD SUBMITTED BY

CHAIRMAN DAVID PRICE

**Ms. Kathleen Kraninger, Deputy Assistant Secretary for Policy, DHS Screening
Coordination Office
Mr. Bob Mocny, Director,
United States Visitor and Immigrant Status Indicator Technology
Biometric Identification**

US-VISIT and Overstay Identification

Question: US-VISIT analyzes entry records to help ICE apprehend those who remain illegally in the U.S., and to enable CBP or the State Department to deny admission to those who may have overstayed but are now out of the U.S. However, without comprehensive exit data, US-VISIT must review thousands of records the CBP automated Arrival-Departure Information System (ADIS) identifies to determine whether a person departed, and if so, if they did so before their authorization expired. Last year DHS testified US-VISIT reviews only 10,000 of 17,000 in-country overstay records *each week*. As a result, in FY07 it did not check 365,000 records. How many overstay records did US-VISIT and its Data Integrity Group (DIG) receive in FY08 and to date in FY09, and of these, how many were not checked?

ANSWER: US-VISIT's Data Integrity Group reviewed 472,286 records of individuals who were potential overstays and who were believed to still be in the country (in-country overstay records) and 47,075 records of individuals who were potential overstays but were believed to have already left the country (out-of-country overstay records) during FY 2008.

To date in FY09: In-country overstay records – 166,521; out-of-country overstay records – 17,662

Of each of these, how many were not checked:

Category	FY 2008	FY 2009 (to date)
In-country overstay records	305,578	137,315
Out-of-country overstay records	151	1,496

US-VISIT uses intelligence prioritization by U.S. Immigration and Customs Enforcement (ICE) to determine which records to review manually for in-country overstay violators. At ICE's request, US-VISIT began reviewing Visa Waiver Program (VWP) in-country overstay records in January 2009. (ICE stood up its interior enforcement program for VWP violators at that time.) As a result of US-VISIT leads, ICE agents apprehended 715 foreign nationals who had overstayed in FY 2008 – a 110 percent increase over FY 2007. Furthermore, 1,441 adverse actions were taken to prevent inadmissible aliens from entering the United States – a 220 percent increase. These are the results of manually vetting just 6 percent of the total overstay records that U.S. Customs and Border Protection provides to US-VISIT.

US-VISIT also prioritizes its reviews of out-of-country overstay records based on the number of days the person has overstayed – focusing on those time periods which result in statutory inadmissibility periods for returning to the U.S. In FY 2008, US-VISIT created 14,276 overstay watchlist records for individuals whose overstays

resulted in one of these statutory inadmissibility periods. These watchlisted records resulted in 550 adverse actions at Department of State consulates and 891 adverse actions at ports of entry.

Question: US-VISIT prioritizes overstay reviews using risk-based criteria for countries and individuals of interest, and manually vets the top 10% it reviews; the rest are "batch processed". As a result of US-VISIT leads, in FY08 ICE agents apprehended 715 overstay aliens, a 110% increase over FY07, and 1,441 adverse actions were taken to block inadmissible aliens from entering the U.S., a 220% increase. These are results of manual vetting just 6% of the total overstay records CBP provides US-VISIT. How does US-VISIT use its risk-based approach to overstay review? Would it be desirable to review all overstay reports?

ANSWER: US-VISIT uses U.S. Immigration and Customs Enforcement (ICE) prioritization for in-country overstay record reviews and updates the countries of interest based on ICE intelligence guidance. US-VISIT also adds groups of countries to the in-country overstay review based on ICE enforcement capacity. US-VISIT manually reviews 100 percent of the in-country and Visa Waiver Program overstay records of ICE-based priority countries of interest. The remaining in-country overstay violator records are batch-processed for closures, and the remaining records are placed in the overstay review backlog.

As noted above, US-VISIT proactively reviews out-of-country overstay violator records, with a focus on the number of days the violator remained in the country past his or her term of admission. In FY 2008, the average number of days in overstay status for individuals encountered in an adverse action was 589.

DHS does not plan to expand to reviewing all overstay reports. Reviews are based on risk and ICE intelligence and any benefits, if any, from additional reviews are unclear.

Based on historical data for out-of-country overstay violators, it would not be a priority to review most overstay records for individuals who have already left the country, but had not overstayed by a period of 180 days or more. As noted above, when a person has overstayed by 180 days or more, they are statutorily inadmissible for a set period. When such out-of-country overstay records are verified, the DIG creates both biographic and biometric watchlist record in TECS (the biographic screening system used by CBP, USCIS and ICE) and IDENT. The exception to this rule is for Visa Waiver Program (VWP) travelers. Any period of overstay would render the individual ineligible for future travel to the U.S. under the VWP. The individual would have to apply for a visa.

Question: Last year the Department estimated it would cost \$14.6 million to check all overstay records. What is the current estimate?

ANSWER: US-VISIT identifies more than 17,000 records per week as in-country overstays. Of the 17,000 records, US-VISIT reviews more than 11,000 ADIS identified in-country overstays per week (9,000 through batch processing, 2,750 through manual vetting), leaving 5,250 records per week that are not reviewed. In the FY 2009 enacted budget, US-VISIT received \$5.7 million to manually review 2,750 records weekly (143,000 annually). To review the remaining 5,250 overstay records per week (273,000 annually), US-VISIT would require an additional \$10.9 million annually. This does not include the cost of additional ICE investigative resources.

The current estimate to review all overstay records remains approximately \$14.6 million.

US-VISIT: Exit

Question: Last year, DHS put out a Request For Information / Sources Sought (RFI/SS) Announcement to gauge the market for providing a US-VISIT biometric *land* exit solution. What was the outcome of this RFI?

ANSWER: To determine the available technology applicable for land exit, US-VISIT issued a Biometric Land Exit Solution/Sources Sought Request for Information (RFI) to the public in May 2008. Although US-VISIT received 27 vendor responses, only 21 of those proposed a solution for land exit and none of the respondents fully answered the RFI as requested. As a result, US-VISIT was able to make some assumptions about the maturity of the technologies and their applicability to land exit.

The RFI results imply that no current technology can solve the land exit challenge alone. Most products described in the RFI responses support an exit process where the in-scope traveler is a pedestrian or has disembarked from some form of motorized conveyance. Collecting biometric and biographic information from in-scope travelers in vehicles would require an infrastructure similar to the current entry process. Any viable solution will consist of a hybrid of processes, technology, and facility arrangements that could vary by port and mode of transportation.

US-VISIT conducted an in-depth technology assessment to provide another layer of insight into the technical feasibility of various solutions. Specifically, the assessment evaluated the technical feasibility and impact of various exit processing technologies across the pedestrian and vehicle solution scenarios. US-VISIT considered the three most mature biometric types – fingerscan, iris recognition and facial recognition – and evaluated each biometric for each scenario with various capture applications (namely kiosk, handheld, fob/card and remote sensor). The key findings were that fingerscan technology is currently the most technically feasible alternative with the lowest solution impact.

The RFI vendor responses were also mapped to the technology assessment for each of the preferred pedestrian and vehicle options. The intent was to confirm the feasibility of these options based on available technology and to integrate the findings.

Question: What is the status of discussions with Canada and Mexico on reciprocity in sharing immigration entry data, and prospects that DHS could benefit by a reduced need for collection of exit data? What is the status of discussions with Mexico on sharing data to reduce immigration fraud and cross-border crime?

ANSWER: DHS recognizes the potential benefit of reciprocity in sharing immigration entry data. The main place this could be of significant importance is at the land border as we already have long standing robust processes for air/sea with the carriers. Given this, Mexico is not a likely partner as they do not have the necessary infrastructure to collect inbound data at land.

DHS has had many discussions with Canada about the potential for an entry into Canada serving as an exit for the U.S. However, Canada has previously expressed concerns that they would not be able to provide the U.S. with data on Canadian citizens or residents. Given that this population forms the bulk of the data collection on land exit, the reduction in U.S. collection may not be significant. DHS plans to continue its discussions with both Canada and Mexico.

Discussions have focused on potential improvements to Mexico's processes. US-VISIT is working closely with the Government of Mexico under the Mérida Initiative to support efforts to incorporate biometrics into Mexico's immigration and border management processes. In an effort to bolster the effectiveness of the Mérida Initiative, US-VISIT and the Government of Mexico (including representation from the National Migration Institute, National Registry of the Population, Secretariat of Public Security, and the Center for Investigations and National Security) formed a bilateral technical working group.

US-VISIT – Migration to 10-Print Standard

Question: Mr. Mocny testified that 10-print scanners and readers are in overseas consulates and at nearly all ports of entry. What locations are still reliant on the 2-print systems and when will they migrate to 10-print?

ANSWER: DHS has deployed 10-print capability to approximately 292 sites (2,504 lanes), covering 97 percent of in-scope travelers. The migration from a two-print system to a 10-print system is scheduled to be completed in September 2009.

According to the most recent daily metrics provided by U.S. Customs and Border Protection, there are currently approximately 79 sites that are not using 10-print capability 100 percent of the time. It should be understood that 10-print equipment and capability has been deployed to these locations. Many of these ports, however, required or will require infrastructure improvements, such as circuit and network upgrades, to accommodate the larger bandwidth required by 10-print processing. Until these upgrades can be completed, many ports will continue to rely on two-print technology when processing requirements exceed bandwidth availability. Even with 79 sites unable to use 10-print processing all of the time, approximately 88 percent of all in-scope travelers are processed through the US-VISIT 10-print system.

Question: US-VISIT has been criticized for its reliance on fingerprints, in part due to association of fingerprinting with criminal records. Has public acceptance of fingerprinting grown, and how do you know? If it is more tolerated, is this due to how fingerprinting collection and validation is conducted, or because increased use of fingerprints by other countries has reduced stigma of the biometric? Will a “multi-modal” approach to biometric collection and verification further reduce public reluctance or resistance to the use of biometrics?

ANSWER: Although there were some initial concerns voiced about fingerprinting aliens, those concerns quickly subsided once the program was launched in 2004 and people from around the world found that the US-VISIT inkless fingerprinting process was quick, easy, and non-invasive. Since the program began, there have been only 516¹ redress requests received from the more than 71 million individuals who have provided their fingerprints to US-VISIT for entry into the United States.

Also, the private sector’s increased use of biometrics for consumer products and services indicates the public’s apparent acceptance of this technology. Disney scans the fingerprints of ticket holders entering its Orlando parks; many laptop computers come equipped with biometric scanners for security; and even biometric locks for houses and cars are now available.

Consumer surveys show a growing acceptance of biometric technology in general, especially with regard to homeland security. For instance, a survey of consumers in the United States and the United Kingdom released in 2007 concluded that:

- More than two-thirds (69 percent) of U.S. consumers and 92 percent of U.K. consumers would prefer that banks, credit card companies, healthcare providers, and government organizations adopt biometric technologies, as compared with other protection measures, to safely and quickly verify personal identities.
- More than one-half (51 percent) of consumers feel that technology plays a significant role in ensuring homeland security and point to biometrics as one of the best ways to improve protection, after physical security.

¹ 516 redress requests as of March 31, 2009.

- Nearly two-thirds (62 percent) of consumers would have greater trust in airport security with the use of frequent flier programs based on biometrics.²

In 2008, results of another survey of U.S. consumers were released indicating that most Americans are comfortable with biometrics being used for authentication. According to that survey, "More than 70 percent of respondents will trust banks and government agencies to ask them for biometric data for identity verification. Additionally, fingerprints nearly tied personal passwords as the primary preferred authentication method, 73 percent to 72 percent, respectively."³

When US-VISIT was first created, the Secretary of Department of Homeland Security made the policy decision to extend certain provisions of the 1974 Privacy Act to foreign nationals who are covered under the US-VISIT screening procedures. This means that, in many instances, personal information – including prints and photos – collected by DHS and stored by US-VISIT will be treated in the same manner as U.S. citizens. During the initial launch of US-VISIT, this fact was publicized to the international traveling public to measure them that they would be treated with as much respect as U.S. citizens.

Finally, a number of countries around the world are also adopting similar programs that use fingerprint technology. For example, Japan implemented a two-fingerprint biometric entry system in 2007. The United Kingdom is collecting 10 fingerprints from visa applicants and is testing fingerprint collection at its ports of entry. Australia has been a pioneer in facial recognition and is seeking to add fingerprints to its biometrics capability. Mexico is planning to modify its successful biographic identification system to incorporate biometrics.

How fingerprinting collection and validation is conducted and increased use of fingerprints by other countries both may play a role in the increasing acceptance of biometrics. The collection process is simple, convenient, and accurate, and more countries are incorporating biometrics into their immigration and border management systems.

However, US-VISIT suggests that there are at least two other possibly more important factors driving the acceptance and use of biometric technology for identification:

- The public's understanding that criminals, terrorists, and other dangerous people who are determined to circumvent U.S. security measures are becoming increasingly more sophisticated in their efforts and that we must therefore use more advanced technologies, such as biometrics.
- The prevalence of identity theft and fraud are also driving the private sector's use of biometrics to address these issues. Furthermore, as personal data is becoming more and more accessible with technological advances, both consumers and the Government are looking for solutions that ensure that personal data is protected from abuse.

The population traveling to the United States already experiences a multimodal approach during the visa application and port-of-entry processes, since both fingerprints and photographs are collected and used in the establishment and verification of the identity of an individual. In other countries, such as Canada, an iris scan is used in the biometric collection for its trusted traveler system.

Although no specific surveys have been conducted to gauge the public's reaction to a multimodal approach, this technology – with the appropriate public education and outreach about the value of multimodal biometrics – has the potential to further reduce public resistance to the use of biometrics. Multimodal biometrics, once mature, may provide biometric identity-management systems with increased assurance, efficiency, ease of use, and

² Data from Unisys survey, released in 2007: http://www.unisys.com/about_unisys/news_a_events/02058750.htm

³ Data from Unisys survey, released in 2008: http://www.unisys.com/financial/news_a_events/all_news/12098939.htm

flexibility. For example, in some cases these additional biometrics can be taken from a distance, so those using the technology experience no physical contact. This has the potential to make the identification process more accurate and less invasive, and to further reduce fraud.

Question: In FY09 CBP received \$62.8 million to pay for costs of US-VISIT systems it used. Is CBP fully funding such systems, and if not, how much is US-VISIT covering?

ANSWER: Prior to FY 2009, US-VISIT transferred funding to Customs and Border Protection (CBP) to pay for Operations and Maintenance (O&M) of US-VISIT functionality. The funding levels provided by US-VISIT over the last few years have declined while the US-VISIT functionality that CBP supports has increased. US-VISIT and CBP agreed that, beginning in FY 2009, CBP would request O&M funding directly. These costs are required to provide recurring support to sustain the US-VISIT programs and enhancements implemented since FY 2003 and are necessary to ensure continued efficient processing of passengers at ports of entry (POEs). The \$62.8 million for FY 2009 covers:

- **Software maintenance:** Includes labor for software maintenance and changes to US-VISIT applications that CBP developed for air/sea and land POEs. Full maintenance life-cycle support includes documentation, software changes, testing, security, quality assurance, configuration management, project support and researching/resolving operational problems with the software.
- **Hardware Maintenance:** Includes maintenance of equipment and systems at the Data Center, including processors, data storage, and workstations used for US-VISIT processing at POEs.
- **Software License Maintenance:** Includes recurring license fees for software used to support US-VISIT at both the Data Center and at the POEs.
- **Telecommunications:** Includes costs for bandwidth used by US-VISIT increments and labor costs for the maintenance and monitoring of the network.
- **Operational Support:** Includes labor for Data Center operations, engineering support, help desk support, security support, asset management, duty officers, situation room monitoring, auto operations support, change management and code migration support, project management support, and field technology officers at the POEs to provide on the ground support.
- **Disaster Recovery:** Includes the maintenance of the environment for disaster recovery, including data replication and circuit costs.

The CBP FY 2009 US-VISIT O&M request was formulated before the transition from two-print to 10-print, which requires a much higher telecommunications bandwidth than two-print. Also, the 10-print capture devices are more expensive to acquire and maintain than the two-print devices. Although US-VISIT funded the initial expense of upgrading circuits and purchasing devices for 10-print, CBP is examining whether the recurring costs to support 10-print in the out years, along with the other US-VISIT operations and maintenance, will be more than \$62.8 million.

US-VISIT Governance

Question: The Executive Stakeholder Board (ESB) was created to oversee US-VISIT service and operational coordination with DHS agency requirements. How does the ESB ensure identity programs under US-VISIT are aligned with DHS component missions and priorities?

ANSWER: The Executive Stakeholder Board (ESB) is a newly created forum in which US-VISIT can solicit input from, and discuss issues with, the DHS customers it supports. For the purposes of the ESB, stakeholders represent DHS components and offices, along with other Federal agencies and departments.

Because US-VISIT provides operational support to numerous organizations, the primary purpose of the ESB is to enhance US-VISIT's ability to meet stakeholder needs and priorities. The ESB will accomplish this by providing a cross-organizational forum to share stakeholder goals and initiatives and to discuss, coordinate and communicate US-VISIT's direction, priorities and efforts.

The ESB is composed primarily of career executive members from each DHS stakeholder agency, as appointed by the chairperson. ESB members are representatives from:

- U.S. Customs and Border Protection, including the Offices of Border Patrol, Air and Marine, Field Operations, and Information and Technology;
- U.S. Immigration and Customs Enforcement, including the Offices of Operations and the Chief Information Officer (CIO);
- U.S. Citizenship and Immigration Services, including the Office of the CIO;
- Transportation Security Administration, including the Offices of Intelligence and Transportation Threat Assessment and Credentialing;
- U.S. Secret Service;
- U.S. Coast Guard, including the Offices of Operations and Command and Control Capabilities;
- DHS Screening Coordination Office;
- Federal Emergency Management Agency, Office of Disaster Assistance;
- DHS Office of Intelligence and Analysis; and
- DHS Science and Technology Directorate.

Board members are executives at DHS components and offices integral to helping US-VISIT achieve its vision and business goals. Additional board members – on a permanent, temporary, or guest basis – may come from non-DHS federal agencies.

The goals of the ESB are to:

- Provide recommendations about the overarching vision and strategic direction of US-VISIT and its responsiveness to applicable operational missions, both within DHS and with other concerned Government agencies;
- Provide a communication link for aligning US-VISIT's strategic direction, priorities, and resources with those of stakeholders;
- Review and recommend new and expanded initiatives that call for US-VISIT participation, including the scope, impact, risks, prioritization, and required resources;
- Allow stakeholders to represent their organizations' positions on recommendations and agenda topics at board meetings and to take individual responsibility for discussion/action items; and

Allow stakeholders to communicate discussion topics, decisions, and issues to their organizations, as appropriate.

Unique Identity

Question: In July 2008 DHS, the Departments of Justice and State signed a Memorandum of Understanding for "Improved Information Sharing Services," enabling more comprehensive matching against the broader FBI, State and DHS databases, and enable CBP, among others, to gain more "real-time" turnaround against databases such as the FBI Criminal Master File when biometric records are checked at high volume sites such as border

ports of entry. When will DHS achieve full operational capability of systems to enable interoperability between the FBI's database and IDENT, BSS, and State Department databases? To what extent is this affected by development of the FBI's next generation information technology system, and a resulting requirement to align IDENT and other systems with that new system?

ANSWER: The Unique Identity/Interoperability between the Department of Homeland Security's Automated Biometric Identification System (IDENT) and the Federal Bureau of Investigation's (FBI's) Integrated Automated Fingerprint Identification System (IAFIS) is being deployed incrementally in alignment with the FBI's Next Generation Identification (NGI) technology system project. As such, US-VISIT and the FBI are projecting achieving full operating capability in 2014.

While full operating capability will bring new services, U.S. Citizenship and Immigration Services and the Department of State (DOS) currently submit fingerprints for a search of the IDENT database and, in the case of DOS, for a search of the FBI Criminal Master File. IDENT then provides a single response back. USCIS currently submits its prints separately to the FBI and DHS. It is scheduled to transition to a single submission through IDENT in late FY 2009. It is important to note that DOS systems, USCIS systems and IDENT are already interoperable as all DOS prints and photographs, as well all USCIS prints and associated photographs, are already matched and stored in IDENT.

Some capabilities originally planned for the second phase of interoperability, the initial operational capability (IOC) scheduled for fall 2008, have been deferred to align timeframes with the new capabilities under the (NGI) technology system. Updated capability deployment dates will become available once NGI planning is further advanced.

US-VISIT Performance

Question: Last year DHS testified it had established an integrated project team (IPT), operating under a set of uniform policies and procedures, to assess progress of US-VISIT on implementing GAO recommendations. In December GAO reported that of a total of 44 recommendations, DHS had not implemented nine and only partially implemented another nine. How many recommendations remain open, and when will you implement them?

ANSWER: As of February 5, 2009, only two of 55 Government Accountability Office (GAO) recommendations remain "not implemented." However, based on recent progress, US-VISIT anticipates that one of the two remaining "not implemented" recommendations will soon be classified as "partially implemented." US-VISIT will discuss the remaining open recommendation with GAO in a meeting planned for early May. The remaining "not implemented" recommendation is awaiting a response from GAO to clarify specific requirements for closure and will also be discussed at the May meeting.

Regarding the remaining 16 "partially implemented" recommendations:

- US-VISIT anticipates full satisfaction (closure) of two recommendations in the very near future (closure based on the 2009 Expenditure Plan briefing to congressional committees).
- Ten of the partially implemented recommendations are awaiting clarification or response from GAO.
- Eight of the partially implemented recommendations have closure criteria that depend on, at least in part, the result of the ongoing Comprehensive Exit audit (310672) or submission of the related land exit report.

US-VISIT Staffing

Question: US-VISIT had 115 federal employee positions in FY 2008. 35 positions were funded in FY 2009, and I understand that DHS plans to hire another 62 positions using funds previously applied to contractor support. What is the status of filling these positions? How many of the projected 212 positions for FY09 are vacant, and how many are filled by contractors? Last year, US-VISIT had 225 contractor FTE positions. How many are currently occupied, and what is the projected number of FTE positions for the end of FY 2009?

ANSWER: US-VISIT is aggressively working to fill these positions by the end of FY 2009. Currently, US-VISIT has staffed 123 positions. US-VISIT has six additional positions with established entry-on-duty dates. In addition, US-VISIT has another 27 positions processing through security and seven positions awaiting final job offers. US-VISIT has selected candidates for an additional eight positions who are currently awaiting tentative job offers. Of the remaining 41 positions, 28 are in various stages of the recruitment process. There are 13 remaining for recruitment – the majority of which are awaiting classification of position descriptions for recruitment to begin.

Eighty-nine of the projected 212 positions for FY 2009 are currently vacant at US-VISIT.

There are 32 positions of the 212 that are currently staffed by contractors. Last year, US-VISIT had 225 contractor FTE positions.

There are 123 government personnel on-board at US-VISIT. The projected number of FTE positions for the end of FY 2009 is 212.

US-VISIT Cybersecurity

Question: Has US-VISIT experienced any cyber attacks? Has the US-VISIT biometric infrastructure been spoofed? What specific steps are being taken to enhance the capability of US-VISIT to defend against cyber attacks and identity fraud?

ANSWER: There is no evidence that the US-VISIT program has ever been compromised. DHS has carefully monitored the systems and security practices in place to protect the privacy of those whose data it collects and to ensure the integrity of that data.

US-VISIT knows of no successful spoofing of its biometric system. US-VISIT vigilantly protects the information it collects from misuse by anyone inside or outside of the Government. The Department of Homeland Security (DHS) uses multiple controls to protect against cyber attacks. In fact, if one control were deficient at the system level, additional controls exist at the network or facility level to compensate. US-VISIT has the appropriate checks and balances to protect information from compromise. US-VISIT is currently migrating from the Department of Justice data centers to DHS security-enhanced data center facilities to expand perimeter defenses and boundary control.

Enrollment

Question: Enrollment in biometric databases can be time-consuming, because multiple reference scans are taken to form a template to match later samples to verify that person's identity. GAO estimated in 2003 that facial recognition systems took 3 minutes to enroll, fingerprint systems 3.5 minutes, and iris scans about 2.25 minutes. Most countries, including the U.S., do not include biometric identifiers in their passports beyond a digital picture for visual inspection or a verbal physical description, such as height, hair and eye color, or weight. How long does it take to enroll an individual in DHS' biometric database network?

ANSWER: As noted, the amount of time needed to collect the biometrics differs by program, in part because of differences in what is collected by each component during that process. The actual enrollment into IDENT – meaning the amount of time to search the new set of fingerprints against every other set of prints in IDENT to determine whether DHS has previously encounter this individual – is very quick. The timeframes under which that process is completed differs by program and is set by service level agreement with the originating entity. For example, our agreement with State states that IDENT will search against all prints and reply back to State for BioVisa in 15 minutes or less so that the results of the full check can be used in the decision. In contrast, the service level agreement for CBP port of entry encounters set the requirement that IDENT will complete a biometric watchlist check or a “one to one” comparison in under 10 seconds, but complete the full search in 24 hours or less. By setting different requirements, DHS can make best use of its matching capacity and meet component needs. As component needs change, these response times can be altered.

DHS Biometrics Technology

Question: DHS, in a recent briefing to staff, identified biometrics as a high priority capability gap for the Department. How is that capability gap defined?

ANSWER: The capability gaps briefed to staff were developed as part of the DHS Science and Technology (S&T) Directorate’s Capstone Integrated Product Teams (IPT) process. S&T stood up IPTs comprised of high level staff from DHS components to identify and prioritize their respective technology needs (i.e., capability gaps) through a process that determines operational requirements, assesses current capabilities to meet operational needs and analyzes gaps in capabilities. S&T then moves forward with coordinated technology-based programs that lead to products that fill the gaps depending on available funding.

- The People Screening IPT (PS-IPT) coordinates the biometrics capability gaps as well as identification and detection of deceptive, hostile or violent intent and the optimization of screener performance. It is managed by the S&T Human Factors and Behavioral Sciences Division and co-chaired by the Deputy Assistant Secretary for DHS Policy (Screening Coordination) and the Deputy Director of U.S. Citizenship and Immigration Services.

Question: What technological hurdles pose the biggest challenges to getting the most out of biometric information?

ANSWER: New sophisticated technical solutions are entering the marketplace creating planning complexities. Different biometric modalities, sensor technologies, pattern recognition engines and decision modules have different implications for the different types of DHS screening operations. Investments in biometrics science, technology development and testing are needed for effective decision making regarding biometric screening. Research is required to develop a scientific understanding of the foundational physiological, chemical, and behavioral attributes and measurement sciences that permit biometric recognition including technologies based on face, iris, and other biometrics. For each modality, DHS must understand key characteristics including (but not limited to) uniqueness, performance and collectability. An incomplete understanding of the underlying science may lead to the acquisition and deployment of costly technologies that ultimately do not meet DHS needs.

Test and Evaluation (T&E) is also required to support the development of and assess the efficacy of biometrics technologies for use in DHS operational environments. Most companies developing biometric technologies have only limited internal resources to support sustained development of effective, scalable technologies suitable for use in harsh and diverse DHS operational environments. Biometric systems at DHS need to satisfy user needs to collect and match biometric data in short time frames while also meeting biometric-specific

requirements, such as quality of collected data. T&E is required to measure performance and assess whether the technologies are likely to successfully “translate” into practical and implementable capabilities.

Data fusion research and techniques are needed to synthesis information into a useful form. One-to-many matching required for identification is significantly more complex, computationally intensive, and prone to higher error rates than one-to-one matching. Research is also required to match biometric information and understand error rates when using different modalities, of operational “field-collected quality”, and with different sensor technologies. This information will aid decision-makers in assessing potential risks associated with incorrectly matching a biometric to the wrong person or failing to match an individual to a watchlist.

Finally, the adoption of robust, technically sound standards and widely accepted T&E capabilities is rapidly emerging as key priorities for the Department. Biometric technology standards need to meet DHS technical requirements and permit data sharing. Otherwise, each system may be stove-piped with little ability to communicate biometric data and screening results between collection points, matching systems and storage repositories. This situation presents a significant risk to the Department since acquisition is currently based, to significant extent, on supplier performance and conformance claims. DHS is participating in private sector standards development organizations to facilitate the development and adoption of appropriate private sector standards. Additionally, DHS is coordinating with the National Institute of Standards and Technology (NIST) to develop an accreditation program for laboratories that perform certain types of biometrics-related testing.

Question: The Science and Technology Directorate is studying new technologies such as touchless fingerprint scanners and improvements in facial geometry and iris capture. Which technologies being researched by DHS are most important to ensuring DHS’s biometric initiatives succeed?

ANSWER: In order to ensure that DHS’s biometrics initiatives succeed, the following technologies are being researched to satisfy DHS-specific requirements:

- Developing robust and resilient sensor technologies for collection of multi-modal biometrics in DHS’ real world mobile and permanent locations on the borders (entry or exit) and at sea. Current multi-modal biometrics being evaluated are fingerprint, face, and iris.
- Developing multi-modal biometric quality assessment, matching and fusion algorithms to enable DHS operators to effectively screen the 414 million individuals that enter our country each year through the 435 points of entry.
- Conducting basic research to understand and test the science behind new and innovative biometrics and credentialing technologies that may be uniquely applied to the DHS screening mission.
- Championing the development of technically sound biometric technology standards and testing programs to prevent stovepipe or proprietary solutions to DHS’ technical and data sharing requirements.

Question: CBP’s Electronic System for Travel Authorization (ESTA) for Visa Waiver Program travelers does not use biometric data, nor does its Advance Passenger Information System (APIS). Both of these programs contribute to identifying potentially dangerous individuals trying to enter the country. Should incorporating biometric data in these systems be a priority?

ANSWER: The Electronic System for Travel Authorization (ESTA) and the Advance Passenger Information System (APIS) are complementary screening programs that conduct checks on international travelers prior to their arrival in the United States using biographic and travel information. The US-VISIT biometric checks at

U.S. ports of entry build upon the screening provided through ESTA and APIS and provide unique identification of covered travelers. Incorporating biometric data into ESTA or APIS would present tremendous business process and technological challenges. As such, it is not a DHS priority at this time.

Question: Since November 2006, Coast Guard has piloted a program to collect biometric data from would-be migrants at sea and check it against shore-based databases to sort out who should be repatriated and who should be prosecuted. This program appears to have been successful, resulting in 467 prosecutions of criminal migrants. At a recent biometrics conference Coast Guard officials said FEMA and CBP are developing their own mobile biometrics collection capacities. If so, why can't FEMA and CBP use the Coast Guard system?

ANSWER: The Department recognizes that a number of DHS components have made advancements related to mobile biometrics. Each system is tailored to meet the component's specific needs, as each component faces a unique set of environmental and technological challenges. Although a singular approach would simplify some aspects of implementation and interoperability, it would not accommodate the diverse needs that exist within DHS. For example, operational environments place different demands on the equipment's ability to capture quality images. In particular, it is important to recognize that biometrics are usually collected as part of a larger process and so DHS components acquire devices that best integrate into their operations.

Question: Coast Guard expanded this program from the Mona Pass by Puerto Rico to the Florida Straits. What is the cost of this program (both for US-VISIT and Coast Guard, if known) in FY 2007-08 and planned for FY 2009; what would it cost to expand it throughout the Coast Guard and other DHS marine operations (e.g., CBP Air and Marine) for mobile biometric collection?

ANSWER: US-VISIT provided \$501,500 in FY 2007 for the Mobile Biometric Link program, a joint project with the U.S. Coast Guard. US-VISIT did not provide any additional funds in FY 2008 for this project.

DHS has not determined a cost estimate at this time for expansion throughout the Coast Guard and other DHS marine operations (e.g., CBP Air and Marine).

A US-VISIT estimate, or rough order of magnitude (ROM), to support a US Coast Guard (USCG) and Customs and Border Protection (CBP) air/marine mobile project would be as follows:

- \$1,000,000 in first-year operation and maintenance (O&M) costs based on no more than 150,000 transactions a year requiring two-minute response times.
- \$3,000,000 in application development, including messaging, security and other changes to the Automated Biometric Identification System to accommodate user-specific requirements.

Total ROM for the first year of operation and development would be \$4,000,000. Additional costs for out-year O&M, estimated to be \$9,000,000 over four years, would also be incurred. These costs do not cover the procurement of devices, device software support, communications, user training, etc., which would need to be provided by CBP and USCG.

The Office of CBP Air and Marine (A&M) advised that it does not process individuals and that its platforms are not sufficient to support the process. Accordingly, CBP A&M sites would support Office of Border Patrol (OBP) and Office of Field Operations (OFO) personnel tasked and trained for biometric collection. Therefore, the following would apply:

- Purchase and maintenance cost estimates per unit (mobile device) would be in line with USCG.

- CBP estimates that it would have one mobile device at each of its 53 sites – 23 air locations and 30 marine locations. Using the \$15,000 cost per unit from the USCG (see below), the estimated cost for CBP A&M for 53 units is \$825,000.
- Deployment costs would be primarily to deliver the mobile device to the site.
- Training costs would be minimal for CBP A&M, because it would not be using the devices but rather making them available to OBP and OFO as needed.

USCG estimates it would cost \$4,733,000 to establish a biometrics program of record and begin expansion throughout parts of the USCG. The cost per unit is \$15,000 per system, which includes one laptop and two handheld biometric collection units. This would build upon the lessons learned from the successful proof of concept in the Mona Pass to:

- Examine the application of biometric collection at sea for maritime law enforcement, domain awareness, security, intelligence collection, and identification of patterns and networks.
- Develop solutions for designated USCG cutters and Deployable Operations Group adaptive-force packages.
- Expand use of this capability in migrant vectors beyond the Mona Pass.
- Support program management for a permanent system of record, including interagency coordination of systems development, engineering, and evolution.
- Provide life-cycle recapitalization, continued system accreditation, and certification.

Enumerator

Question: In 2007, IDENT began to provide “enumeration services,” generating a unique identifier (“enumerator”) for any individual with ten fingerprints and minimal biographic data on file. This number is reportedly intended to be used for work in the border security/immigration environment only. In 2007, DHS acknowledged in a Privacy Impact Assessment update that use of the enumerator generated by this system as a ready-made individual identifier is possible by public or private entities. Despite assurances that DHS does not intend the enumerator to be used in this way, the update does not indicate what specific steps are being taken to prevent that outcome. What is the Status of the enumerator services program at this point, and what specific steps is DHS taking to prevent enumerators from becoming a de facto identifier for U.S. persons – citizens and residents?

ANSWER: The enumeration service has been completed. In other words, IDENT will provide a unique identifier to a DHS program or U.S. government agency upon their submission of a new set of fingerprints to IDENT. IDENT will also be able to use that identifier as part of the verification process upon subsequent encounters by enabling IDENT to conduct a one to one automated fingerprint match against the fingerprints on file associated with that unique identifier.

However, DHS recognizes the inherent vulnerabilities created by giving a single ID number as an indispensable public-facing identifier or global record locator and therefore will not use a single enumerator with any public-facing use.

DHS has determined that the use of a single public-facing enumerator would pose an unnecessary risk to privacy and security for the Department and the individual seeking a license, privilege, or status without providing additional capabilities. A single enumerator is not required by DHS. The Department currently utilizes multiple enumerators/identifiers to achieve similar goals when interacting with individuals. The use of multiple identifiers offers more options for individuals interacting with the Department while mitigating security and privacy risks. The use of multiple types of enumeration/identifiers coupled with the creation of robust information management and sharing rules across DHS will result in readily available information for

DHS decision-makers while deterring fraudulent activity, and prevents the creation of a single identifier for any U.S. person.

DHS will establish policy to this effect and maintain and monitor compliance of DHS components and programs with this policy.

Effectiveness

Question: How does DHS measure the effectiveness of a biometric as a reliable tool for identity determination and validation? If some biometric data in DHS databases is less effective than others, why keep them?

ANSWER: A basic measure of biometrics as an effective, reliable tool for identity determination and validation is the number of criminals and immigration violators US-VISIT has identified and prevented from entering the United States based on biometrics alone. Using biometric identification, US-VISIT has helped the Department of State and U.S. Customs and Border Protection stop thousands of criminals, immigration violators, and others committing identity fraud from traveling to or entering the United States who otherwise would not have been identified and stopped. US-VISIT biometric identification services assist the U.S. Border Patrol and the U.S. Coast Guard (USCG) to identify hundreds of illegal migrants per year trying to evade detection through the use of false or nonexistent identification. In the case of the USCG, interdictions are down by 60 percent due to the use of biometrics. US-VISIT also supports U.S. Citizenship and Immigration Services to prevent fraud among immigration benefit applicants. Because fraudulent travel documents are one of the primary tools that criminals, terrorists, and others use to evade detection, the value of biometric identity validation cannot be understated. All of these benefits have been achieved without adversely affecting wait times at the border.

Additionally, US-VISIT manages the technical effectiveness of the IDENT biometric system. US-VISIT captures and manages information regarding the accuracy of underlying biometric matching systems. There are two types of errors inherent in biometric matching systems that must be balanced to assure accurate yet timely screening of individuals; false match rates – the percentage of individuals falsely identified by the system, and false non-match rates – the percentage of individuals that should be identified by the system but are not.

In verification systems, where an individual presents documents known to the enterprise and is expected to be identified based on previous encounters, US-VISIT manages the system to less than 1 percent error (false non-match rate). In screening systems, such as US-VISIT's biometric watch list, false match rates are managed to less than 0.1 percent error. These measures and other performance data are captured, reported and acted on as part of routine system and screening process management.

DHS retains the data because it continues to be useful. Each biometric record DHS maintains can still be used to identify a person and conduct checks, even after we migrate to a new standard.

Question: Since data is stored digitally, why not skip the middleman and use an ID number?

ANSWER: DHS uses biometrics to perform two primary functions: Providing the ability to verify that the person before us is the same one we've seen previously (confirmation of identity), and the ability to conduct appropriate screening.

DHS does not believe an ID number is appropriate to solve either of these two problems. First, should someone acquire an ID number that is not theirs, they can pretend to be another individual. Second, DHS screens

individuals based on matching to data of a known individual – using fingerprints, name, etc. DHS would not be able to use an ID number as a substitute.

Finally, DHS has no interest in creating a single ID number that would be used across programs given the potential for misuse and identity theft.

Question: How does DHS measure effectiveness against the risk to the privacy of individuals?

ANSWER: The DHS Privacy Office works closely with DHS program offices and Components to ensure privacy concerns are addressed at the earliest stages of program development, frequently resulting in a formal, written Privacy Impact Assessment (PIA). DHS conducts PIAs of systems as required under Section 208 of the E-Government Act and on programs, offices or policies that impact privacy under Section 222 of the Homeland Security Act. The PIAs examine potential privacy risks of the system or policy and outline steps the program has taken or should take to mitigate those potential risks.

Question: Could DHS upgrade biometric data in legacy databases for modern systems, such as using existing photographs for facial geometry matches, or using non-standard fingerprint data?

ANSWER: Yes, DHS can use much of the existing biometric data in legacy systems. Where this is possible, DHS is examining options on how best to do so. For example, DHS already uses legacy photographs. Many of our systems are now built to present the photo to an officer, who is then able to compare the photo on the screen to the photo in the document as well as the person. This helps to protect against photo substitution and identity theft. DHS is also examining options for automated facial recognition, where appropriate.

In terms of fingerprints, DHS does use existing data wherever possible. For example, the two prints collected electronically under the US-VISIT program and stored in IDENT will continue to be used. Fingerprints stored on paper cards may be able to be scanned in over time. In certain cases, however, the standards to which certain legacy data was electronically stored (e.g., the USCIS press prints from card production) is insufficient and will not support matching.

Impact on Travel and Trade

Question: Have biometric measures sped or slowed entry into the U.S. for foreign visitors and goods, and what evidence exists to support your answer?

ANSWER: The Department's use of biometrics through the US-VISIT program is facilitating legitimate travel by making the entry process more efficient, accurate, and secure. Since US-VISIT was established, DHS has processed millions of travelers through the program and intercepted thousands of criminals and immigration violators using biometrics, all without affecting wait times at our ports of entry.

In fact, in the secondary inspection areas of some of the land border ports, automation of the former paper processes through US-VISIT procedures have significantly reduced the time it takes for a visitor to obtain a Form I-94 and be admitted into the country. For example, in Laredo, Texas, the Form I-94 issuance process has been reduced from an average time of eight to 11 minutes to just two to five minutes, despite the fact that the collection of biometrics and additional security screening were added.

Question: What feedback has DHS received from U.S. implementation of biometric requirements in the visa process and for passports? Do you have survey results that you can provide to the Committee?

ANSWER: The Department receives anecdotal feedback from U.S. government partners and travel and tourism industry representatives about how biometric procedures are being received by travelers from countries around the world. Such feedback is informal and provided through discussions or e-mail. US-VISIT also holds briefings to update key organizations and government partners about the program, during which attendees provide feedback about US-VISIT. In general, these entities report that the requirements are understood by travelers. However, they suggest that the need for public education and outreach internationally remains critical to ensuring that travelers understand changing travel requirements.

US-VISIT was recognized in a 2007 report by the Discover America Partnership, a leading organization that advocated on behalf of the travel and tourism industry at that time, as an "example of how we can deploy technology to enhance security and increase confidence among our front-line visa officers, allowing them to admit more legitimate travelers into the U.S." This report, "A Blueprint To Discover America," also called for the United States to develop a "21st Century travel system that builds off the successes of the US-VISIT program."

US-VISIT also works closely with other countries that are developing similar programs and receives feedback from those governments.

US-VISIT has not conducted "formal surveys" to gauge public perception of the US-VISIT Program. Instead, we rely upon information received informally from travelers and others affected by the program as well as industry representatives and media reports.

Proper Use of Data

Question: DHS databases contain biometric data of citizens and noncitizens, criminals and innocent people alike, for many different purposes. To what extent is data pooled across programs? As databases are combined and repurposed, how does the Department ensure such information is not being used improperly?

ANSWER: Biometric data is not generally pooled across the Department. The Department has a single repository for large portion of biometric data at NPPD US-VISIT in the IDENT (fingerprint) system. When IDENT is used by DHS for immigration, border crossing, and other security duties, it is accessed in IDENT, rather than pooled with other systems.

DHS and its components engage in extensive security and privacy training to ensure that IT resources and Personally Identifiable Information (PII) are accessed and handled appropriately. Additionally, further specific safeguards exist within each component and each operational program to ensure that information is handled appropriately.

All systems that have PII and are combined or repurposed are subject to the E-Government Act and Privacy Act. The Privacy Act requires the Department to publish a System of Records Notice (SORN) describing the allowable uses. The E-Government Act requires the Department to conduct Privacy Impact Assessments (PIAs) which identify the potential privacy risks in the system and the steps the program has taken to mitigate those risks.

Question: In terms of the number of individual records, how much data in DHS databases is on U.S. citizens?

ANSWER: DHS does not count individual records. To the extent that DHS's operations directly involve U.S. citizens, DHS captures that information as it would any individual of any other citizenship status. U.S. citizens are, however, afforded greater rights under the Privacy Act of 1974 than non-citizens although in practice DHS

components apply largely the same security safeguards and privacy protections to non-citizen data. USCIS, the administrator of immigration benefits, does not interface with U.S. citizens as often as a component like CBP, that screens all individuals crossing the U.S. border but collects biometric information on foreign nationals. Other components like U.S. Coast Guard and TSA have information on U.S. citizens and non-citizens in execution of their maritime and general transportation safety missions.

Question: What measures are in place to ensure that biometric data of an innocent bystander at the scene of a terror incident is not picked up and characterized as belonging to a suspect, thus putting an unsuspecting individual on a DHS watchlist?

ANSWER: As the example notes, latent fingerprints collected at an incident scene could belong to a perpetrator or an innocent bystander. For that reason, when DHS or law enforcement identify a match to such latent prints, further investigation and coordination is required to determine what action is appropriate. Through both the encounter management process (used to collect information during an encounter with a person on the watchlist) and the redress process, information is added to the watchlist record to prevent future misidentification.

The U.S. government has a rigorous set of criteria to meet before a person or identifier is added to the terrorist watchlist. This set of criteria is documented in the Terrorist Screening Center protocol for minimum standards for nomination to the terror watchlist which ensures that an individual is reasonably suspected of supporting terrorist activity prior to nomination and establishes mechanisms for review of watchlist records.

Persistence of Data Presented by Individuals

Question: When an individual claims an identity and presents biometric data to verify it, how long does DHS retain that information?

ANSWER: The length of time the information is retained is based on the authority under which the DHS program collected the data and the DHS retention schedule as established through our System of Records Notices and Privacy Impact Assessments. For example, DHS has a long established retention requirement for data collected on applicants for immigration benefits at 75 years, including biometrics. Similarly, biometrics collected under the US-VISIT program from non-U.S. citizens entering the country are also retained for 75 years. Conversely, TSA screening and credentialing programs (except for Secure Flight) retain program data, including biometrics, on individuals who were not a possible match to a watchlist for 1 year after their access based on the vetting expires or is terminated; for individuals who were a possible match but cleared, 7 years from the vetting; for actual matches to a watchlist, 99 years.

Question: A recent press report indicated USCIS is considering using a biometric identifier to help track applications for naturalization and immigration benefits. How far along is USCIS in this effort and what plans have they made to implement such a system?

ANSWER: It is important to note that USCIS has collected biometrics, fingerprints and photographs, on certain individuals applying for immigration benefits for decades. USCIS implemented the electronic collection of biometrics through their Application Support Centers (ASCs) in 1998. USCIS biometrics collected after 2003, are stored electronically in IDENT. Through its transformation efforts, USCIS is modifying its business process to become person-centric rather than application centered. Biometrics will play a role in uniquely identifying and verifying an individual and enabling USCIS to link to records from State Department, CBP, and ICE to ensure USCIS is able to view all relevant information about a person as part of their immigration benefits decision.

Question: What does DHS do with biometric data of an individual once they become a naturalized citizen? Does it remain in a DHS database?

ANSWER: As described in our System of Records Notices and Privacy Impact Assessments, this data remains in DHS systems, including paper A-files and USCIS systems, for 75 years. The A-files are retained to maintain records for immigration benefits processing, protection of national security, and to administer and enforce immigration and nationality laws.

Yes, it remains in a DHS database.

IDENT/BSS

Question: The IDENT database is the primary functional repository of biometric information held by DHS, including US-VISIT data. IDENT is reportedly updated daily by the Biometric Storage System (BSS), which contains all biometric data captured by USCIS. When BSS was established, it was intended to create new direct links to the FBI's Integrated Automated Fingerprint Identification System (IAFIS) and improve data sharing with the IDENT database. What is the purpose of having what seem to be parallel systems in IDENT and BSS inside DHS?

ANSWER: Because interoperability between IDENT and FBI's IAFIS did not exist when BSS was established, USCIS currently uses BSS to send fingerprints separately to IDENT and FBI's IAFIS. However, in the future USCIS will send fingerprints only to IDENT and, using the capabilities developed through IDENT/IAFIS interoperability, receive an integrated response from both biometric systems.

State Department Databases and DHS

Question: The Department of State has extensive information in its Consular Consolidated Database (CCD), which has data from 82 million visa applications, including some biometrics in the form of left and right index finger prints and digital photographs. How does DHS work with State to leverage that information?

ANSWER: The Department of State (DOS) and DHS work together very closely and share significant amounts of information given the integrally linked mission and processes for immigration and border management. As is noted in the following questions, DOS sends some CCD data directly to DHS, and DHS provides certain data for incorporation into the CCD. Further, DOS provides DHS officers with direct user accounts to CCD, and DHS provides appropriate DOS personnel with user accounts to its systems.

Question: Is CCD data duplicated in the DHS system? If so, why, and how is it updated if changes are needed? What is the status of integrating these databases with those in DHS under US-VISIT?

ANSWER: Certain data associated with nonimmigrant visas, immigrant visas, passport books and passport cards are transmitted from the Department of State (DOS) to DHS and stored in the DHS IDENT system, managed by US-VISIT, or the TECS system, managed by CBP. Passport and visa issuance data (e.g., name, document number, passport photo) are held in TECS. Visa biometric information (e.g., fingerprints and digital facial images (photos)) is stored in IDENT.

The data is transmitted and stored in sections of IDENT and TECS so that it can be quickly retrieved at the time the person applies for entry into the United States at the border in order to verify the authenticity of the visa, the

passport book, or passport card as well as ensuring that the person presenting it is the person to whom State issued. As an example, when a U.S. citizen presents a passport, the CBP officer “swipes” the Machine Readable Zone on the document, the TECS system then retrieves the biographic data and photo provided by DOS and displays it so that the CBP officer can compare the stored data to the photo and biographic data printed on the document presented.

A similar process is used when a non-U.S. citizen presents a visa. The CBP officer “swipes” the visa, and directs the person to provide his fingerprints. The photo and other issuance data is presented on the screen, and the fingerprints are electronically compared to those in IDENT.

Visa and passport data are transmitted and updated in real time. This means that as soon as the visa or passport application data has been entered or updated by the Department of State it is transmitted to DHS and stored in the appropriate sections of the TECS and IDENT systems.

DOS systems and data are integrated into the DHS environment, particularly with respect to the data used in the US-VISIT process. As an example, all BioVisa biometrics (fingerprints and photographs), along with base biographic data, are sent to DHS’ IDENT for search and then stored in IDENT. As is noted above, DHS is then able to use this information to verify that the person presenting the visa to the CBP officer at the port of entry is the one to whom State issued it.

DOD Databases and DHS and HSPD 6

Question: Homeland Security Presidential Directive 6 (HSPD 6) made it U.S. policy to develop, integrate, and maintain terrorist information to use it, to the extent permitted by law, for screening purposes to include intelligence, law enforcement, immigration, and visa processes. An October 2008 GAO report (GAO-09-49) noted that there is no direct link between DOD biometrics and identification information (for Iraq and Afghanistan conflicts in particular) and DHS, with only part of DOD data made available in the Justice Department IAFIS database. What is being done, under the Intelligence Reform and Terrorism Prevention Act, as well as the National Science and Technology Council, to enable sharing of such information collected by DOD with DHS?

ANSWER: DHS and DOD have a very positive and close working relationship that includes efforts to effectively share biometrics in order to identify individuals who may present a threat. As a specific example, DHS checks all biometrics collected for Iraqi refugees against DOD biometric holdings. In addition, DOD provides records from its biometrically-enabled watchlist directly to DHS for use in all DHS biometric screening programs.

In addition, DHS and DOD are working with the larger interagency community to ensure that DOD and DHS biometrics associated with known or suspected terrorists are made available to other U.S. government entities as required by HSPD-6 and HSPD-24/NSPD-59 *Biometrics for Identification and Screening to Enhance National Security*.

HSPD 24

Question: Homeland Security Presidential Directive 24 (HSPD 24), in effect since June 2008, was intended to establish a framework to ensure the Executive branch uses compatible methods and procedures in collection, storage and sharing of biometric information and its contextual background. Item 16(a) of HSPD 24 indicates that the Secretaries of State, Defense and Homeland Security, the Attorney General, the Director of National Intelligence and the heads of other appropriate agencies shall develop and implement mutually compatible guidelines for the collection, storage, use, analysis, and sharing of biometric and contextual data. Furthermore,

it calls on those agency heads to establish “objectives, priorities and guidance” to make sure such information is used in a timely and effective fashion. Please describe specific efforts DHS is making under HSPD 24, and how it aims to increase transparency in the process of developing these guidelines, objectives and priorities for the use of biometric data.

ANSWER: DHS has a number of efforts underway that relate to HSPD-24. Some of these efforts pre-existed the HSPD-24 effort though were further prioritized as a result.

- (1) Use of standards for collection of biometrics. HSPD-24 emphasizes the need to collect biometrics to recognized standards. DHS has been working with the National Science and Technology Council (NSTC) working group on development and maintenance of biometric collection and transmission standards for a number of years and uses those standards.
- (2) Enhancing the existing identification and screening processes associated with the known or suspected terrorist (KST) watchlist. DHS has been working closely with the Terrorist Screening Center (TSC) and the National Counterterrorism Center, as well as other members of the interagency, to fully integrate biometrics into the existing KST biographic process. As an example, DHS is emphasizing the ability to receive records from the TSC and provide encounter responses back through a more highly automated process that emphasizes consistency, accuracy, and timeliness.
- (3) Research and development efforts for additional biometric modalities. DHS has a very robust fingerprint collection, storage, and matching capability and routinely collects and stores digital facial images (photos). DHS will continue efforts to examine options for other biometric modalities as appropriate.

Question: HSPD 24 seems focused on tracking known and suspected terrorists. Does data collected under US-VISIT or the Registered Traveler program fall under HSPD 24?

ANSWER: The intent of the presidential directive is to build upon the success of the integrated screening capability to protect the Nation against “known and suspected terrorists” (KSTs), by enhancing the U.S. government’s capability to collect, store, use, analyze, and share biometrics to identify and screen KSTs and other persons who may pose a threat to national security. As such, it applies to any DHS screening, credentialing or law enforcement program.

It is important to understand, however, that the Presidential Directive does not create any new requirements to collect, retain, or share biometric or other data. The Directive provides direction to enhance current screening and identification capabilities, especially with respect to the identification and screening for KSTs.

On a last note, the TSA Registered Traveler (RT) pilot has been terminated. TSA no longer collects or screens any data associated with Registered Traveler members. Any current collection of data on RT members is being done solely by private sector RT vendors on behalf of their airport and air carrier clients. As such, DHS has no plans to modify or otherwise change RT because of HSPD-24.

Question: HSPD 24 also references the sharing of biometric data with other countries. What biometric data collected by the United States is currently shared with foreign countries, and under what mechanisms?

ANSWER: Where the U.S. shares information with a foreign government, it often occurs between agencies that have similar missions with the sharing clearly tied to those missions. As an example, the Department of Justice has established a number of mutual legal assistance treaties (MLATs) that provide for the sharing of information for the investigation and prosecution of crime.

In keeping with its mission, DHS has agreements and arrangements that support immigration or border screening. A recent example includes the sharing of biometric data for asylum applicants for the purpose of determining fraud. Sharing of information for known or suspected terrorists is managed by the Terrorist Screening Center and State Department, as required by HSPD-6.

In general, information and data sharing occurs through non-binding arrangements or memoranda of understanding or other formal written documents.

Question: For example, the “four country conference” which US-VISIT has engaged Britain, Canada and Australia (and possibly New Zealand) has resulted in sharing of fingerprints under a protocol for “high value data sharing.” While I understand this has primarily focused on the use of biometric information to adjudicate asylum claims and deter fraud, is it under consideration for broader use?

ANSWER: The exchanges conducted under the High Value Data Sharing Protocol are primarily designed for immigration and nationality purposes, to facilitate border security and maintain effective immigration control. At this time, Four Country Conference participants are working to operationalize the Protocol as it was initially envisioned. DHS is not contemplating any expansions beyond the immigration and border security arena at this time.

Question: Last March the U.S. and Germany agreed to establish watch list and limited sharing of fingerprint sharing. What is the status of planning and implementation of such agreements?

ANSWER: DHS signed the Preventing and Combating Serious Crime (or “Prüm-like,” as it is modeled on the Prüm Convention concluded among a number of European countries) agreement with Germany in October 2008. The German parliament must now ratify the agreement, which they are expected to do later this year. In the meantime, experts from DHS, the FBI and the German federal police began meeting in January 2009 to start planning for the implementation of the agreement following ratification.

Question: An action plan is called for under HSPD 24 for implementing the directive’s many provisions, and for recommending how to enhance “the existing terrorist-oriented identification and screening processes by expanding the use of biometrics.” Has that action plan been produced? If so, did it recommend action to protect privacy of innocent individuals whose biometric data is swept up in terrorism investigations or screening processes? What funding is required to carry this out?

ANSWER: Yes, the Action Plan called for by HSPD-24/NSPD-59 has been completed. It was finalized by the former Administration in December 2008.

The Action Plan reiterated that the intent of the Presidential Directive is to provide, “a framework to ensure that federal executive departments and agencies (agencies) use mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals in a lawful and appropriate manner, while respecting their information privacy and other legal rights under United States law.”

The Action Plan noted that, to ensure full interagency integration on privacy and civil liberties issues concerning biometrics, the effort should be coordinated with the CIO Council Privacy Committee and make full use of the National Science and Technology Council’s privacy working group.

The interagency has not yet developed a full estimate of costs for this effort. A number of activities are being implemented through existing funding.

Question: US-VISIT has an Information Sharing and Technical Assistance component that has been developing bilateral and multilateral relationships for assisting other governments in developing biometric and biographic identity management systems. Could you list some of the major countries with whom US-VISIT is working, and the nature of the cooperation or information sharing?

ANSWER: As part of broader DHS efforts to promote information sharing and immigration and border security, US-VISIT is actively building partnerships with selected foreign governments to promote biometric identity management and ensure interoperability. US-VISIT's Information Sharing and Technical Assistance Branch provides technical assistance on biometric collection and applications through all phases of the immigration and border travel continuum, beginning with the issuance of a travel document and continuing through visa issuance, inspections at the ports of entry, adjudication of immigration benefits, enforcement of immigration law, and, ultimately, exit.

US-VISIT collaborates with national and international organizations to identify and align biometric standards that support the identity-management infrastructure and to facilitate data sharing with domestic and foreign partners. Data sharing with a foreign government might include the pilot exchange of data to demonstrate interoperability, encounter-based sharing for law enforcement purposes, and systematic sharing to provide real-time information in an immigration and border management environment. US-VISIT provides technical assistance and/or shares information with the following countries:

Country	Technical Assistance	Biometric Data Information Sharing
United Kingdom	Current	Current
Canada	Current	Planned
Germany	Current	Planned
Mexico	Current	Planned
Australia	Current	Planned
Japan	Current	
Korea	Current	

United Kingdom: In 2007, DHS and UKvisas – now the U.K. Border Agency (UKBA) – concluded an arrangement to allow the sharing of biometric data. As part of this arrangement, applicants for visas to the UK may go to a U.S. Citizenship and Immigration Services Application Support Center in order to more conveniently provide their biometrics (photo and fingerprints) to the UK.

To support U.K. efforts to collect, store, and match biometrics in a border and immigration environment, US-VISIT seconded a technical expert to UKvisas in 2007. This technical expert worked with a counterpart in the United Kingdom to ensure interoperability between U.S. and U.K. systems and to provide best practices related to the development of biometric identity-management systems. US-VISIT and the UKBA also participate in the Biometrics and Technology Working Group of the Four Country Conference (4CC).

Canada: A statement of mutual understanding signed by the Governments of the United States and Canada allows for the reciprocal sharing of biometric and biographic information "...relevant to the prevention, investigation, or punishment of conduct that would render a person inadmissible or removable under the citizenship or immigration laws." To further the biometric sharing allowed under this arrangement, US-VISIT and the Canada Border Services Agency (CBSA) formed a technical working group on biometric identity management.

As part of this group, US-VISIT is working with Canada to exchange information that would serve both countries in their efforts to establish entry/exit records. US-VISIT is currently conducting impact assessments of proposed entry/exit data-sharing scenarios to determine which arrangements will effectively confirm third-country national exit from the United States, and which will also assist in the prevention of immigration fraud and cross-border crime. Canada and the United States have also exchanged biometric data through the Biometrics and Technology Working Group of the 4CC.

Germany: In 2008, the U.S. and German governments signed the Agreement between the Government of the United States of America and the Government of the Federal Republic of Germany on enhancing cooperation in preventing and combating serious crime. As part of this agreement, DHS and the Federal Bureau of Investigation (FBI) are developing an implementation framework that will allow for the reciprocal exchange of biometric data. Within this framework, the German Federal Criminal Police (BKA) will send prints of known or suspected terrorists and criminals to both DHS and the FBI.

Mexico: US-VISIT is working closely with the Government of Mexico under the Mérida Initiative to support efforts to incorporate biometrics into Mexico's immigration and border management processes. In an effort to bolster the effectiveness of the Mérida Initiative, US-VISIT and the Government of Mexico (including representation from the National Migration Institute, National Registry of the Population, Secretariat of Public Security, and the Center for Investigations and National Security) formed a bilateral technical working group. **Australia:** In 2008, US-VISIT seconded a technical expert to the Australian Department of Immigration and Citizenship. This technical expert provides Australia with best practices and lessons learned that support Australia's efforts to incorporate biometric identity management into its immigration and border management systems. DHS and Australia are also exploring opportunities to exchange biometric data on persons of interest. US-VISIT and Australia's Department of Immigration and Citizenship also participate in the Biometrics and Technology Working Group of the 4CC, which consists of representatives from the immigration agencies of the United States, Canada, Australia, the United Kingdom, and New Zealand (which will become a member of the conference in June 2009).

Japan: The Japan Immigration Bureau introduced its Biometric Immigration Control System (BICS) on November 20, 2007. This system is compatible with US-VISIT's system, both in standards and technology, and contains data sets of aliens found inadmissible to Japan and those who have been expelled from Japan. In January 2008, reports from Japan surfaced that a Korean woman had foiled the Japanese biometric immigration system by using special tape and documents she had purchased from a "broker" to pass through the Japanese biometric screening process. Following reports of that incident, US-VISIT provided Japan with technical assistance to mitigate the threat of future biometric-spoofing incidents. This technical assistance included background information on forms of biometrics spoofing and fingerprint mutilation, as well as prescribed methods to combat future spoofing efforts.

Korea: US-VISIT hosted a meeting with representatives from the Korean Immigration Service in 2008 and provided technical briefings and demonstrations on US-VISIT's biometric capabilities. Korea is introducing biometrics into its border and immigration management control and will model its system after US-VISIT. **Group of Eight (G8):** The G8 is a collaborative forum of representatives from Canada, France, Germany, Italy, Japan, Russia, the United Kingdom, and the United States that addresses a wide range of international economic, political, and security issues, including migration. US-VISIT developed a proposal with the U.K. Home Office for the G8 Roma/Lyon Migration Experts Subgroup (MESG), which promotes biometric identity management across the G8 member states. The MESG coordinates best practices among the member states to collectively reduce illegal migration, protect those who seek refuge, prevent the use of fraudulent documents, develop strategies to defeat identity imposters, and investigate human traffickers and smugglers. The best practices identified by the MESG strengthen and promote cooperation and information sharing among police and border and immigration officials within the G8 and beyond.

HSPD 12

Question: Homeland Security Presidential Directive 12, which was laid out in 2004 by the previous Administration, aimed at establishing a unified standard for government identification card, including biometrics, to allow for building and computer access for authorized individuals. DHS and other agencies have been developing these new ID cards, although it is our understanding that work is continuing on the implementation of technologies to make full use of these cards. What is the current timeline for the implementation of HSPD 12 functionality across DHS? How much is it expected to cost?

ANSWER: DHS' milestone for completion of DHS Personal Identity Verification (PIV) card issuance to employees and contractors is December 31, 2010. DHS plans to meet this milestone by issuing cards in a three-phased approach starting with issuance in the National Capital Region, followed by issuance in several major US cities, then expanding to include the remainder of employees and contractors nationwide.

DHS anticipates needing to provide surge support in terms of labor to complete initial card issuance and also anticipates upfront costs for purchase of initial HSPD-12 required technology.

Estimated program cost is \$46,250,000 for a population of 250,000 to complete DHS PIV card issuance by 2010. This is an estimated per person cost of approximately \$185. These cost estimates are based on an enterprise approach centrally managed by DHS Headquarters.

These cost estimates are based on an enterprise approach centrally managed by DHS Headquarters. If funding is not available for a single collaborative effort, each Component will be required to conduct their own implementation and total costs will be higher. It is estimated that costs for Component-specific implementation would be at least \$20 million more over a five-year period.

Question: Does the Administration plan to review or alter the implementation of HSPD 12?

ANSWER: To date, implementation of HSPD-12 continues.

Question: What will happen to the biometric information of people issued HSPD 12-compliant IDs when they leave government service?

ANSWER: Currently, biometric information is stored on the HSPD-12-compliant IDs and within the identity management system with access information.

The retention policy is as follows: Records relating to persons' access covered by this system are retained in accordance with General Records Schedule 18, Item 17 approved by the National Archives and Records Administration (NARA). For security facilities, records of access are maintained for five years and then destroyed unless retained for specific, ongoing security investigations. For other facilities, records are maintained for two years and then destroyed. All other records relating to individuals are retained and disposed of in accordance with General Records Schedule 18, item 22a, approved by NARA. Records are destroyed upon notification of death or not later than five years after separation or transfer of employee, whichever is applicable.

The policy is also being updated to reflect this addition: In accordance with HSPD-12, PIV Cards are deactivated within 18 hours of cardholder separation, loss of card, or expiration. The information on PIV Cards is maintained in accordance with General Records Schedule 11, Item 4. PIV Cards are destroyed by cross-cut shredding no later than 90 days after deactivation.

Airport Credentialing and Biometrics:

Question: In the aviation environment, airports have operated robust access control systems linked to identity verification with airport-issued badges. Most agree that incorporating biometrics into existing, locally controlled credentialing and access control processes is important. Many airports and TSA are working to accomplish that goal. What is the federal government currently doing to encourage the deployment of biometrics in the airport environment?

ANSWER: DHS has worked closely with the aviation community toward development of standards for the use of biometrics in the airport environment. Specifically, two key standards have been developed. The first entitled, RTCA 230B "Integrated Security System Standard for Airport Access Control," provides standards and guidelines for implementing access control systems in the context of an integrated security system for an airport. The document provides guidance on acquiring and designing such systems, testing and evaluating system performance, and operational requirements. The document incorporates the latest technological advances in security access control systems and identity management technologies, including smart cards and biometrics. The second is a joint TSA-industry effort entitled Aviation Credential Interoperability Solution (ACIS).

The goal of ACIS is to enhance personnel credentialing standards across the industry by leveraging best practices within processes and applying open technology standards where appropriate. DHS seeks to leverage significant government credentialing expertise and investments, support consistency in policy across the various stakeholders, and enhance screening efficiency. Airports and airlines would continue to collect and submit vetting requests, adjudicate criminal history records check results, issue cards, and manage physical access. This approach supports enhanced biometrics-enabled identity verification and physical access control security capabilities within existing roles and responsibilities of the various entities involved in the screening, credentialing, access control and decision making processes.

Question: Does it make sense to build on the locally controlled access control and credentialing system already in place at airports?

ANSWER: Yes. Airports have a significant start in terms of their screening, credentialing and access control business processes. In terms of technology, however, DHS is encouraging airports to work toward an interoperable framework as they build for the future state, specifically the implementation and use of airport biometric access control systems interoperable with FIPS 201 standards. Where practicable, airports should explore biometric access control systems and identity verification technologies that will enhance the airport's ability to reduce unauthorized access and verify user identity.

Biometrics are clearly the access control media of the future. Investment in this media is costly and dictates that future planned airport construction and refurbishment projects be the methods by which the technology installation happens.

In addition the incorporation of biometrics involves a major training initiative by the user to ensure that employees use the system correctly. This in itself is a major task that must be phased over time.

Question: It is my understanding that a handful of airports are working to develop and implement standards for biometric based access control systems. Is DHS involved in that process? Are you encouraging it?

ANSWER: Yes, TSA, in collaboration with the aviation industry associations and airports, is reviewing best practices to effectively control and monitor airport employee portals and perimeter fences. Where possible,

TSA encourages voluntary implementation of technology by airport operators, such as biometric credentials and corresponding physical access control systems. However, to ensure that airport systems incorporate up-to-date standards and that TSA receives adequate information to conduct background checks, TSA is reviewing the possibility of establishing minimum standards through rulemaking. Rulemaking would seek to codify the standards and ensure consistency in data collection, card information configuration, and biometric information.

As previously stated in response to the above recommendation, TSA also posted three documents, the Aviation Credential Interoperability Solution (ACIS), ACIS-Basic Comparison Matrix and the Biometric Definition and Terminology Document for airports and industry to review and comment. This document discusses many of the technical issues TSA will consider in establishing standards.

TSA also encouraged the airport operators to refer to the RTCA DO 230-B Integrated Security Standards for Airport Access Control document posted on their website on June 25, 2008. This document aggregates industry best practices for employment of perimeter security measures, including biometric smart card control points and complements the ACIS concept.

On December 10, 2008, TSA issued Security Directive (SD) 1542-04-08F, which requires airport operators to submit additional biographical information enhancing the TSA security threat assessments (STA). These individuals are perpetually vetted against various databases until such time as they no longer hold an airport identification media. TSA via the same SD encourages airports to implement and use biometric access control systems aligned with FIPS 201 standards. Where practicable, airports should explore biometric access control systems and identity verification technologies that will enhance their airport's ability to reduce unauthorized access and verify user identity.

Question: Currently, the role of the federal government in airport credentialing centers around vetting individuals who have applied for airport badges. However, in the 2010 budget blueprint, there is \$64 million that will be used for vetting and credentialing programs. Will some of this funding be used to take a more active role with airport employee identity verification? If so, what will the federal government do that local governments or airport authorities may currently be doing?

ANSWER: Congress has not provided funds to support biometric access control pilots or to support initial airport implementation. The \$64 million within the FY 2010 Budget Request are to support ongoing TSA screening process, system enhancement, and modernization efforts. With these resources, TSA supports the ongoing screening, vetting, and adjudication of various programmatic efforts as authorized by Congress (for example, SIDA badge holders, TWIC, HAZMAT).

DHS is participating in standards efforts for the aviation community, is providing subject matter expertise and seeks to leverage key policy efforts, technology pilot efforts, and open standards development efforts for similar interoperable programs. Currently, airports can seek FAA AIP Funds and DHS Grants to augment implementation of enhanced credentialing and biometric capability.

Question: If DHS supports a more active role, similar to the TWIC program, do you envision scrapping the system currently in place at airports with a new credentialing and access control system or upgrading it?

ANSWER: DHS actively works with airports today to support their credentialing of individuals with SIDA access by performing robust background checks and developing standards. Any enhancements to the systems currently in place at airports would involve a similar delineation of responsibilities between DHS and the airports. In terms of the technology, DHS is encouraging a movement toward FIPS-201 interoperable credentials that would build upon the current credentialing and biometric systems within airports. Cost and

technical integration with existing systems was a high priority within NIST development and Departments' and Agencies implementation of FIPS-201 standards and systems.

Global Entry

Question: In 2006 CBP began work on a fully integrated system of international Registered Travelers under the Global Entry System (GES). The Privacy Impact Assessment of the system noted that some biometric information that would have been maintained in GES is maintained in the IDENT database to eliminate redundancy. Why is only some of the information being stored in IDENT or the biometric storage system (which contains all biometric data captured by USCIS) rather than all of it? Where will the remainder of the biometric data be stored?

ANSWER: All biometric data for Global Entry is stored in IDENT. CBP's Global Enrollment System (GES) no longer stores any biometric data.

Global Entry is operated by CBP, operates at seven airports and has fewer than 10,000 enrollees. Its domestic counterpart, the Registered Traveler program, is operated by TSA-approved private sector service providers at security checkpoints at 20 of our largest airports and has more than 250,000 enrollees already. Registered Traveler has biometrically verified travelers at airport checkpoints more than 2 million times in its brief life. Neither program currently has the ability to enroll individuals in the other, even though the programs require applicants to provide virtually identical biographic and biometric data and the programs are managed by sister agencies within DHS.

Question: Global Entry is operated by CBP, operates at seven airports and has fewer than 10,000 enrollees. Its domestic counterpart, the Registered Traveler program, is operated by TSA-approved private sector service providers at security checkpoints at 20 of our largest airports and has more than 250,000 enrollees already. Registered Traveler has biometrically verified travelers at airport checkpoints more than 2 million times in its brief life. Neither program has the ability to enroll individuals in the other, even though the programs require applicants to provide virtually identical biographic and biometric data and the programs are managed by sister agencies within DHS. What steps are being taken to leverage these two programs, and if appropriate, cross-enroll trusted travelers, possibly with private sector partnerships? What efficiencies and security benefits might come from such coordination?

ANSWER: The overlap of activities between Global Entry and Registered Traveler is minimal. Global Entry is a DHS screening program in which the government performs applicant interviews and conducts extensive screening on applicants for membership and recurrent checks on members. Registered Traveler is a private sector program without a government vetting component. As of July 2008, TSA no longer receives, stores or manages any applicant information nor does it perform any screening of applicants or members.

As you note, applicants for the two programs are asked to provide much of the same information. For Global Entry, applicants currently submit biographic data online via CBP's Global Online Enrollment System (GOES) and biometrics in person before the CBP officer. For Registered Traveler, the applicant submits it directly to the Registered Traveler vendor. Potential exists to build bridges between private sector entities and GOES that already have the necessary biographic data to allow the transmission of that data to CBP with permission from the individual. The Federal Register Notice launching the Global Entry pilot explicitly recognizes that the opportunity to provide enrollment data via private sector entities will be considered as program develops.

Accepting enrollment data via private sector entities might provide convenience to the Global Entry applicant who had previously provided the biographic information to a Registered Traveler vendor.

Because CBP's costs for receiving Global Entry application data through GOES are minimal, however, allowing the individual to authorize the Registered Traveler vendor to provide the data to CBP would not result in a reduction of fees for applicant. CBP and the private sector would also have new costs related to building the information technology security measures necessary to meet government requirements and privacy standards.

Registered Traveler

Question: In July 2008, a laptop containing the personal data of 33,000 passengers, almost a fifth of the enrolled travelers in the largest Registered Traveler contract, went missing for a week and a half. In violation of TSA rules, the data was stored in an unencrypted file. A biometric identifier may be thought of as a password that can never be lost – but it also can never be changed if someone else is able to duplicate it. How can U.S. travelers be sure personal information and biometric data is secure, and that there are safeguards to keep records from being compromised, altered or misused? What changes have been made to the RT program as a result of this incident?

ANSWER: TSA requires Registered Traveler service providers and sponsoring entities to encrypt all files containing participants' sensitive personal information. Noncompliance with such requirements can result in actions including suspension of a program and possible civil penalties.

On August 4, 2008, TSA suspended Verified Identity Pass, Inc. (VIP) from enrolling new applicants in Registered Traveler (RT) due to vulnerabilities discovered in the company's storage of Clear® applicants' sensitive personal information. The vulnerabilities came to light after an unencrypted VIP laptop computer was discovered to be missing from San Francisco International Airport (SFO). TSA instructed SFO as VIP's sponsoring entity to notify immediately the individuals impacted, suspend enrollment, cease use of any unencrypted computers and secure the devices until encryption can be installed. The suspension protected consumers waiting to enroll in RT and allowed VIP to bring its procedures into compliance. VIP was required to submit an independent audit, verifying that the required security measures were in place before the suspension was lifted on August 11.

TSA contacted all Registered Traveler service providers to reaffirm proper security measures were in place, including encryption of sensitive personal information of participants.

TSA asked VIP to provide a comprehensive report detailing the status of all security features associated with the Clear® program and to conduct a new and complete annual audit consistent with program standards.

Question: What occurs to data on Registered Travelers who withdraw from the program?

ANSWER: TSA requires RT vendors to develop, implement, and make available to their members privacy statements. Those statements and company policy govern the retention and disposal of data held by the private sector.

TSA no longer collects, receives, manages nor stores personal data on RT member since the end of the RT pilots. Limited biographic information was transmitted to TSA during the pilots for vetting. TSA is in the process of disposing that information in accordance with its privacy governance documents and records retention schedule.

QUESTIONS FOR THE RECORD SUBMITTED BY

THE HONORABLE HAROLD ROGERS

**Ms. Kathleen Kraninger, Deputy Assistant Secretary for Policy, DHS Screening
Coordination Office
Mr. Bob Mocny, Director,
United States Visitor and Immigrant Status Indicator Technology
Biometric Identification**

TWIC

Question: What is DHS doing to ensure a more expeditious processing and activation of TWICs?

ANSWER: Several actions are ongoing to expedite the processing and activation of TWICs. For example: The current activation time is about 8.5 minutes. The certificates are now being loaded on the cards at the enrollment sites by the trusted agents before the individual worker returns to the enrollment center to activate their card. This has reduced the activation time to 1-3 minutes for individual workers allowing more workers to get cards across the enrollment sites. In addition, system enhancements are planned to ensure the correct immigration documentation is collected during the enrollment process. This will reduce the number of immigration cases during the adjudication process significantly reducing the time to get a TWIC for those born outside of the United States.

Screening Coordination

Question: Please explain DHS's efforts to consolidate and coordinate the various background checks across the Department's screening and credentialing programs?

ANSWER: The Screening Coordination Office (SCO) was established to identify opportunities to harmonize and enhance screening processes across DHS "people screening" programs and move toward harmonization in an effective and efficient manner. In order to meet its mission, the SCO worked with program managers to identify core problem areas within DHS screening and credentialing, such as: inefficient information and data collection, the issuance of multiple credentials, inconsistent vetting processes for like programs and re-vetting of the same individuals, and reliance on visual inspection of credentials.

The DHS Credentialing Framework addresses these problem areas through a set of strategic objectives, including: designing credentials to support multiple licenses, privileges, or status, based on the risks associated with the environments in which they will be used; designing enrollment platforms and data collection investments so that they can be reused by other DHS programs where appropriate; ensuring that vetting, associated with like uses and like risks, should be the same; that entitlement to a license, privilege, or status should be verified using technology; that immigration status determinations by DHS components should be verified electronically; and that we should ensure opportunities for redress – individuals should be able correct information held about them. Through the investment review, enterprise architecture and budget processes and through program reviews, the SCO is overseeing the consolidation and coordination of business processes and IT systems where appropriate.

Screening Redundancy with TWIC and HAZMAT

Question: Within the Department's screening coordination efforts, has DHS issued any guidance to the States regarding the fact that TWIC holders have already undergone the screening requirements for applicants seeking Hazmat Endorsement? If not, please explain whether any such guidance will be issued in the near future, or explain the need for such redundancy.

ANSWER: DHS is working to implement process, technology, and operational changes that will allow states to issue Hazardous Materials Endorsements (HME) to drivers who already have undergone screening for the TWIC program and for drivers to obtain a reduced fee HME if they take advantage of their comparable TWIC screening as was done for HME holders who applied for TWICs. DHS will issue guidance to the States on how they can take advantage of the new processes, as well as a revised fee rule for HME holders who wish to take advantage of their comparable TWIC screening.

THURSDAY, MARCH 26, 2009.

**DEVELOPING AND TRANSITIONING HOMELAND
SECURITY RESEARCH PRODUCTS INTO USE**

WITNESS

**BRADLEY BUSWELL, ACTING UNDERSECRETARY FOR SCIENCE AND
TECHNOLOGY, DEPARTMENT OF HOMELAND SECURITY**

Mr. PRICE. The Subcommittee will come to order. Good morning.

Today we have before our Subcommittee Bradley Buswell, the Acting Undersecretary for Science and Technology, Directorate at DHS, to discuss how the Agency develops and translates advanced research into operational homeland security products.

Welcome, Mr. Buswell.

Mr. BUSWELL. Thank you. It is great to be here.

OPENING STATEMENT OF CHAIRMAN PRICE

Mr. PRICE. Today one of our main focuses is to obtain greater understanding of how S&T identifies and selects promising technologies for further development, and how you find ways to efficiently leverage existing technologies into new uses.

Your predecessor as Director took a proactive stance, seeking to ensure that the research S&T undertook was relevant to the operational needs of the components with DHS. We would like to hear from you how you are continuing these efforts, and how you are building upon them.

S&T is a very young agency, formed when DHS was created in 2003. In its infancy, we were concerned that it was replicating research done either by other federal government entities or by other DHS agencies.

In 2008, this Subcommittee commissioned a study by the National Academy of Public Administration to look at how S&T's research portfolio fits into the broader scope of research in the federal government, to assess that portfolio on its own terms, and also to assess the fit, the complementarity, between the DHS portfolio and what is going on elsewhere in the federal establishment. This review we anticipate will be completed in June.

In the meantime, we are interested in discussing what specific steps S&T is taking to ensure that efforts within the innovation portfolio in particular are not duplicative or research that either precedes it or is going on elsewhere in the government or in DHS; how S&T coordinates its work within the department; and how other DHS components test and utilize technology S&T develops in their own work, so that promising technologies do not sit on the shelf.

Recently some disturbing news surfaced about internal coordination with S&T related to the Biowatch program. We have been told

that one component of S&T is field testing a biowatch prototype without coordination, while the Test & Evaluation and Standards Office, which claims they do not have any access to any of that data.

Now, we will be holding a hearing later this year to discuss the specific challenges that the Biowatch program poses. But this, I believe, is a good example of what we need you to be mindful of as S&T executes the Fiscal Year 2009 budget that we approved, and as we consider the budget going forward.

At our hearing with S&T last year we talked at length about better ways to include the private sector in the development of new technologies, as well as S&T's role as a technology clearinghouse for Homeland Security-related research.

We continue to have a strong interest in improving S&T's capacity to evaluate promising technologies and research proposals from outside.

S&T's upcoming installation of Resilient Electric Grid technology in New York City is a great example of how the Agency should be leveraging prior investments, both public and private, to accomplish the mission. This technology would help prevent the spread of blackouts, such as we saw in 2003, and it could maintain power in more areas affected by a disaster by isolating blackouts before they spread.

We would like to hear about your recent accomplishments and upcoming plans for this promising technology.

Finally, just last week, in our hearing on interoperability we discussed the importance of field demonstrations and pilot programs. This is surely an integral step in S&T's technology development process. Because a large portion of your budget has been devoted to these efforts, it would be helpful if you could discuss some recent pilots S&T has been involved in since our hearings last year, and your future plans for performing demonstrations with your customers.

Obviously, pilot programs serve a couple of critical functions. They demonstrate the linkage that I mentioned earlier between research and the practical applications, the missions of the agencies. They give us a way of making a test run before investing a huge amount of dollars in deployment of technologies or programs.

Before we begin, I would like to point out that while S&T's university programs are not the main focus of this hearing, we should not downplay the crucial role basic research plays in a homeland security environment. This type of investment helps us gain a greater understanding of the world around us, which in turn affords us greater insight into how we can better provide disaster relief, for example, or more effectively protect our borders with technological advances.

So Mr. Buswell, we look forward to your testimony. Please summarize your oral statement if you will, in about five minutes, and your entire written statement will be placed in the record.



COMMITTEE ON APPROPRIATIONS

David Price (D-NC), Chairman, Subcommittee on Homeland Security

FOR RELEASE UPON DELIVERY

Media Contact:
Phil Feagan

Thursday, March 26, 2009
202-225-1784

OPENING STATEMENT OF CHAIRMAN DAVID PRICE
Developing and Transitioning Homeland Security Research Products
Into Use
March 26, 2009 / 10:00 am

This morning we have before the Subcommittee Mr. Bradley Buswell, Acting Under Secretary for the Science and Technology (S&T) Directorate at DHS to discuss how the agency develops and translates advanced research into operational homeland security products.

Welcome Mr. Buswell.

Today, one of our main focuses is to obtain a greater understanding of how S&T identifies and selects promising technologies for further development, and how you find ways to efficiently leverage existing technologies into new uses. Your predecessor took a proactive stance, seeking to ensure that the research S&T undertook was relevant to the operational needs of the components within DHS. We would like to hear from you about how you are continuing these efforts.

S&T is a very young agency, formed when DHS was created in 2003. In its infancy, we were concerned that it was replicating research done either by other Federal Government entities or by other DHS agencies. As such, in 2008, this Subcommittee commissioned a study by NAPA to look at how S&T's research portfolio fits into the broader scope of research in the

Federal Government. This review should be completed in June. In the interim, we are interested in discussing: what specific steps is S&T taking to ensure that efforts, within the Innovation portfolio in particular, are not duplicative of research that either precedes it, or is ongoing elsewhere in DHS; how does S&T coordinate its work within the Department; and how do other DHS components test and utilize technologies S&T develops in their own work so that promising technologies don't sit on the shelf.

Recently, some disturbing news surfaced about internal coordination within S&T related to the BioWatch program. Specifically, we have been told that one component of S&T is field-testing a Bio Watch prototype, without coordination with the Test & Evaluation and Standards Office, which claims they don't have access to any of that data. Although we will be holding a hearing later this year to discuss the specific challenges related to the BioWatch program, this a good example of what we need you to be mindful of as S&T executes the fiscal year 2009 budget that we approved, and as we consider the upcoming fiscal year's request.

At our hearing with S&T last year, we talked at length about better ways to include the private sector in the development of new technologies, as well as S&T's role as a technology clearing house for homeland security-related research. We continue to have a strong interest in improving S&T's capacity to evaluate promising technologies and research proposals from outside. S&T's upcoming installation of "Resilient Electric Grid" technology in New York City is a great example of how they should be leveraging prior investment, both public and private, to accomplish their mission. This technology would help prevent the spread of blackouts such as we saw in 2003, and could maintain power in more areas affected by a disaster by isolating blackouts before they spread. We would like to hear about your recent accomplishments and upcoming plans for this promising technology.

Finally, just last week, at our hearing on Interoperability, we discussed the importance of field demonstrations and pilot programs. This surely is an integral step in S&T's technology development process. Because a large portion of your budget has been devoted to these efforts, it would be helpful if you could discuss some recent pilots S&T has been involved in since our hearing last year and your future plans for performing demonstrations with your customers.

Before we begin, I would like to point out that while S&T's University Programs are not the main focus of this hearing, we should not downplay the crucial role basic research plays in a homeland security environment. This type of investment helps us gain a greater understanding of the world around us, which, in turn, affords us greater insight into how we can better provide disaster relief, for example, or more effectively protect our borders with technological advances.

Mr. Buswell, we look forward to your testimony. Please summarize your oral statement in about five minutes as your entire written statement will be placed into the record. But before your testimony, let me turn to the distinguished ranking member, Mr. Rogers, for any comments he may wish to make.

###

Before we begin, I want to turn to the distinguished Ranking Member, Mr. Rogers, for his comments.

OPENING STATEMENT OF RANKING MEMBER ROGERS

Mr. ROGERS. Thank you, Mr. Chairman. And welcome to Undersecretary Buswell.

By just about anyone's measure, S&T's effectiveness or its ability to field technical solutions to meet our homeland security challenges has been mixed over the last six years.

On the one hand, S&T has delivered some useful products, including the Dazzler non-lethal weapon, cyber security tools, and mobile biometric readers used by the Coast Guard to identify illegal immigrants and smuggling suspects in the waters off Florida and Puerto Rico.

The Directorate has also made strides in organizational layout and a reasonable budget framework, including basic research, innovation investments, and transition to the field.

But on the other hand, S&T has failed to deliver on what appear to be some straightforward technological challenges. Most notably, my favorite project, the container security device, the CSD. We have been talking about this ever since we formed the Department, even before. And after almost four years of work, S&T and CBP have utterly failed to produce a viable security container device that will simply tell us whether or not a container was tampered with in transit. It baffles me.

In the time we have devoted to the container security device, our country invented the atomic bomb and sent men into space, achievements that should not even be mentioned in the same sentence as the container security device. And yet the device is an achievement that is still sadly out of reach.

I have a long-held view that a workable technology solution exists that can provide some level of assurance for the integrity of inbound cargo containers, especially in high-risk trade lanes. And this subcommittee has prioritized such a development, and yet, here we are, still waiting.

There are also several other key homeland security challenges where the development of an effective technical solution would vastly improve operations. Whether it is a viable exit reader for our land ports that we have heard about just last week at our US-VISIT hearing, our foliage-penetrating radar that CBP could use to better detect unauthorized entries along the borders, there are plenty of problems that need solving.

And that is precisely why S&T exists. I remember a time when we were talking about the need in Homeland Security for something similar to DARPA at Defense. And S&T I think really was a product of that conversation. And then we decided to create a HSARPA, a Homeland Security research group.

I am of the firm belief that private industry holds the answers to technical challenges like we have talked about. So we need to continue probing how S&T can best access the talent and innovation that only resides in the commercial sector, in the private sector.

As many of us can recall, we heard from CIA's venture capital arm last year, known as In-Q-Tel, in our hearing. And they made

a very compelling case, I thought, for how to harness the ingenuity of the private sector.

I would like to hear about your progress in doing just that. Because after all, S&T's success is ultimately determined by the products and solutions it actually delivers. Whether it is first responders communicating in the midst of an ice storm, like we saw a month ago in Kentucky, where a S&T project was used to establish interoperative communications from an area where all communications had been snuffed out—I forgot the name of the project—MITOC, yes, M-I-T-O-C, which is an S&T creation. Incidentally, coincidentally, manufactured or put together by the University of Louisville and Western Kentucky University as another product of the work of this subcommittee.

Or it could be border patrol agents interdicting smugglers in Arizona. Our front-line operators are counting on the scientists and engineers of S&T to evaluate and deliver the tools that enhance their work and improve our homeland security.

Mr. Chairman, thank you for the time. I look forward to our discussion.

[The information follows:]

OPENING STATEMENT

CONGRESSMAN
Hal Rogers



FIFTH DISTRICT • KENTUCKY

Offices in
Washington, D.C.
Somerset, Prestonsburg,
Hazard

Contact: Stefani Zimmerman

202.225.4601

Opening Statement
Subcommittee on Homeland Security Appropriations

Developing and Transitioning Homeland Security Research Products into Use
Witness:

Brad Buswell, Acting Under Secretary, Science and Technology Directorate
10:00 AM | Thursday | March 26, 2009 | 2358-A

Thank you Mr. Chairman, and welcome to Under Secretary Buswell.

By just about anyone's measure, S&T's effectiveness – or its ability to field technical solutions to meet our homeland security challenges – has been mixed over the last six years.

On one hand, S&T has delivered some useful products, including: the Dazzler non-lethal weapon, cyber security tools, and mobile biometric readers used by the Coast Guard to identify illegal immigrants and smuggling suspects in the waters off Florida and Puerto Rico. The Directorate has also made strides in organizational layout and a reasonable budget framework including basic research, innovation investments, and transition to the field.

But on the other hand, S&T has failed to deliver on what appear to be some straightforward technological challenges—most notably, the Container Security Device or CSD.

⇒ After almost four years of work, S&T and CBP have utterly failed to produce a viable CSD that will simply tell us whether or not a container was tampered with in transit.

⇒ This failure baffles me. In the time we've devoted to the CSD, our country invented the atomic bomb and sent men into space – two scientific achievements that should not be even mentioned in the same sentence as the CSD. And, yet, the CSD is an “achievement” that is still sadly out of reach.

⇒ I have long held the view that a workable technology solution exists that can provide some level of assurance for the integrity of inbound cargo containers – especially in high-risk trade lanes. And this Subcommittee has prioritized such development, and yet we're still waiting.

There are also several other key homeland security challenges where the development of an effective technical solution would vastly improve operations. Whether it's a viable exit reader for our land ports of entry that we heard about just last week at our US-VISIT hearing, or foliage-penetrating radar that CBP could use to better detect unauthorized entries along the our borders, there are plenty of problems that need solving.

And that's precisely why S&T exists.

I am of the firm belief that private industry holds the answers to technical challenges such as these – so we need to continue probing how S&T can best access the talent and innovation that only resides in the commercial sector. As many of you recall, we heard from CIA's venture capital arm known as "In-Q-Tel" at last year's S&T hearing and they made a compelling case for how to harness the ingenuity of the private sector.

Today, I'd like to hear about S&T's progress at doing just that.

After all, S&T's success is ultimately determined by the products and solutions it actually delivers. Whether it's first responders communicating in the midst of an ice storm or Border Patrol agents interdicting smugglers in Arizona, our front line operators are counting on the scientists and engineers of S&T to evaluate and deliver the tools that enhance their work and improve our homeland security.

Thank you, Mr. Chairman, I look forward to today's discussion.

###

Mr. PRICE. Thank you. Mr. Buswell, please proceed.

OPENING STATEMENT OF BRADLEY BUSWELL

Mr. BUSWELL. Good morning, Chairman Price, Ranking Member Rogers, and distinguished members of the committee. I am honored to appear before you today for the first time in my acting role as Undersecretary for Science and Technology, and I am delighted to update you on the progress and accomplishments of the S&T directorate in providing technological capabilities to our customers, the operating components of DHS, and also importantly, the nation's first responders.

First, let me say that I am grateful for the immediate and strong leadership and support of Secretary Napolitano. From day one in her seat, she has been very supportive of S&T, and has consistently emphasized the importance of Science and Technology in accomplishing all of the missions of the Department, as has been mentioned already this morning in your opening statements. I value the opportunity to support that, and accept the accompanying responsibility.

I am also very appreciative of the leadership of this Committee, and the support of the Directorate's endeavors, the informed counsel. There is no substitute for the informed counsel of Committee members and staff. And it has been critical to the Department's success in positioning S&T up to this point for accountability and tangible results, for today and into the future.

The Committee is well aware of the Directorate's efforts over the last couple of years to reorganize its structure, its research portfolio, its business operations in order to expedite the delivery of technology to our customers. And I am proud to report that these efforts are taking hold, and the Directorate is delivering.

We are successfully maturing our 12 Capstone Integrated Product Teams (IPT) that we use to identify the highest priority technology needs of our DHS operating components. And in the last month we have also added a thirteenth IPT that is focused on the needs of the state and local first responders, our nation's heroes that are out on the front lines of homeland security every day. We are delivering products across the spectrum of, across the spectrum of homeland security.

You mentioned, Mr. Chairman, the Innovation portfolio. We are very proud of that portfolio, particularly because it is new. It began two years ago, as we started the reorganization of the Directorate, and it is providing exciting, innovative solutions to homeland security problems that are higher risk than the operating components are willing to take in their acquisition programs. But that is why we have S&T.

We can talk about, you mentioned the Resilient Electric Grid, we can talk more about that. We had a recent test. We have a levee-strengthening and damage-mitigation technology that is, that will prove, I think, to be a critical component in levee barriers, stopping the flooding. And then things such as the Magnetic Visibility MAGVIZ, which is the magnetic resonance-based security checkpoint device that will help us screen liquids going on the aircraft, or any other, any other checkpoint situation.

You mentioned the basic research portfolio. We are executing that at laboratories and universities across the nation and around the world, to keep that technology pipeline full into the future.

So I guess in conclusion, I am looking forward to talking more specifically about the things that you would like to hear about. But I want to say that I am honored to serve with the talented scientists and engineers and other professionals who support them in this mission, to field technologies that protect our homeland and defend our freedom. And I am looking forward to continued, to continued interaction with this Committee and the support of the Committee in accomplishing those missions.

So thank you again for the opportunity to appear, and I look forward to your questions.

[The information follows:]

Statement for the Record

Bradley I. Buswell
Under Secretary (Acting), Science and Technology Directorate
Department of Homeland Security

Before the U.S. House of Representatives
Committee on Appropriations
Subcommittee on Homeland Security

March 26, 2009

INTRODUCTION

Good Morning, Chairman Price, Ranking Member Rogers, and distinguished Members of the Committee. I am honored to appear before you today to update you on the progress of the Department of Homeland Security's (DHS) Science and Technology Directorate (S&T Directorate). I also plan to detail the Directorate's many accomplishments from the past year; discuss current programs on track to provide future technological capabilities to our customers, the operating components of DHS and our Nation's first responders; and describe how our efforts are helping to unify the Department.

I am grateful for the immediate and strong leadership of Secretary Napolitano. She is committed to the mission of the Department: protecting the Nation from terrorist threats and promoting a nation-wide culture of preparedness for dealing with natural disasters. The Secretary has also testified to the importance of greater use of science and technology in improving our capabilities to accomplish that mission. I am pleased to report to you the S&T Directorate has been successful in improving our capabilities across the extremely diverse homeland security mission set.

I am very appreciative of the leadership of the Congress in supporting of the Directorate's endeavors. I am also grateful for the engaged and non-partisan relationship we enjoy. The informed counsel of Committee Members with homeland security oversight, and that of their staffs, has been invaluable to the Department's efforts to position the S&T Directorate for accountability, tangible results, and success – both today and for the future.

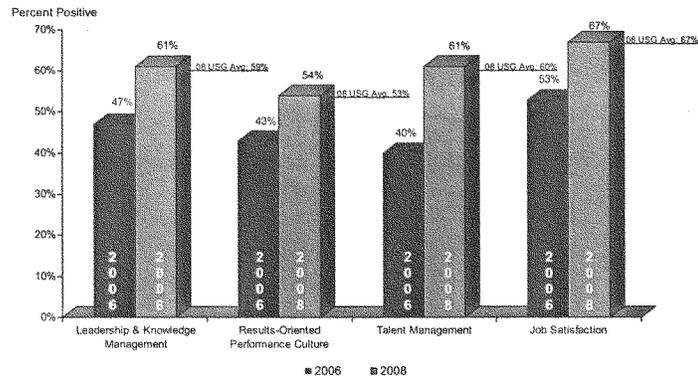
The Committee is familiar with the Directorate's efforts over the past two years to reorganize its structure, research portfolio, and business operations in order to expedite the delivery of cutting edge technological solutions to our customers. I am proud to report that these efforts have been successful, and the Directorate is now fully focused on fulfilling our customers' near-term and long-term technological capability needs. I am obliged to update the Committee on the status of the Directorate's personnel and processes before we focus on the myriad technological achievements we have provided, or will provide, to our customers.

SUCCESSFUL TURNAROUND – PEOPLE & PROCESS

People

I am honored to serve with the many talented scientists and engineers, and other professionals who support these dedicated Americans in our shared mission to field technologies that secure our homeland and defend our freedoms. The Directorate has seen significant improvement in workforce morale over the past two years. This is best highlighted by the results of the 2008 Federal Human Capital Survey which clearly indicate that we are making noteworthy progress on the management shortcomings that previously hindered the Directorate's performance. The 2008 results demonstrate dramatic improvement for the Directorate since the 2006 survey, and indicate that S&T is now on par with the Federal government as a whole.

2008 Federal Human Capital Survey DHS Science & Technology



While I am pleased with the results of our efforts over the past two years, I am not satisfied. There are still areas that need attention, and I am committed to maintaining the momentum.

Process

Basic Research. The Directorate's basic research portfolio addresses long-term research and development needs in support of DHS mission areas that will provide the nation with an enduring capability in homeland security. This type of focused research investment has the potential to lead to paradigm shifts in the nation's homeland security capabilities through investment in our universities, government laboratories, and the private sector.

During this past year, in order to facilitate better integration and coordination of effort within S&T, the Director of Research established a Research Council and developed the initial draft of the DHS S&T Basic Research Strategic Plan. This plan will outline our strategy for basic research and codify best practices from the members of the Research Council and other stakeholders in the basic research community. To further refine the metrics used in all the Directorate's portfolios, we initiated a contract for the National Academies of Science to study this issue.

Additionally, to better communicate the areas of research in which the Directorate is interested, we issued the initial draft of our basic research focus areas and met with our customers and university and laboratory partners to refine them based not only on what is desirable, but also what is realistically achievable within the realm of cutting edge research. In the coming year we

will be distributing the refined version of these basic research focus areas so as to improve communications between S&T and others on our basic research portfolio, thereby encouraging interaction and helping interested stakeholders to provide applicable research efforts.

Innovation. The Directorate's Homeland Security Advanced Research Programs Agency (HSARPA) has implemented a transparent process for identifying, prioritizing, and selecting new High Impact Prototypical Solutions (HIPS) and High Impact Technology Solutions (HITS) projects in the Innovation budget line and has used this process to re-evaluate existing projects and to select future "new start" projects.

The first step is for the HSARPA staff and other members of the Directorate to gather ideas for potential new HIPS and HITS projects from documented needs of DHS customers, solicitations and proposals, discussions with S&T stakeholders, technology conferences and symposia, university, laboratory and industry interaction, and international collaboration. Next, the Director of Innovation/HSARPA screens the list of potential projects to ensure that they meet the fundamental philosophy of the innovation portfolio, namely that though they still contain high risk, they offer substantially higher payoff than programs currently handled in the transition portfolio or an actual acquisition program of record. The Director then presents this list of recommended new start HIPS and HITS to the S&T Corporate Board to ensure the recommended efforts are not redundant with efforts already under way, and to obtain corporate board agreement that the recommended projects are neither more appropriate for the basic research or transition portfolios.

Following concurrence by the S&T Corporate Board, the Director of Innovation/HSARPA presents the list of recommended new starts to the Deputy Under Secretary and the Under Secretary for Science and Technology for concurrence. The final phase of the approval process takes place annually when the Under Secretary presents the recommended new starts to the DHS Technology Oversight Group (TOG) for approval. The TOG is chaired by the DHS Deputy Secretary with membership of the Under Secretary for Management and the Under Secretary for NPPD.

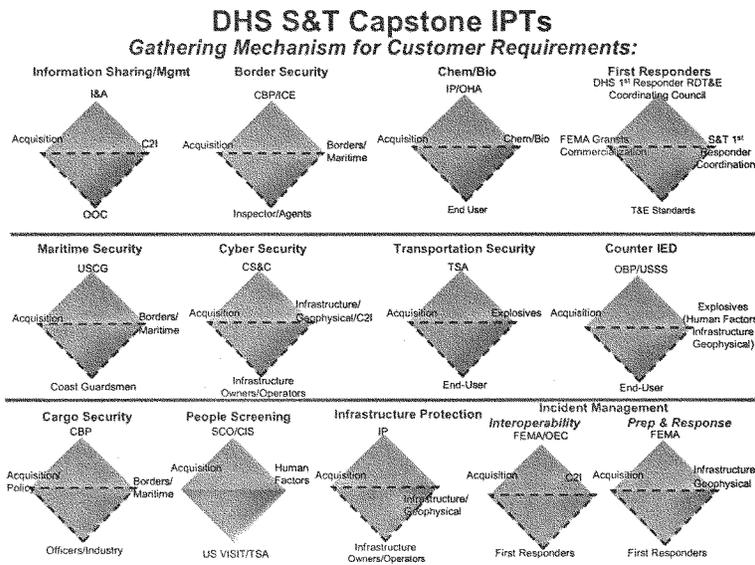
During the past year, HSARPA completed several demonstrations of prototypes that had been developed over the previous two years. Those demonstrations included:

- Future Attributes Screening Technology (FAST)
- Magnetic Visibility (MAGVIZ)
- Resilient Electric Grid (REG)
- Levee Strengthening and Damage Mitigation
- Tunnel Detection
- Biometric Detector
- Resilient Tunnel

The most important process that the Directorate uses is the one that puts us in direct contact with our customers: the Capstone Integrated Product Team (IPT) process. It ensures that we are identifying our customers' highest priority needs and providing near-term capabilities to address them. These Capstone IPTs engage DHS customers, acquisition partners, Directorate Division Heads, and end users as appropriate to align our research, development and product transition

activities to their requirements and acquisition activities. The science and technology solutions that are the outcome of this process, referred to as Enabling Homeland Capabilities, draw upon technologies that can be developed and delivered to our customer acquisition programs within three years. As with the Innovation Portfolio, the Under Secretary presents recommended new start programs to the DHS Technology Oversight Group (TOG) for approval.

Our experience over the last year has led us to maintain twelve Capstone IPT areas – Information Sharing/Management; Border Security; Chemical Defense; Biological/Agricultural Defense; Maritime Security; Cyber Security; Transportation Security; Counter IED; Cargo Security; People Screening; Infrastructure Protection; and Incident Management – and add a thirteenth to directly support first responders.



The thirteenth Capstone IPT was officially announced in February 2009 at the DHS S&T West Coast Stakeholder Conference in Bellevue, Washington. The conference focused exclusively on First Responder technology needs and existing technological gaps. As an aside, we had a substantial turnout from the First Responder community at Bellevue. The outreach initiative demonstrated at this conference is representative of the larger DHS-wide effort to identify First Responder needs and requirements and bring resources together to address the most pressing issues.

Within the various First Responder communities there are several mechanisms currently employed to research and identify First Responder technical requirements. While the First Responder Capstone IPT will not replace tried and true processes, it will formalize and align

those processes to the way the Directorate does business. The First Responder IPT will also allow the community to leverage the processes and relationship the Directorate has developed with the International Community, within the Interagency, and at our Universities.

In order to accomplish this, the IPT will formally establish an Emergency Services Sector Research, Development, Test, and Evaluation (RDT&E) Working Group comprised of representatives from the National Protection Programs Directorate (NPPD), the Office of Infrastructure Protection (OIP), the Emergency Services Sector Coordinating Council (SCC) and the Emergency Service Sector Government Coordinating Council (GCC). This group will serve as the primary engine for identifying technology gaps in the Law Enforcement, Fire, Emergency Management, and Emergency Medical Services areas. Because Federal Advisory Committee Act (FACA) rules apply when communicating RDT&E requirements to the Capstone IPT, a government-only unit comprised of members from the Assistant Secretary for State and Local Law Enforcement, the Office of Health Affairs, the Fire Administrator, and the GCC will officially represent the First Responder community to the IPT.

The Capstone IPT process for First Responders is similar to that of the other twelve IPTs. As technology gaps or technology needs are identified by the RDT&E Working Group, the Directorate will first examine the DHS S&T and FEMA investment portfolio to determine if the requested technology already exists or if R&D is currently underway in the interest area. If a solution is not available or research and development is not underway, the Commercialization Office will communicate the First Responder requirements to the private sector and solicit a solution. The Directorate will also begin the planning necessary to seek a technological solution. The FEMA Grants Office will provide input regarding the availability of grant money to support development and deployment of the requested technology. DHS T&E will play a substantial role in ensuring appropriate rigor is applied to the test and evaluation process and in the use of approved standards.

PRODUCT IS JOB ONE

Delivery of technological capabilities to our customers is the reason the S&T Directorate exists. In the past year, the Directorate has had numerous products which we have transitioned to our customers in the Capstone IPT capability areas, and we are on track to continue this performance in the future.

Transportation Security

Air Cargo Screening. In helping TSA meet its congressional deadline to screen 100 percent of air cargo carried on passenger planes by 2010, S&T conducted a number of assessments of Advanced Technology and X-ray machines. Machine and screener performance was evaluated for six different break-bulk systems. Because a majority of air cargo arriving at Independent Air Carriers (IAC) is on wooden pallets, the Directorate also conducted six initial assessments of palletized cargo screening systems. This will relieve IACs from having to break down pallets, screen the individual parcels, and build the pallet back to its original configuration. Over the past year, the Directorate has:

- Completed the congressionally-directed **Air Cargo Explosives Detection Pilot Program** which tested new concepts of operation for screening a significant percentage of air cargo above current levels. Conducted at the San Francisco, Cincinnati and Seattle international airports, the program examined different approaches to screening air cargo for explosives and stowaways. Analytical data, results, analysis and conclusions will be provided to TSA in order to determine how to best use new screening technologies and properly implement new explosives detection technology within the cargo handling systems at major US airports.
- Developed a **mass-spectrometry based trace explosives detection systems** for air cargo screening designed to reduce labor costs and false alarm rates. These systems will be evaluated by S&T and TSA in an operational environment beginning in spring 2009. If successful, these systems will undergo Independent Test & Evaluation against TSA detection standards.
- Developed a **Cargo Screening Metal Detector** to screen pallets of non-metallic air cargo (e.g., flowers, produce). The first prototype system will be delivered for testing by the Transportation Security Laboratory in June 2009. If successful, vendors and shippers can use this technology to screen their products for metal components of Improvised Explosive Devices streamlining the screening process.
- Evaluated the performance of a **modified Explosive Detection Systems (EDS)**, originally designed to be used for checked baggage, optimized for screening air cargo for explosives.

Checkpoint Screening. Developed technologies and concepts of operations for TSA to improve checkpoint screening systems throughput, capacity, reliability and effectiveness while minimizing false alarm rates and cost and labor. To support this program's customers, the Directorate:

- Developed a **Digital Imaging and Communications for Security (DICOS)** standard to serve as the standard image file format to enable data exchange between security screening equipment and allow threat detection algorithms to be used in x-ray based screening of checked baggage and carry-on luggage. The draft standard is expected to be released in late FY 2009, and will provide TSA with significant cost savings when acquiring technology by promoting competition among algorithm developers.
- Initiated evaluation of **Magnetic Visibility (MAGVIZ)**, a proof of concept program to identify by chemical name any liquid being carried through a security screening checkpoint. This system was tested at Sunport Airport in Albuquerque, NM, and successfully demonstrated the ability to detect and identify dangerous liquids surrounded by non-hazardous liquids in a 3-1-1 size container tray.
- Conducted **laboratory assessments** to support development of technical requirements for technologies concerned with Whole Body Imaging, Shoe Scanner Systems, and Carry-On Baggage Explosives Detection.
- Completed a prototype **Three-Dimensional Computed Tomography** system for use at checkpoints. These prototypes are down-scaled versions of the systems currently in use at large checked bag screening systems and provide improved explosives detection capabilities. These systems would be especially beneficial in smaller airports where they can serve as "dual use" systems, processing checked and carry on baggage in the same space constrained location. TSA will begin qualification testing for checkpoint use in FY 2009.

Home Made Explosives (HME). As a result of attempted and executed terrorist attacks involving Home Made Explosives (HME), particularly hydrogen peroxide threats, DHS recognized an urgent operational need to detect HME threats to the transportation infrastructure in the U.S. To combat this threat DHS has structured a HME program with the goals of (1) systematically determining the physical and chemical properties of HME threats; (2) identifying, evaluating and improving HME detection and screening methodology; and (3) developing, verifying and validating models to determine HME damage effects. To support this program's customers, the Directorate:

- Sponsored the **development and validation** of predictive modeling tools to predict HME chemistry and potential damage effects caused by HME to be used by the TSA to determine the explosive threat amounts which must be detected in TSA operated environments.
- Tested potential **HME detection technologies and screening methods** through the collection of raw data and images from explosives detection equipment for a wide variety of Commercial Off The Shelf (COTS) EDS, Computed Tomography (CT) and x-ray diffraction equipment to allow TSA to determine the feasible explosive threat amounts which need be detected for various HME explosives threats in TSA operated environments.

Technical evaluations. Evaluated numerous other transportation security technologies for conformity to performance requirements and certification. To support this program's customers, the Directorate:

- Completed conformity assessment of **Advanced Technology (AT) Checkpoint X-ray** equipment. The primary performance requirement evaluated was the Transportation Security Officer ability to identify and detect a wide variety of threats to civil aviation. The evaluation involved development of over 1000 test bags some of which contained functional IEDs with live explosives. The output of this effort drove TSA procurement and deployment of checkpoint AT in FY 2008.
- Completed **laboratory evaluation of three Bottle Liquid Scanner (BLS) devices** and their ability to detect hazardous liquids including liquid explosives. Evaluation included operational usability and suitability requirements along with the capability to distinguish dangerous liquids from those typically carried aboard aircraft. Results from this test will allow TSA to move forward with an operational evaluation of promising products.
- Conducted a series of eight lab assessments of **whole body imagers (WBI)** for use in passenger checkpoint screening. This assessment spanned 18 months involving up to four different imaging devices, 30 mock-passengers and six TSA-certified TSOs per device and per trial to evaluate a subset of TSA-specified detection performance and operational suitability as a pre-condition to TSA piloting and trial deployment at several domestic airports. In addition, these lab assessments that TSL conducted provided data to TSA to enable them to optimize system configuration, training methods and passenger stance protocols.
- Completed Certification Test and Evaluation of the first 600+ bag/hour **High Throughput In-Line Explosives Detection System (EDS)**. Successful certification was the culmination of over six months of extensive laboratory testing involving analysis of over 7,000 test objects. Results will permit TSA to install the system in their new Transportation Security Integration Facility in order to evaluate key integration parameters prior to field trials.
- Completed a **multi-year program evaluating two Directed Infrared Countermeasures (DIRCM) systems**, including live-fire tests utilizing real threats and extensive operational

service evaluations on both cargo transport and passenger transport planes, to determine the affectability and suitability of DIRCM technology in the protection the U.S. air transport community against the Man Portable Air Defense System (MANPADS) threat. Final results of this program will be delivered to Congress in late FY 2009.

In the upcoming year, the Directorate will deliver to potential customers, including TSA and mass transit authorities, a rugged canine harness with a suite of sensors to command and communicate with canines off-leash; conduct field tests with TSA canine teams to assess currently available HME canine training aids as viable options for training TSA canines; perform technical evaluations of COTS systems designed for screening palletized cargo; and field test a new Bottled Liquid Screening system with TSA.

Border & Maritime Security

Border & Maritime Security Technologies. The Directorate develops and transitions technical capabilities that enhance U.S. border security without impeding the flow of commerce and travelers by working closely with its operational customers, such as the USCG, CBP, and ICE, to identify gaps in current capabilities and future needs in order to determine and prioritize investments in new technologies for securing U.S. borders. Its area of responsibility encompasses all air, land, and maritime borders, including U.S. ports-of-entry and inland waterways. To support this program's customers, the Directorate:

- Installed a **BorderNet prototype** at the U.S. Border Patrol Station in Douglas, AZ to connect law enforcement officers in the field with real-time tactical information such as detection, sensor data, agent location data, and local geographic features, as well as field access to select law enforcement databases, using a wireless data network and commercial and Government developed software. S&T has an approved Privacy Impact Assessment (PIA) in place for this program (formerly known as BTSNet), which is currently being updated to reflect ongoing project development.
- Installed a prototype system in a **public infrastructure drainage tunnel at Nogales, AZ, to detect (illegal) human activities**. The sensor is emplaced behind the concrete tunnel wall to avoid sabotage while reliably detecting the presence of humans. Preliminary testing was completed and successful. Current work is focused on software upgrades for false alarm 'tuning' and improved user interface.
- Developed a distributed, ad-hoc, mesh network capability for **Unattended Ground Sensors (UGS)**. This enables the "hopping" of alerts through the network and eliminates the need for every UGS node to be within communication range of a repeater's site. Nodes will "auto-locate" an alternate communication path if one unit fails or is discovered by adversaries. This will enable agents to deploy UGS in many more locations than previously possible.
- Developed and delivered an **immigration model** that serves as a decision-aid tool for border enforcement agencies by determining the tactical implications of changes in immigration/border security policy and operations. This tool is being used by CBP and is being planned for use by the ICE Secure Communities. It can be available to support the Administration and Congress in addressing questions that may arise during future discussions of Immigration Reform.
- Developed an **eco-friendly removal agent for Arundo donax (Carrizo Cane)** along the Rio Grande River to increase border security and officer safety by eliminating possible use of

areas infested with this thickly grown weed as coverage for human and contraband smuggling.

- Deployed two differently designed prototypes of off-shore buoys for an on-going evaluation of **Vessel Detection capability**. This is aimed at improving the Coast Guard's off-shore surveillance capability with detection ranges up to 20 nautical miles from the buoys' locations and at depths up to 4 km, in order to allow sufficient time for the Coast Guard to investigate suspicious vessels before they are in ports.
- Demonstrated the ability to successfully locate an underground tunnel at forty feet with **Tunnel Detection**, a proof of concept project that creates a means to rapidly screen a large geographical area for underground tunnels by using a small unmanned areal platform with a radio frequency transmitter/receiver.

In the upcoming year, the Directorate's Border/Maritime Security projects will include the installation of a North East border testbed to provide a system architecture that supports the integration and evaluation of new sensors and data fusion technologies; the installation of a maritime testbed with the Port of Los Angeles for advanced fusion technologies that will provide DHS Components with an environment to derive changes in Concepts of Operations as a result of new technologies; the start-up of a pilot tripwire system on the Southern border to both sense intrusions and to provide communications to remote locations; a demonstration of a new port and coastal surveillance system in Long Island Sound to evaluate the feasibility of coupling a low cost, off-the-shelf radar with high-end, sophisticated signal processing to detect, track and identify large and small vessels from 0-12 nm in the port and coastal regions; and an assessment of our capabilities to detect and interdict Self Propelled Semi-Submersible vessels. The BorderNet Privacy Impact Assessment is being updated to cover these activities.

Container Security. The objective of the Homeland Security Cargo Security Program is to develop advanced technologies to address supply chain security and to test those technologies for functionality and ultimately for certification as acceptable security devices and/or methodologies. As such, all designs must comply to international standards and trade regulations and be tested in a variety of international supply chain environments in addition to those applicable to the U.S. To support this program's customers, the Directorate:

- Completed the development, prototype delivery (20 from each vendor) of the **Advanced Container Security Device (ACSD)** for testing. The ACSD is a small unit that attaches to the inside of a container to monitor all six sides of the container to report any intrusion or door opening. It will also detect the presence of humans in the container. Vendor is working on correcting certain deficiencies identified by the recent test. Testing is expected to complete by early FY 2010.
- Completed the development, prototype delivery (40 units – 20 from each vendor) and testing of a **Container Security Device (CSD)** prototype which is a small, low cost device, mounted on or within a container, specifically directed at monitoring the opening or removal of the container doors. Vendor is working on correcting certain deficiencies identified by the recent test. Testing is expected to be complete by early FY 2010.
- Developed, delivered and ISO tested a first version of the **Hybrid Composite Container**, which is a potential next-generation ISO shipping container with embedded security sensors. These sensors are designed to detect intrusions from the point of cargo consolidation to the point of deconsolidation in the global maritime supply chain. The container will be

constructed from composite material with embedded sensors. Composites are stronger than steel and hybrid composite containers are expected to be 10-15 percent lighter than current shipping containers. Development and refinement of manufacturing process for hybrid containers are on-going.

- Delivered **Secure Carton** first prototypes for tamper resistance testing (ongoing). These cartons have an embedded tamper-evident sensor and an embedded Radio Frequency ID (RFID) chip which is activated once the carton is sealed and will alert authorities in the event of subsequent tampering or intrusion.
- Completed **Secure Wrap**, a Phase I Small Business Innovative Research Program (SBIR) which is a tamper-indicative wrapping material for palletized cargo. It will enable inspectors to more easily and quickly identify whether the cargo has been tampered. Phase-II development and prototyping began in February 2009.
- Developed software and delivered functional workstations for an **Advanced Screening & Targeting I (ASAT-I)** capability for cargo security. ASAT-I provides next-generation risk assessment and targeting tools to complement the CBP Automated Targeting System (ATS). It provides automated anomaly detection and pattern discovery algorithms to target high-risk cargo. ASAT-II (FY 2009 start) will further advance computer algorithms and software that will automatically collect data from a broad spectrum of sources and combine and analyze shipping information to find suspicious relationships and patterns.

In the upcoming year, the Directorate will continue to mature and transition Cargo Security technologies as described above and initiate a myriad of new projects such as Automatic Target Recognition (ATR), a program to provide automated imagery detection capability for anomalous content (e.g. persons, hidden compartments, contraband) for maritime & air cargo; a SBIR Project to develop a small, highly portable Remotely Operated Vehicle/Autonomous Submerged Vehicle (ROV/ASV) to inspect the interior holding compartments of tanker ships for weapons and contraband; a second SBIR to non-intrusively examine the voids (i.e., fuselage, empennage, wings and fuel tanks, and cargo holds) in General Aviation (GA) aircraft, and the Marine Asset Tracking Tag System (MATTS) to serve as the global communication backbone for the ACSD/CSD and Hybrid composite containers.

Chem/Bio Defense

The Chemical and Biological portfolio works to increase the Nation's preparedness against chemical and biological threats through improved threat awareness, advanced surveillance and detection, and protective countermeasures. Through its strategic objectives, it seeks to enable comprehensive understand and analyses of biological and chemical threats in the domestic domain; develop pre-event assessment, discovery, and interdiction capabilities for biological and chemical threats; develop capabilities for warning, notification, and timely analysis of biological and chemical attacks; optimize technology and processes for recovery from biological and chemical attack; enhance the capability to identify biological and chemical attack sources; and develop vaccines and diagnostics for high-priority foreign animal diseases (FADs). To support this program's customers, the Directorate:

- Dedicated the **National Biodefense Analysis and Countermeasures Center (NBACC)**, located in Fort Detrick, Maryland, as part of the National Interagency Biodefense Campus to support law enforcement by characterizing existing biological threats, anticipate future

threats, and provide an enduring national forensics capability to support attribution of biocrimes and terrorism. The laboratory is expected to be fully operational by October 2009.

- Delivered the **2008 Bioterrorism Risk Assessment (BTRA)**. The BTRA provides an expansive analysis of bioterrorism risk to help decision makers evaluate risk mitigation strategies. Results are used to prioritize the risks posed by various agents, identify vulnerabilities, and identify associated major scientific knowledge gaps. The report expanded upon the 2006 BTRA to include enhanced threat agents, agricultural (livestock) agents and direct and indirect economic impact.
- Completed the **Chemical Terrorism Risk Assessment (CTRA)**, a first-time assessment of highly toxic chemicals identified through interagency processes as those of potentially greatest concern for homeland security. The assessment developed a quantitative rank order of risk presented by toxic chemical hazards by combining an intelligence informed threat perspective, a science based analyses, and a complex assessment of potential consequences. Completion of this effort informs the acquisition of medical countermeasures, the development and testing of non-medical countermeasures, the development of new procedures to mitigate contamination, and the identification of chemicals on hazard lists developed to improve security in the chemical supply chain to include industrial and transportation concerns.
- Delivered the first **integrated CBRN Terrorism Risk Assessment (iCBRNra)**, a quantitative risk assessment that incorporates intelligence, public health, and scientific information together to inform decision making across the Chemical, Biological, Radiological, and Nuclear threat areas in support of medical countermeasures and other strategic requirements.
- Developed **Consequence Management Guidance for a Wide-Area Biological Attack** to guide decision-makers in remediation of and recovery from a biological incident affecting urban areas. This guidance expands an existing interagency framework to be more operationally useful. It serves as a current baseline and can be used to develop a comprehensive roadmap outlining key science and technology areas as well as planning priorities for a wide-area biological incident.
- Transitioned to the EPA the **Portable High-throughput Integrated Laboratory Identification System (PHILIS)**, a mobile chemical lab system that can be rapidly deployed in the field to support high throughput analysis (several hundred samples per day) of environmental samples that may contain toxic industrial chemicals (TICs) and chemical warfare agents (CWAs).
- Established a formal partnership with USDA for a **Joint Modeling Operational Capability** to provide coordinated response plans to outbreaks of selected foreign animal diseases. The model will support decision making by evaluating the benefits and costs of strategies for mitigating and controlling outbreaks, and will also inform the development of requirements for future countermeasures.
- Received pre-licensing from USDA Center for Veterinary Biologics for the first ever **next-generation molecular vaccine for Foot and Mouth Disease virus** to significantly improve the Nation's ability to prevent, protect and mitigate the effects of an outbreak of FMD. The Foreign Animal Disease vaccines and diagnostics program is on schedule to have the vaccine fully licensed and ready for production by private industry and procurement to the National Veterinary Stockpile by November 2009. Technology used in the next-generation DIVA vaccine will also accelerate the speed at which new vaccines can be produced.

- Established, through interagency consensus, target and near-neighbor strain panels, performance requirements, and validation protocols for the independent evaluation and validation of **assay technologies that detect *Bacillus anthracis***.
- Developed the capability to rapidly and simultaneously **detect four common serotypes of Botulinum Neurotoxin (BoNT)**, a Category A bioterrorism agent. Each of these serotypes can be detected at low levels, which provides the capability to detect trace amounts of the agent. Further testing and validation of the assays in the Laboratory Response Network (LRN) is anticipated in FY 2009.
- Initiated field testing of two major new classes of next generation rapid biological sensors for continuous monitoring of facilities in the **Detect-to-Protect: Triggers and Confirmers Project**. These sensors will detect and identify aerosolized biological warfare agents within 15 minutes, have very low false alarm rates, and be affordable to own and operate by localities. Fieldable prototypes of multiple approaches meeting the Detect-to-Protect requirements are being evaluated in both laboratory and field environments.
- Developed fieldable prototypes (Phase III) of the of the **Autonomous Rapid Facility Chemical Agent Monitor (ARFCAM) and Lightweight Autonomous Chemical Identification System (LACIS)** chemical detectors which employ multiple technological approaches in their systems for chemical threat agent detection applications; one for continuous monitoring of facilities (ARFCAM) and the other for hand-held use by first responders (LACIS). These sensors will address both chemical warfare agents and a broad range of toxic industrial chemical, have very low false alarm rates, and be affordable to own and operate by localities.

In the upcoming year, the Directorate will transition the autonomous biological detector (BAND) prototypes to OHA for testing and possible deployment on large scale to upgrade BioWatch by decreasing time for detection of wide area bioaerosol release; complete guidance for restoration of transit systems following chemical attack; complete development of an integrated response architecture under the Integrated Consortium of Laboratory Networks (ICLN) to improve coordination of Nation's laboratory response networks to large scale CBR attacks; and complete licensure of the first Foot and Mouth Disease vaccine that differentiates between infected and vaccinated animals.

People Screening

The Directorate is developing a variety of technologies and knowledge products that can assist our law enforcement officers in differentiating between law-abiding individuals and those who mean to break our laws or do us harm. As we conduct this research, we are diligent in honoring the rights of Americans. S&T works closely with the DHS Privacy Office and the Office of Civil Rights and Civil Liberties (CRCL) to ensure that our research protects both individual rights and homeland security. Furthermore, we have a robust internal privacy compliance framework in place to ensure that all S&T-funded research that involves or impacts Personally Identifiable Information is reviewed and approved in advance by the Department's Privacy Office. We are also collaborating with CRCL to conduct Civil Liberties Impact Assessments (CLIAs) of S&T research that could impact civil liberties. To support this program's customers, the Directorate:

- Deployed **Mobile biometric collection technologies** with the Coast Guard to identify migrants and smugglers attempting to illegally enter the United States through the waters

near Puerto Rico and the Florida Straits. The program has resulted in a total of 3,143 people interdicted at sea, 269 brought ashore for prosecution – with 152 convicted so far. It is estimated that it has reduced the flow of illegal immigration in this area by 60 percent.

- Successfully demonstrated proof-of-concept technologies to acquire **high resolution, high quality single fingerprints without require physical contact**. The success of this effort has resulted in coordination with DoD on future year efforts to develop less intrusive, culturally acceptable fingerprinting technologies. The demonstrated technologies also allows for the possibility to examine three-dimensional features of fingerprints for recognition, providing revolutionary capabilities for fingerprint matching and latent fingerprint examiners in the future.
- Co-sponsored with the National Institute of Standards and Technology (NIST) the creation of the **Multiple Biometrics Grand Challenge (MBGC)** in order to improve face recognition performance. Early results of small data sets show near 100 percent performance when fusing face and iris biometrics together – a critical advancement for biometrics to function in non-contact applications.
- Performed initial validation of **behavioral indicators associated with possession of contraband**, such as weapons, false documents, and illegal drugs. The latest analysis provides statistically significant support that persons demonstrating select behavioral indicators are more likely to possess banned/illegal items. These indicators leverage those used by DHS operational customers such as TSA and CBP.
- Demonstrated proof of concept with TSA's Screening Passengers by Observation Technique (SPOT) program of **MobileSPOT technology**, a hand-held device that will enable the extension of TSA security layers beyond the checkpoint area by enabling SPOT Behavior Detection Officers (BDOs) to wirelessly share information that is currently exchanged manually or not at all.
- Conducted preliminary laboratory validation of **behavioral indicators associated with verbal deception** within a primary or secondary interview environment. These behavioral indicators distinguish deceptive from non-deceptive subjects at a statistically significant accuracy rate and are enabling the development of an automated deception detection prototype and training/training simulation materials.
- Demonstrated a **real-time stand-off system to identify behavioral indicators associated with hostile intent** and deception – the first step in developing a deployed system to detect hostile intent in real time.
- Deployed **deception-detecting techniques and support materials** to TSA and local law enforcement to provide them with behavioral indicators of hostile intent.
- Developed and conducted initial validation of the **Future Attribute Screening Technology (FAST) Theory of Malintent** (the intent to cause harm) for a primary screening environment, identifying specific cues that are diagnostic of malintent.
- Demonstrated **FAST initial sensor integration and command and control framework**.
- Convened the **Community Perceptions of Technology (CPT) Panel** to understand and incorporate community perceptions in the development and deployment of critical technologies within the United States such as microwave vehicle stopping technology, Raman spectroscopy for standoff detection of explosives, mobile biometrics, and acoustic non-linear technology for standoff threat detection.

In the upcoming year, the Directorate will execute malintent detection protocols with over 400 volunteer subjects to test theories and support data analysis; deliver a multi-modal (face, iris, finger) biometrics test and evaluation framework for government-sponsored multi-modal vendor tests that set the stage for incorporation of multi-biometric collection and fusion to support higher throughput screening applications; create a multi-biometric reference research database that will be used to evaluate biometrics algorithms and system performance for use by DHS operational components and continue to improve technical performance through industry and university challenge problems; develop technologies, in coordination with DoD, to collect multiple fingerprints for biometric matching without requiring physical contact; and develop technologies and procedures to enhance screener-performance and reduce human fatigue and injury while reducing training requirements and overall cost.

Cyber Security

The Directorate's Cyber Security program conducts the full spectrum of research, development, testing, evaluation and transition activities related to protecting critical information infrastructure; developing the cyber research infrastructure; and delivering new technologies. These efforts support a broad customer base including critical infrastructure operators/owners in the private sector; the general public; the Federal government; and specific DHS customers such as the US Computer Emergency Readiness Team and the United States Secret Service. To support this program's customers, the Directorate:

- Developed and deployed **Domain Name System Security (DNSSEC)** throughout the U.S. Government to address security weaknesses in the Internet's domain name system (DNS). The DNSSEC standard addresses DNS weaknesses that result in forged or compromised data, DNS cache poisoning, or man-in-the-middle attacks. Development included Federal agencies, private industry, and global Internet owners and operators.
- Funded the **Domain Name System Security (DNSSEC) – Secure Signer** effort to provide certainty for consumers, businesses and government that their web transactions and online communications have not been compromised.
- Funded and distributed **secure Ironkey USB drives** throughout Federal agencies to deliver "always-on" protection against simple and sophisticated cyber attacks – including USB sniffing, physical disassembly, differential power analysis, and chip inspection – to provide secure web browsing, cryptographic authentication, end point security, self-service password recovery, and secure password management, thus resulting in improved security of the data on the drives and a reduction of malicious software-related threats delivered via USB devices.
- Deployed the **Protected Repository for the Defense of Infrastructure against Cyber Threats (PREDICT) – Data Repository** to provide privacy-protected operational network traffic datasets to the cyber security research and development community to help them create and develop new models, technologies, and products which assess cyber threats to the country's computing infrastructure and increase cyber security capabilities.
- Completed the **DHS Secure Wireless Access Prototype (DSWAP)** pilot, a secure wireless access solution that provides enhanced, layered defense beginning with the mobile wireless user, specifically using 802.11 WiFi networks, and extending back to protected networks to minimize risk in using public networks to securely connect to DHS networks. The S&T CIO is working with the DHS CIO to have this accepted as a DHS standard.

- Transitioned **Botnet detection and mitigation technology** to US-Computer Emergency Readiness Team (US-CERT) to provide quicker detection and adaptability in an easily deployable manner against attackers attempting to evade the system.
- Transitioned **Data Visualization Tools** to US-CERT for operational use in a software analysis package for data-monitoring analysis.
- Transitioned to the National Cyber Security Division (NCSA) the **Cyber Scenario Modeling and Reporting Tool (CyberSMART)**, an on-line collaborative Exercise Scenario and Modeling Tool to assist cyber exercise developers in identifying where further planning and process improvements are needed. In a pilot project, CyberSMART was used in Mass-Attack, the Massachusetts Commonwealth's first cyber-exercise designed to test communications, operational, and command & control related policies, procedures, and practices. The tool has been transitioned to NCSA and is awaiting a decision on whether to be included in the Homeland Security Exercise and Evaluation Program (HSEEP).
- Delivered to the Internet routing community, both operational and research, **RouteViews**, an enhanced routing data collector that provides scalable, real-time access to Border Gateway Protocol (BGP) data as it is being collected from ISPs around the globe to enable the expansion of internet data sources through the increase of both the number of data collectors and the number of peers monitored (the operational routers from which BGP data is collected). This expanded data will allow faster discovery and more comprehensive analysis of attacks on the Internet routing infrastructure.
- Developed the **Rootkit Detection and Mitigation Technology** to protect against malicious software programs designed to take control of a computer's operating system at the administrator level, where they can often hide from detection by standard anti-malware software. This technology was developed by Komoku, a Maryland company, and acquired by Microsoft in March 2008.
- Developed **Active Malware Protection (AMP)**, a product which provides increased computer security and reliability by capturing malware on the wire as opposed to the traditional technique of capturing it on the host. This technology was developed by Endeavor Systems, a Virginia company, and acquired by McAfee in January 2009.

In the upcoming year, the Directorate will continue the deployment of the DNSSEC solution within the U.S. Government and major domains such as ".org" and ".edu"; (2) initiate the Secure Protocols for the Routing Infrastructure (SPRI) program to enhance the security of the BGP, a major part of the Internet infrastructure; initiate a Cyber Forensics program in partnership with both DHS and external law enforcement participants; and initiate the Homeland Open Security Technology (HOST) program that will promote the development and implementation of open source solutions within US Federal, state and municipal government agencies.

Interoperability

While governance and other human dimensions of communications interoperability are critical to any solution, technology remains at the center of the issue, making research, development, testing, evaluation and piloting of new interoperable technologies vital to the creation of a comprehensive solution. To support this program, the Directorate:

- Launched and operated the Congressionally-required **P25 Compliance Assessment Program (P25 CAP)**. P25 CAP will provide manufacturers with a method for testing their communications equipment for compliance with P25 standards and to ensure it is capable of

interoperating across manufacturers. P25 CAP will encourage the inclusion of P25 standards in communications systems while creating a means for the emergency response community to confidently purchase and use P25-compliant products.

- Expanded on the **Radio Over Wireless-Broadband** project, a partnership with industry, local government, NIST, and the Institute for Telecommunication Sciences (ITS) that seeks to bridge existing land mobile radio systems with advanced broadband technologies. Broadband technologies, such as Push-To-Talk over Cellular and the Geographic Information System, allow emergency responders to form talk groups and use location-based services for situational awareness and coordination—ultimately saving critical response time.
- Published **Emergency Data Exchange Language (EDXL) data messaging standards** for numerous programs, including the Common Alerting Protocol (CAP) all-hazard emergency alert system, the Distribution Element flexible message-distribution framework for emergency data sharing, the Hospital Availability Exchange, and Resource Messaging. These information sharing standards will improve emergency preparedness, response, and recovery efforts and will be used in partnership with the FEMA Integrated Public Alert and Warning System (IPAWs), to enable local, tribal, and state practitioners to provide reliable and accurate alerts and warnings to more of the public.

In the upcoming year, the Directorate will conduct demonstrations and pilots of the MBR across the Nation; announce the initial group of laboratories that have been assessed as part of P25 CAP and begin testing equipment to ensure that radios from different manufacturers are capable of interoperating; accelerate the development and adoption of voice and data communications standards; and continue to encourage the development and implementation of new, standards-based, non-proprietary solutions that use Project 25, Voice over Internet Protocol, and other voluntary consensus standards.

Information Sharing/Management

Relevant and timely information is vital for making tactical, strategic, and planning decisions when responding to natural and man-made incidents and disasters. The Directorate provides homeland security practitioners with a toolkit of technologies, processes and mechanisms to support gathering, analyzing, managing, sharing, and protecting information. The current information sharing environment consists of stove-piped communities that have developed their own policies, rules, standards, architectures, and systems to channel information to meet mission requirements. The Information Sharing program works to overcome these barriers by developing national solutions for sharing all-hazards information in manner consistent with national security and legal standards that create new technologies to share, search, and analyze homeland security information across jurisdictional boundaries; provide technologies to enable a distributed, secure, and trusted environment for transforming data into actionable information; and recognize and leverage the vital roles played by state and major urban area information fusion centers. To support this program's customers, the Directorate:

- Deployed the **Critical Infrastructure Inspection Management System (CIIMS)**, a new, cost-effective, technology that enables police to more efficiently manage inspections of important structures such as dams, bridges, large industrial complexes, as well as urban areas. CIIMS was piloted in Maryland by the Maryland State Police Department and further developed for the Los Angeles Police Department in an effort called LA Shield to address large urban environments.

- Established and piloted digital image exchange specifications for the **NLETS Image Sharing Program (NISP)** to enable state and local law enforcement personnel to query and retrieve driver's license photos across state lines via the NLETS network. DHS S&T partnered with the National Institute of Justice (NIJ) to examine the technical, policy, and privacy challenges of enabling law enforcement personnel to share interstate driver's license photos for field identification and threat assessment functions. In addition to DHS and NIJ, agencies participating in the interstate photo sharing program include the International Justice and Public Safety Information Sharing Network (NLETS), the American Association of Motor Vehicle Administrators, the North Carolina Highway Patrol, and the South Carolina and Virginia State Police.
- Developed the **Scalable Reasoning System (SRS)**, an advanced web-based and mobile incident analysis and collaboration technology for front-line law enforcement and counter-terrorism personnel. Deployed at the San Diego Automated Regional Justice Information System (ARJIS) and the Port Authority of New York and New Jersey (PANYNJ), SRS provides access to readily usable, up-to-date information analysis tools.
- Developed a **handheld device software application** that retrieves digital photographs from the California Department of Motor Vehicles (DMV) to enable law enforcement personnel away from their office or vehicle to quickly query, retrieve, and view California driver's license photographs on a range of handheld devices (PDAs), greatly enhancing their ability to positively identify individuals in the field. This application was certified by California Department of Justice, and nearly 500 federal, state, and local law enforcement personnel throughout Southern California are currently participating in its operational testing.
- Developed a regional communications architecture – **the State, Regional, and Federal Enterprise Retrieval System (SRFERS)** – to facilitate data sharing and software integration between multi-jurisdictional criminal justice agencies separated by physical and political boundaries. SRFERS uses existing information infrastructures, such as the International Justice and Public Safety Information Sharing Network, the Automated Regional Justice Information Sharing (ARJIS) network and state networks in place to demonstrate connectivity and exchange data in real time across state lines. Through these existing networks, SRFERS provides a toolkit—consisting of successful architectural models, technical specifications for open source messaging applications, transactions and scripts, templates for information sharing agreements, and technical and policy documentation guidance—to enable agencies to seamlessly share justice information.
- Deployed the **Spatial Temporal Visualization (STV) and Criminal Activity Network (CAN)** visualization toolset to the Tucson Police Department. The STV tool enables crime analysts to plot suspicious or criminal incidents near critical infrastructure and explore distribution of those incidents by time period while the CAN visualization tool integrates CBP License Plate Reader data with a local criminal record set to reveal links among subjects who routinely crossed the border and are known offenders in the Tucson region.
- Developed and deployed multiple new data cubes for the **Immigration and Customs Enforcement Pattern Analysis and Information Collection (ICEPIC) System**. These data cubes are intuitive but sophisticated representations of multi-dimensional structured information within the On-Line Analytical Processing (OLAP) database paradigm. This technology is complementary to both relational and graph-based representations, and provides a “third view” of the data supporting summary queries, including trend analysis and statistical analysis.

- Tailored and deployed the **Everest graph visualization and link-analysis tool** to 200 ICE investigators utilizing ICEPIC data sets. This capability provides the ability to create a graph-based view of information from one or more relational databases, and perform graph queries across this view. The ability to ask questions such as, how are two entities connected, what is the shortest path between two entities, and what entities are connected to a known entity, is a powerful complement to traditional relational queries.
- Developed the **Wireless Airport Surveillance Platform (WASP)**, an information-sharing pilot program which uses pan-tilt-zoom cameras and an information-sharing network backbone to detect unrecorded and illegal air traffic. During the first phase of the pilot with the San Diego County Police Department in California, WASP identified a significant amount of flight traffic in the San Diego area which was previously unknown to operators. WASP was successfully transitioned to Customs and Border Protection (CBP) in 2008 and is now in the planning phases of deployment with CBP. CBP is planning to expand the use of WASP to several airports and airfields in the southern border area, and then potentially across the Nation.

During the coming year, the Directorate plans to continue with the AZLink, and SRFERS development efforts currently underway along with continuing to deploy CIIMS, NISP, STV CAN visualization toolset and new data cubes for the ICEPIC system. New efforts will be initiated including the piloting of systems analyzing fusion center information usage and sharing; suspicious capability reporting; developing a HSPD-12-related identity management system broadly applicable across the Federal government; and piloting a geospatial analytics tool for use in fusion centers that will support situational awareness and critical decision making.

Infrastructure Protection

The Directorate's Infrastructure Protection portfolio conducts research and development activities based on the 18 Critical Infrastructure/Key Resource (CI/KR) sectors identified in the National Infrastructure Protection Plan (NIPP). This meets the requirements of the Office of Infrastructure Protection (IP) in the National Preparedness and Programs Directorate (NPPD), and requirements set forth in other Homeland Security directives. Some specific program areas include: Modeling, Simulation, and Analysis, Protective Technologies against blast and projectile damage, Response and Recovery Technologies including damage and cascading effects prevention, and finally Advanced Surveillance and Detection. To support this program's customers, the Directorate:

- Transitioned the **Critical Infrastructure Protection Decision Support System (CIPDSS)** to the Office of Infrastructure Protection for inclusion in the suite of operational tools at the National Infrastructure Simulation and Analysis Center (NISAC). The CIPDSS allows analysis of interdependencies among infrastructure sectors and impacts when a sector is struck by an event. It was successfully used in the preparation of the Pandemic Flu study performed by NISAC.
- Conducted test and evaluation of **flexible concrete mats** that could be deployed to protect underwater tunnels by stemming water inflow following a breach. The effectiveness of the mats has led a major U.S. transit system to consider operational deployment of the system.
- Developed new **material solutions to harden tunnels and other mass transit infrastructure** against IED threats. Existing materials, new materials, and innovative combinations are being evaluated for their effectiveness in protecting different types of

tunnels. Results will provide novel solutions and design guidance for transit owners and operators.

- Demonstrated the cover-deployment mechanism for the proof-of-concept **Secure Against Fire and Embers (SAFE)**, a quick-cover application for automatic shielding of a home with a fire retardant tarp to protect against wildfires.
- Demonstrated a **scaled prototype solution for rapidly closing a levee breach using a water-filled tube**. This levee plug was deployed from a floating platform and guided into place where, due to the rushing water, it then conformed to the breach, thereby reducing the flow of water by approximately 95 percent.
- Demonstrated the **Resilient Tunnel** project, an early prototype of an inflatable tunnel plug to protect tunnels from fire, flooding, and potentially other hazards. Continued development of inflatable plugs is being done in close coordination with the Washington, DC Metro and the Port Authority of New York and New Jersey in order to provide a cost-effective solution for isolating hazards in transit tunnels to protect occupants and system infrastructure.
- Demonstrated across a three meter cable the proof of concept **Resilient Electric Grid (REG)**, a project which incorporates high temperature superconducting technology to ensure the reliable distribution and protection of electrical power acting as a fault current limiter for both DC and AC power to prevent rolling brown outs and black outs.
- Demonstrated a **prototype wireless security system** to monitor and assure the delivery of milk, milk samples, and security information from dairy farms to the dairy plants. Potential exists for broad use across the dairy industry. Having been successfully tested through some 50 loads from dairy farm to commercial plants, this technology will be commercial ready in December 2009.

In the upcoming year, the Directorate will conduct an analysis of existing surveillance technologies and select sets of sensor systems (optical, infrared, ultraviolet, and acoustic) appropriate for monitoring selected infrastructure types; begin development of computational models for blast effects on tunnels, bridges, and urban environments, and conduct experiments to validate the numerical predictions; and focus response and recovery technologies on rail cars carrying chlorine, a toxic inhalation hazard (TIH) material and design and demonstrate a recovery transformer in a laboratory environment.

Preparedness and Response

In the event of a terrorist attack, natural disaster or other large-scale emergency, the Department is responsible for providing a coordinated, comprehensive federal response so as to mount a swift and effective recovery effort. The Preparedness and Response program focuses on the Directorate's effort for ensuring that emergency response professionals are prepared for any situation. To support this program's customers, the Directorate:

- Coordinated national capabilities in atmospheric modeling and provided Federal prediction of atmospheric hazards and their consequences with the **Interagency Modeling and Atmospheric Assessment Center (IMAAC)**. In the past year, IMAAC responded to over 1000 requests throughout the United States, including several fires and chemical releases such as a downwind smoke plume from fire caused by an accidental plane crash into an apartment building in New York, NY, multiple explosions and fire at the Barton Solvents chemical plant in Wichita, KS, chlorine release at a water treatment facility in Berthoud, CO, and the derailment of five phosphoric railcars in Chicago, IL.

- Demonstrated **Man Portable Interoperable Tactical Operations Center**, a services-oriented portable platform that can be transported to an incident scene in an SUV, truck, boat, helicopter or trailer. MITOC is an integrated suite of commercial-off-the-shelf (COTS) tools to enhance communications, situational awareness, radio/voice/data interoperability and applications access developed in support of the Kentucky Critical Infrastructure Protection Program (KCI).
- Field tested a **concealable escape hood** for Secret Service agents which provides fifteen minutes of protection agent chem/bio attacks.
- Developed early concepts in support of **Physiological Health Assessment Sensor for Emergency Responders (PHASER)**, a program for monitoring the vital measurements of agents in real time through the use of intelligent algorithms, in order to provide an alarm to both responder and commander if a responder is going to experience any health threatening events.
- Tested the **Geospatial Location Accountability and Navigation System for Emergency Responders (GLANSER)** to allow for tracking of first responders inside buildings, below ground, above ground, and in rubble where GPS is denied, with an accuracy of three meters in all dimensions.
- Developed and tested the **Controlled Impact Rescue Tool (CIRT)** for Urban Search and Rescue teams to breach concrete barriers in a safe and efficient manner.
- Developed the **Unified Incident Command and Decision Support (UICDS) Information Architecture**, a blueprint for managing and sharing incident information across state and local jurisdictional lines and with DHS and other federal agencies. This national architecture, a response to issues identified in the 9/11 Commission Report, is aimed at establishing a set of standards to which solution developers for incident management tools will adhere in order to ensure that recipients of DHS funds at the state/local level will procure incident information management systems that comply with the UICDS standards in order to solve the information interoperability problems. While the initial framework was completed in 2007, the architecture is currently being developed and will be tested in FY 2009.
- Demonstrated **Training, Exercise, and Lessons Learned (TELL)** a prototype system to enable cost effective training for emergency management teams. Using models and simulations and leveraging graphics engines from the gaming industry, the system provides for a live, virtual, and constructive environment so policy makers, elected officials and incident commanders can quickly assess the consequence of their decisions during an incident. The TELL prototype was used in preparation for exercises in Anaheim, California and Cincinnati, Ohio and will be deployed at the FEMA National Exercise and Simulation Center (NESC) for nationwide exercises and operations analysis. This capability is being developed in response to the Katrina White House Lessons Learned Report.

In the upcoming year, the Directorate will deliver a report detailing temporal and geospatial analysis of needs for shelter, food, and disaster relief as identified by callers into the Texas 2-1-1 System during Hurricanes Katrina and Rita in order to provide first responders/response planners with the ability to more accurately plan for resource requirements and evacuation strategies in future catastrophic events; test the UICDS system; demonstrate a concept prototype of PHASER to validate system requirements, architecture, and concept of operations; utilize TELL to conduct disaster planning training scenarios to prepare FEMA decision and policy makers to validate their plans, procedures, tactics, and doctrine when responding to major events; test and

validate GLANSER against a prioritized list of technology challenges (i.e., underground, over ground) at major urban areas such as New York City and Seattle; seek NIOSH certification for the concealable hood so that it can become available as a commercial product; and deliver the iEOC connectivity solution deployed in Seattle to the Cincinnati urban area to enhance situational awareness during an emergency incident.

Counter Improvised Explosive Devices (IED)

The Directorate established the Program Executive Office for Countering Improvised Explosive Devices (PEO (C-IED)) to manage counter-IED efforts in response to the direction provided by Homeland Security Presidential Directive 19 (HSPD-19), *Combating Terrorist Use of Explosives in the United States*. PEO-(CIED) focuses its portfolio in following areas: Prevent/Deter, Predict, Detect, Defeat, and Respond/Mitigate. To support this program's customers, the Directorate:

- Developed the **Standoff Technology Integration Demonstration Program (STIDP)** to provide for the evaluation of a layered approach to security against IEDs. It involves the integration of sensors and technologies into a unified system to detect the approach of a person carrying an IED. The system was successfully tested in Kennewick, WA, in October-November 2008. The data collected will be very valuable in highlighting the outstanding challenges in screening crowds of people at large public events, and in demonstrating how multiple systems can be integrated into a comprehensive approach to screening that will be minimally intrusive and will provide warning of IEDs early enough for action to be taken to prevent the IED from being used as intended.
- Developed an **X-Ray Backscatter System** to detect, diagnose, and defeat vehicle-borne IEDs (VBIEDs). This system provides bomb technicians with the capability to examine suspect vehicles when access to only one side is possible. It has been delivered to a company to integrate into a robot, and the integrated system will be demonstrated in 2009 when it will then be further evaluated by a select bomb squad.
- Characterized **VBIED disruption tools** for validation and testing against mock vehicle bombs as part of an operational database for use by Bomb Squads.
- Developed a **real-time, 360-degree, imaging system** for the detection of concealed objects on people which does not require an individual to stop and "pose" while being interrogated.
- Tested the decommissioned **Waldo Hancock Bridge** to understand the vulnerability of vintage bridge components to terrorist attack scenarios and gain data to enable improvement of numerical models to predict bridge cable response to an IED attack.

In the upcoming year, the Directorate will demonstrate a new VBIED disruptor and make it available for Bomb Squad evaluation and publish reports on trends in support for jihadi terrorism within the United States based on the results of existing surveys; characteristics of groups that use IEDs and trends in IED use over time based on analyses of quantitative databases; and de-radicalization initiatives in five countries and their applicability to the U.S. context.

First Responder Technologies

Although our thirteenth IPT is new and will serve to better coordinate our support of the first responder community, many of the technologies that Directorate has delivered to operational

components of DHS will also help first responders. To support this program's customers, the Directorate:

- Developed the **Digital Ink Library** for the Secret Service forensic investigators to create a quick-reference database of inks critical to the investigation of criminal and terrorist casework involving fraudulent financial documents (such as checks and money orders), property and asset documents.
- Demonstrated a prototype **Handheld LED-Based Incapacitator (Dazzler)** to serve as a less-than-lethal technology to better control hostile persons in a standoff environment.
- Facilitated the technology transfer of the U.S. Air Force's **ROVER air to ground surveillance system** program making it available to requesting state and local first responders to assist with firefighting and law enforcement activities.
- Produced **publications for First Responder groups** by the Environmental Measurements Laboratory (EML). Publications include Urban Atmospheric Plume Models for Emergency Response; Dosimeters; and Technologies for Radioactive Decontamination of Building Surfaces.
- Developed **prototype protective suits** using nanotechnology materials and multiple layers to provide active protection elements to block hazardous chemical/biological agents. The suits, several of which have been produced, also have fire retardant properties and are undergoing detailed testing this year.

The Directorate's First Responder Technologies (R-Tech) Division is another avenue by which we deliver products to the First Responder community. Comprised of the Tech Solutions and Tech Clearinghouse subdivisions, R-Tech uses interaction and information sharing with First Responders to provide quick-reaction S&T solutions to their capability gaps. To support this program, the Directorate:

- Produced the **FireGround Compass** to provide Firefighters with a ruggedized portable tool that enables them to maintain their reference point as they fight interior structural fires.
- Prototyped an **Ocular Scanner** to provide the emergency medical service (EMS) community a rapid screening technology for victims with possible exposure to a wide variety of hazardous and toxic agents.

Within the next year, the R-Tech intends to transition a Next Generation Self Contained Breathing Apparatus and Three-Dimension Locator System to Fire Fighters.

Additionally, some core S&T investment has been directed at first responder needs. To support the First Responders over the past year, the Directorate has:

- Developed a pilot program for a **Digital Multi-Band Radio (MBR)** to allow communications interoperability across multiple bands without a gateway or other bridging technology during emergency situations. S&T completed privacy compliance documentation for this pilot project.
- Developed the **AZLink wireless technology system** under the Regional Information Sharing and Collaboration program which provides law enforcement officers with the capability to use PDAs to access information—including criminal histories, mug shots, driver's license data, maps aerial photographs, and incident reports—that they otherwise would need a computer system to access.
- Established the **RealEyes** system to allow users to send and receive live video and geospatial coordinates, view video from fixed or mobile cameras and receive data from a field

command post using basic cellular technology in order to increase situational awareness for law enforcement operations and emergency situations. S&T has completed a PIA for this project.

In February 2009, S&T assumed from FEMA **responsibility for the System Assessment and Validation for Emergency Responders (SAVER) Program** to assist emergency responders making procurement decisions. SAVER conducts objective assessments and validations on commercial responder equipment and systems and provides those results along with other relevant equipment information to the emergency response community in an operationally useful form.

UNIFYING DHS

S&T, by virtue of our role supporting operating components across the Department, is in a unique position to help accelerate the maturation and unification of the Department. To be sure, the Capstone IPT process has helped do that. Additionally, S&T provides other Department-wide services that help DHS operate better as one Department.

Test & Evaluation

Section 302 (12) of the Homeland Security Act of 2002 (PL 107-296) assigns me the responsibility of “coordinating and integrating all research, development, demonstration, testing, and evaluation activities of the Department.” The S&T Directorate established the Test and Evaluation and Standards Division (TSD) in FY 2007 to develop Department-wide T&E policy and provide T&E oversight of the major acquisition programs. TSD is working closely with DHS Undersecretary for Management and all DHS components to develop and implement a robust department-wide Test and Evaluation (T&E) policy that will be fully integrated into the Department’s Acquisition process framework. The Directorate/TSD has created a draft T&E Directive that complements the new DHS Acquisition Directive (Management Directive 102-01). Together these policies will provide the appropriate component review and DHS oversight for test planning, execution and reporting. The T&E policy will require components to participate in development and approval of the Test and Evaluation Master Plan (TEMP) that will describe the necessary Developmental Test and Evaluation (DT&E) and Operational Test and Evaluation (OT&E) that must be conducted in order to determine system technical performance and operational effectiveness and suitability throughout the development process. TSD is currently providing oversight to major acquisition programs by participating in T&E working groups, approving TEMPs, approving Operational Test Plans, participating in Operational Test Readiness Reviews, observing testing, and participating in Acquisition Review Boards. Over the past year, we have:

- Established a **T&E Council** to advise the senior DHS management in matters relating to T&E. This Council includes participation by all components in promoting T&E best practices and lessons learned, ensuring adequate T&E infrastructure, and establishing consistent T&E policy and processes for use in acquisition programs throughout the Department.
- Provided **T&E oversight** on critical acquisition programs throughout the Department, including Advanced Spectroscopic Portal (Cargo) ASP(C), BioWatch Generation 3, Secure Border Initiative network (SBInet), Air/Sea Exit, National Cyber Security Program (NCSP),

U.S. Visit, Western Hemisphere Traveler Initiative (WHTI), Secure Flight, Transformation and Systems Consolidation (TASC), USCIS Transformation, Transportation Worker Identification Card (TWIC), and Automated Commercial Environment (ACE).

- Partnered with the United States Navy (USN), NIST and DOJ to develop an **initial set of standard test methodologies** applicable to small unmanned aerial systems (sUAS) in support of law enforcement and urban search and rescue missions.

Standards

S&T is the Standards Executive for the Department, with responsibility for coordination of standards activities for the entire DHS as prescribed in OMB Circular A119 and the National Technology Transfer and Advancement Act (PL 104 -113). Standards for the DHS components include performance specifications, documentary standards, measurement standards and process standards as well as interoperability and safety standards. The Office of Standards within TSD has three main functions: 1) coordination of standards within the Department, 2) outreach to the private sector standards development community, and 3) management of a program to develop critical standards for homeland security applications. The Office manages the processes for formal adoption of standards as *DHS National Standards*. The Office also coordinates with private sector Standards Development Organizations (SDOs) that address the homeland security community, ensuring that the standards produced meet the requirements of the DHS components as well as state, local and tribal users of equipment and processes. The Office also manages an investment of funds in development of standards to meet mission needs. This includes evaluating standards needs; participation in standards development planning; coordinating standards development efforts with DHS components and other state and federal agencies and appropriate SDOs; and supporting activities at NIST, NIOSH, DOD and the national labs and other partners in standards related technology development. Over the last year, we have:

- Established an **intra-agency accreditation and certification program** with FEMA, the DHS Private Sector Office, the DHS OIP, and the DHS Office of General Counsel (OGC) to help ensure emergency preparedness and business continuity in the private sector.
- Developed a **Standards Council** to support the department-wide development and adoption of standards. In the last year, the Council has adopted twenty-one new standards for homeland security mission needs, including the American National Standard for High-Visibility Safety Apparel, the Headwear American National Standard for Industrial Head Protection, the Common Alerting Protocol v1.1, the NIOSH Statement of Standard for Chemical, Biological, Radiological, and Nuclear (CBRN) Powered Air-Purifying Respirators (PAPR), the Emergency Data Exchange Language (EDXL) Distribution Element, v 1.0; and sixteen additional National Fire Protection Association Standards.

Federally Funded Research & Development Centers (FFRDCs)

The Directorate recently established two new FFRDCs, the Homeland Security Studies and Analysis Institute (HSSAI) and the Homeland Security Systems Engineering and Development Institute (HSSEDI), which it will manage on behalf of the Department. These institutes will promote fair and open competition for the development and delivery of Department capabilities by providing independent and objective technical expertise. HSSAI will provide special technical expertise to Department mission owners to help them transform mission-level goals into strategies, operational requirements, and performance metrics constrained by cost and schedule. The HSSEDI will provide expertise in support of the Department's acquisition process

by assisting in the development of technical concepts, standardized technical data packages, development modeling and simulation, and developmental testing and lab experiments. Through their long-term relationships with the Department, I believe these new FFRDCs will contribute substantially to reducing our Nation's risk to terrorism and catastrophic incidents.

Commercialization and Private Sector Engagement

The Directorate's Commercialization Office and the Office of SAFETY Act Implementation (OSAI) have both contributed to expand upon and improve the Directorate's relationship with business and industry. Responsible for creating initiatives that identify, evaluate and commercialize technology for the specific goal of rapidly developing and deploying products and services that meet the specific operational requirements of our customers, the Commercialization Office establishes and fosters working relationships with the private sector to facilitate cost-effective and efficient product/service development efforts.

In the past year, OSAI has been responsible for coordinating 179 applications from industry partners seeking Federal protection for their technology under the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act). This office links the private sector with not only DHS S&T, but also other members of the Federal government

The Directorate also officially stood up the Commercialization Office in 2008 to develop and execute programs and processes that identify, evaluate and commercialize widely-distributed products or services that meet the operational requirements of the Department of Homeland Security's operating components, first responder community, critical infrastructure/key resources owners and operators and other Department users. It is committed to conducting outreach with the private sector in order to engage and leverage the expertise, skills and resources of the private sector. This outreach includes a concerted effort to engage small, minority, disadvantaged and HUB Zone groups. As a result of these efforts, the Commercialization Office has compiled a listing of well-over 300 companies, outlining over 2,000 technologies, products and/or services that may possess potential alignment to DHS needs. Information has also been compiled to show the number of small, medium and large businesses with whom the Commercialization Office has interfaced. A majority of those companies are small businesses.

Since its inception, the Office has published a number of materials, including briefs, books and articles that outline the major activities of the Commercialization Office and provide readers with easy-to-understand guides to execute effective detailed operational requirements documents (ORDs) and the newly created and implemented commercialization process. Furthermore, the Office has published three popular books to assist in the development of detailed operational requirements. These books serve as a useful resource to explain both the critical role of detailed requirements to cost-effective and efficient product development, and also as an easy-to-use guide to aid in the articulation of requirements.

Another avenue by which the Office performs outreach to the private sector is the System Efficacy through Commercialization, Utilization, Relevance and Evaluation (SECURE) Program, an innovative public-private partnership in which DHS leverages the skills, expertise, and resources of industry to develop products or services aligned to DHS-written and vetted ORDs. Here, DHS posts detailed ORDs on its web portal

(http://www.dhs.gov/xres/programs/gc_1211996620526.shtm), along with a conservative estimate of the potential available market (PAM) of a given product/service and invites the private sector to use this information to formulate a business case to pursue potential sales opportunities found within DHS operating components and its many ancillary markets including first responders and CI/KR owners and operators. This program has been well received by the private sector who has been asking DHS to provide more information into the detailed needs and requirements of its stakeholders.

CONCLUSION

I am glad to report that, with our People and Processes securely in place, the Department of Homeland Security Science and Technology Directorate has made significant progress this past year in getting product to our customers. Doing so has helped enable DHS to better protect our Nation. I look forward to working with the Committee to ensure continued success in both the near and long-term future.

Members of the Committee, I thank you for the opportunity to meet with you today and look forward to answering your questions.

Bradley Buswell
Acting Under Secretary for Science and Technology
U.S. Department of Homeland Security



A native of Durango, Colorado and a graduate of the United States Naval Academy, Bradley Buswell is a retired submarine officer who has served in numerous posts at sea and in Washington, DC.

His Washington assignments have included serving as Congressional Liaison for Navy Research and Development Programs in the Navy Office of Legislative Affairs; Assistant to the Chief of Naval Operations for Force Transformation; and Executive Assistant to the Chief of Naval Research, among other positions on the Navy staff.

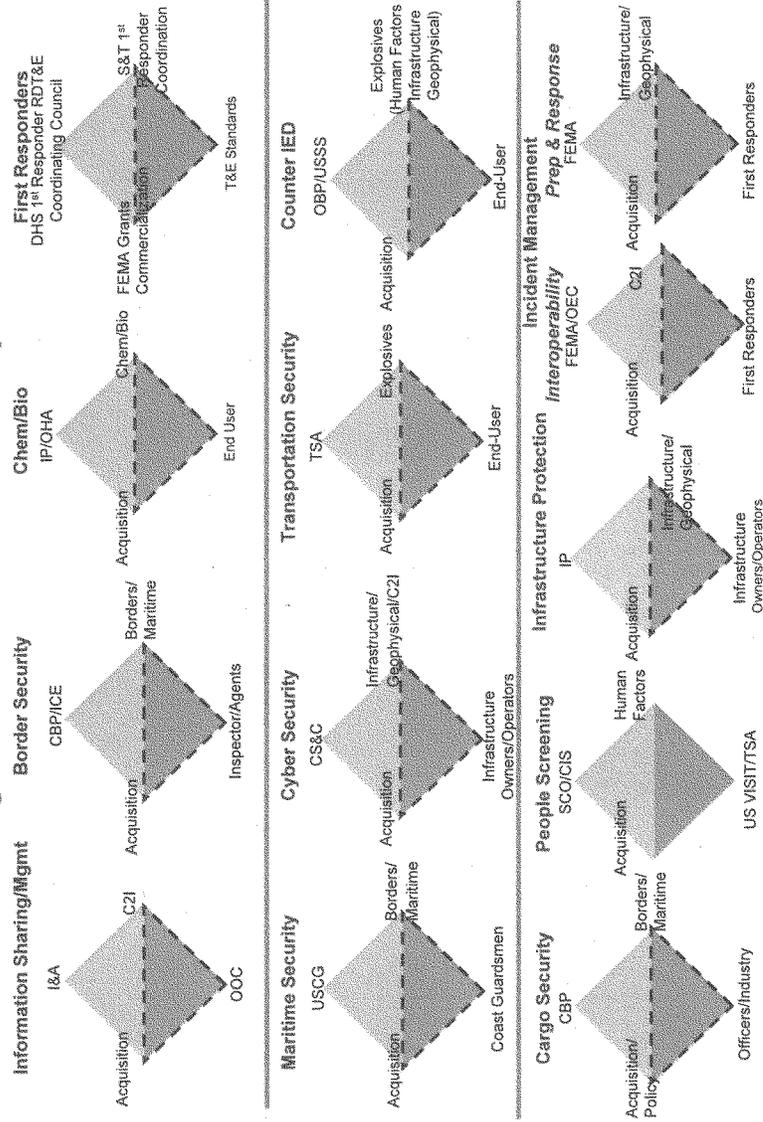
Mr. Buswell joined the private sector following his retirement from the U.S. Navy, working for General Electric as Manager of Government Relations for GE Global Research in Washington, DC.

He joined the Department of Homeland Security's Science & Technology Directorate in October 2006.

Mr. Buswell holds a Bachelors of Science in Systems Engineering from the U.S. Naval Academy and a Masters of Business Administration from The George Washington University.

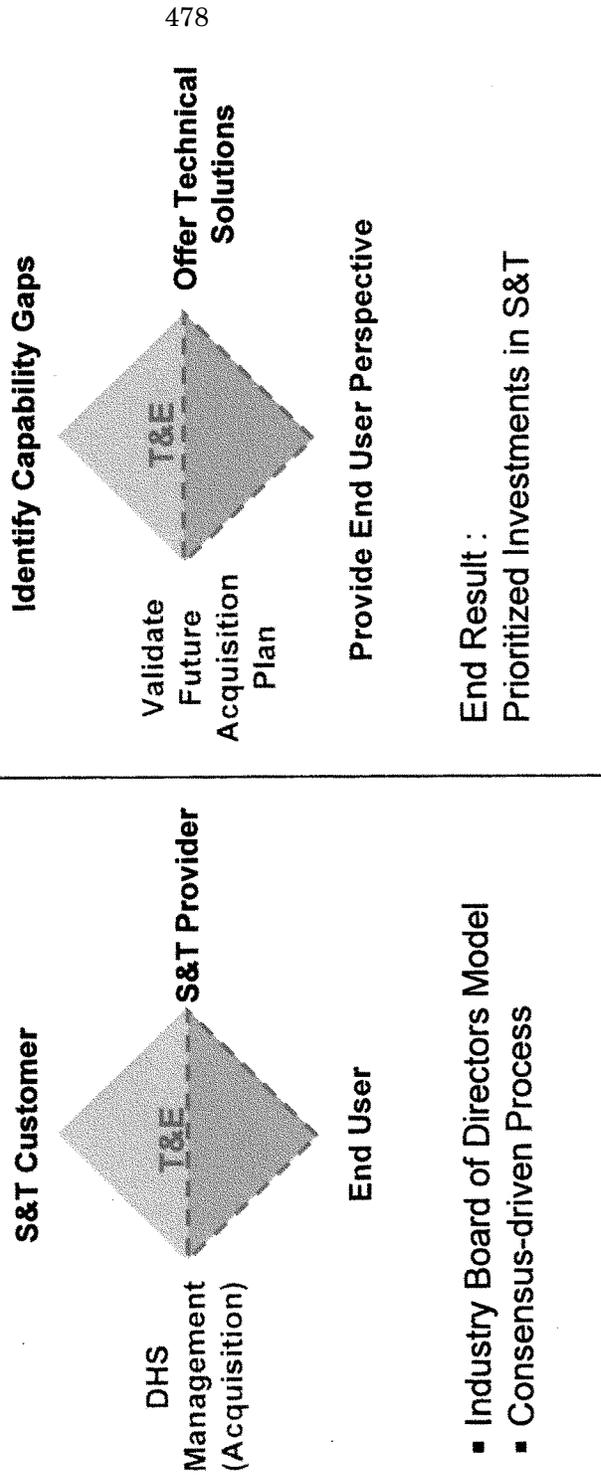
DHS S&T Capstone IPTs

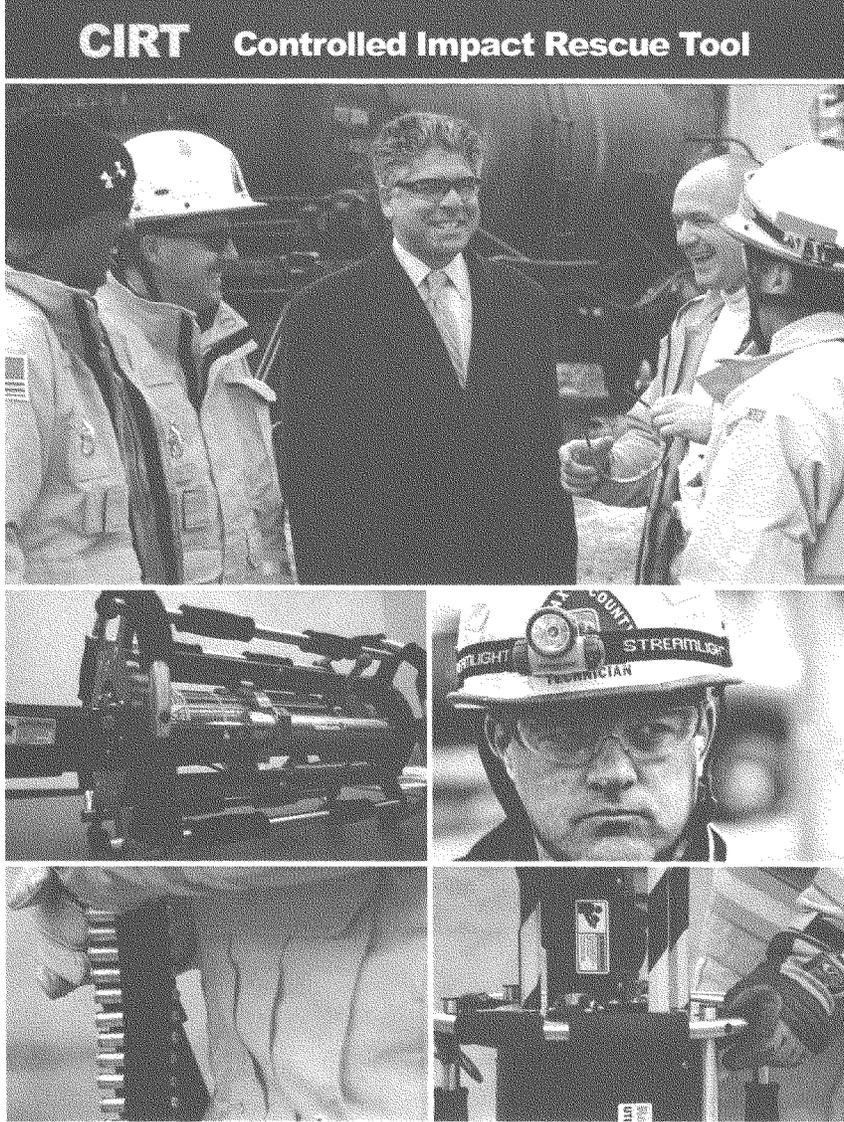
Gathering Mechanism for Customer Requirements:



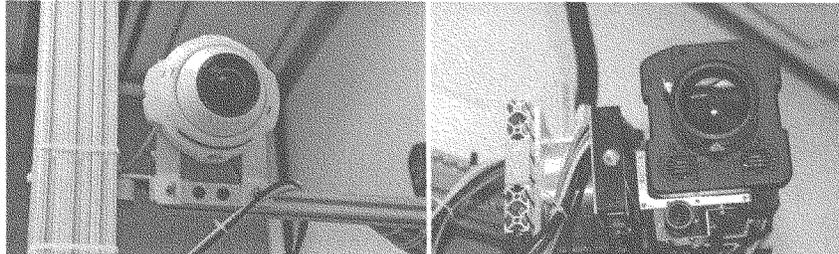
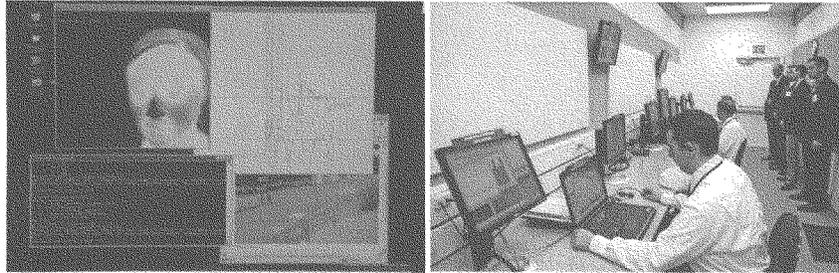
S&T Transition IPT

Members and Function



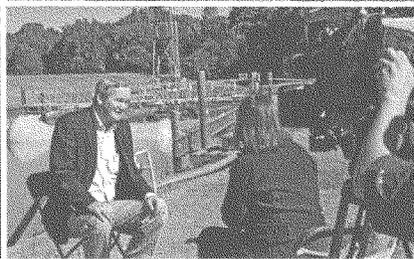
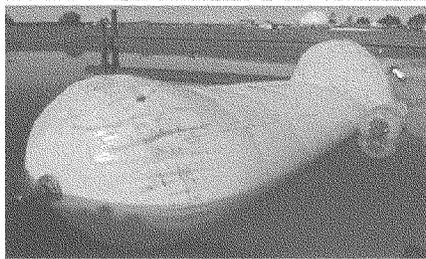
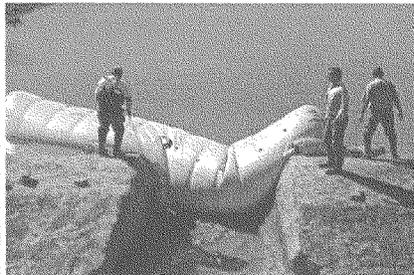
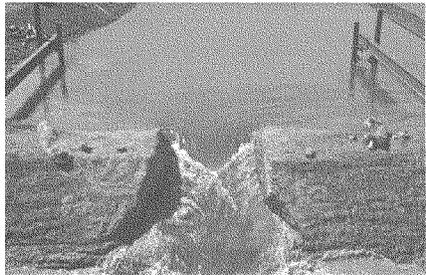


FAST Future Attribute Screening Technology

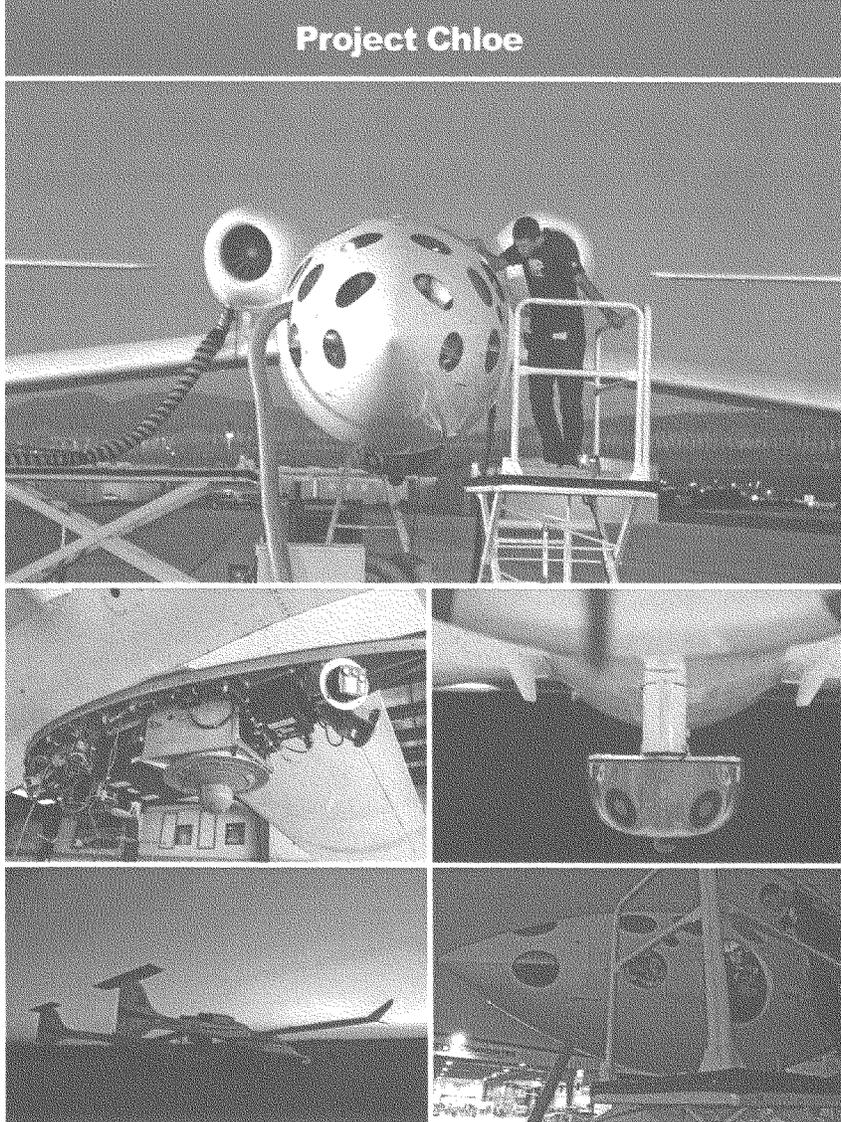




Rapid repair of levee breaching



Project Chloe



RESILIENT ELECTRIC GRID

Mr. PRICE. Thank you. Well, I will begin the questions, and we will focus initially on the innovation projects you touched on, and one of them in particular.

S&T's focus with regard to its research portfolio has been centered on high-risk, high-reward technologies. Because of the high-risk element, and sometimes the high-cost element, it is vital that any opportunity to leverage worked by outside entities is taken, and that there be good coordination with relevant work in the public and private sector.

Now, a good example of one of these high-impact projects is the Resilient Electric Grid, which you referenced. This technology would create a smarter and more efficient electric grid, less susceptible to rolling blackouts by creating a failsafe mechanism within the transmission infrastructure.

A couple of questions about this project, which may illumine the way you operate more broadly.

Please explain briefly what your partnership with Con Edison in the pilot of this project entails. What is the timeline for installing and testing this technology? When will you know if the pilots prove successful? And when could this capability be commercially available?

Secondly, we have had some news reports recently that expressed fears that some of the automated meters and two-way communications and advance sensors in a smart grid infrastructure could be prone to hacking. So I wonder how the resilient electric grid project fits into the overall concept of smart grid technology.

We are putting a lot of investment in this smart grid effort. It is a major component of the Recovery Bill that we passed here. I have some of this work going on in my own district. In many research centers around the country this work is proceeding, and we put great stock in it.

But how does the resilient grid research work? And particularly the focus on the potential disruptions and catastrophes, how does that fit with the overall smart grid work and that concept? Does your project have any role in developing sensors or communications infrastructures that could be susceptible to a cyber attack? And if that is the case, then what have you been doing to leverage the general cyber security efforts to address the problem?

Mr. BUSWELL. Well, thank you, sir, that is an excellent question.

The day before yesterday I was in Oak Ridge National Laboratory at a demonstration of the inherently fault-limiting, fault-current-limiting capabilities of the Resilient Electric Grid.

Now, a little bit of background on the Resilient Electric Grid. This is, as you said, is an HSARPA project working closely with industry, American Superconductor, and also the private sector, Con Ed, or the public utility sector, Con Ed. And it is a cost share. I mean, you know, cost sharing is essentially a third industry and two-thirds DHS.

So the government is getting this product for two-thirds of the price. So I mean, that highlights, as Mr. Rogers indicated, the value, one of the values of the public-private partnerships.

But this is a sample of the high-temperature superconducting cable that was tested Tuesday at Oak Ridge. And this size cable can carry the same amount of electricity as six of these bundles. So 18 of these copper cables would feed the same amount of electricity as this high-temperature superconductor.

So you can see in locations, such as Manhattan, where we are looking at piloting this, that if you look under the streets in Manhattan, it is spaghetti. I mean, there is no room for 18 more of these bundles to feed the electricity, when we can replace it with this.

Now, the value of the superconducting is more than just the compactness and the reliability. If we can connect substations with superconducting capability, we can mitigate the exact kinds of things that you are talking about in the smart grid, that could happen to the smart grid.

The cyber security aside, the SCADA aspects of cyber security aside, which we are doing a lot of work in also, to make sure that the infrastructure is protected from cyber attacks—and I can talk about that separately—the value of this is to connect, for example, in this pilot two substations. We have a fault in one substation. The current is picked up through the superconducting cable between substations, and the loads are uninterrupted. Critically important in critical infrastructure applications, such as the financial district, that relies on power to accomplish its missions; airports. I mean, I cannot think of, I am sure you can think of more examples than I can of critical infrastructure that could be supported by continuous power.

We are looking at a couple of final laboratory tests over the course of this year, and Con Ed is reevaluating where they want to install this technology. Their previously planned location, for a number of reasons, has, they have shifted their thoughts on that. So rather than the upper Manhattan site that they had prepared, they were prepared to install it at, they think that that capital improvement is going to be pushed out because of the electricity demand in that area. So they are looking at a lower Manhattan application. And we expect to have that installed in the next 18 months. And we will know at that point whether it is successful or not.

So this is a really exciting one. And this highlights the importance of basic research, as well. This technology began 20 years before there was a Department of Homeland Security, with the Department of Energy investment in superconducting.

Mr. PRICE. With the basic research taking place at Oak Ridge.

Mr. BUSWELL. Exactly. And other places. But yes, sir, this was Department of Energy basic research on superconducting, for reliability purposes, that we are taking advantage of for homeland security applications, to keep critical infrastructure powered in the event of natural or manmade disasters.

So I think it is, you know, this is a classic example of taking some research that is on the shelf, or has been funded by other agencies; applying it to homeland security situations; and providing increased protection for the critical infrastructure and for the American people.

Mr. PRICE. Thank you. Mr. Rogers.

ENGAGE THE PRIVATE SECTOR

Mr. ROGERS. Interesting discussion. I think what we are trying to get at here at the hearing, among other things, as well as your budget, is how can we engage the private sector in the ingenuity that resides out there, to match that up with the intellectual firepower in our research universities and research labs and so on? And all the while, try to develop an answer to a problem that we have to solve. And in the process, spin off some jobs, producing these products that are being developed?

One innovative way that is working is something that you started three or four years ago. We put together in Kentucky a consortium of all universities and colleges, and asked S&T what the laboratories and scientists that they have on board might be able to tackle. And out of that came a great host of problems that you wanted solved.

And you matched up the research capabilities on those campuses with the problem that you wanted solved. And out of that have come these research projects. And from those projects, for example, I mentioned briefly the MITOC, the Manned Portable Interoperable Tactical Operations Center, which is a mobile unit that was sent to Kentucky during the bad ice storm we had a month ago, where all of the communications were shut down. The Governor could not communicate in or out of any of the towns, practically the whole state.

And the MITOC van, packed with its gear, was sent in, and established interoperable communications between the state and local, and between locals and each other, and saved the day. And that was a product of one of those research programs; University of Louisville and one other university produced that product.

Now it is being commercialized. And the manufacturer, small companies are beginning to hire people to make the product.

Another, for example, is something as simple, how do we protect the raw milk from being contaminated between the milk barn and the processing plant? And we learned in China that that could be a very deadly problem.

And the University of Kentucky and Western Kentucky University put together a project, which I happened to look at a while back, now being commercialized, which establishes a way, utilizing a central communications checkpoint on computer consolidation, to keep track of that milk from milk barn to processing plant. And it is a pretty good link to the fix. That was an S&T project through this university research program.

I think it is an innovative way, and there are many others. But the main idea, of course, is to employ the intellectual firepower that we have on the campuses with the brainpower out there in the private sector, and harness that energy towards the goals that you want. Much like we did in World War II, where we came from nowhere, with nothing; and within four years, was the world's superpower, and defeated two major axes around the world.

I think we are really being slow these days. We are not doing that now as we could and should. And that is why we have you.

Did you hear the In-Q-Tel hearing last year?

Mr. BUSWELL. I did. I was here.

Mr. ROGERS. Is that a workable model? In-Q-Tel has been able to, as an arm of the intelligence community, I think pretty well interact with the private sector and the college sector, research sector. And the private sector, to develop jobs. Is that a good model?

Mr. BUSWELL. It seems to work for the intelligence community. We are not sure. And so what we have done is TSA has initiated a contract with In-Q-Tel to test whether or not this actually works for the Department of Homeland Security. So TSA has committed some funding, I believe it is about \$5 million, to In-Q-Tel; has highlighted some areas that they would like In-Q-Tel to investigate for them. And we will see whether or not we get results.

I am hopeful. But let me talk a little bit about the model that we have in place. And you are absolutely right. The metric of success is deployment of technology into use. I mean, that is the end, that is the end state.

The earlier we can get the private sector involved in that process, the better, because we do not manufacture things. The private sector manufactures things.

And so when public-private partnerships are a win-win-win for DHS, the private sector, and the taxpayer. You get faster speed of execution with the private sector, I believe. Obviously you create jobs and revenue through the production of valuable products that can then be sold in the market. And under certain circumstances, we can actually leverage research and development dollars in the private sector for homeland security applications.

This is our first connection with the private sector. This is the output of our 12 capstone IPTs, the high-priority technology needs. And each one of the IPTs lists 12 or so areas that they are interested in, or problems that have been identified by our customers. When we first published this, you know, I got a lot of phone calls saying are you crazy? You are telling everyone what we are worried about here.

But I went back to my, to a lesson I learned as a young submarine officer, where an old-time Captain—I mean, this guy was really old, he was probably 45—was teaching me how to do a traditional periscope approach and attack on a surface ship. And he looked over at Seaman Diller—and I will never forget Seaman Diller. He was from Snow Camp, North Carolina. May be in your district, I am not even sure. I did not think about that.

Mr. PRICE. Pretty close.

Mr. BUSWELL. But I will tell you, you know, it stuck with me, Seaman Diller from Snow Camp. But he was a fathometer operator. I mean, all he did was do the sounding and make sure the ship did not run aground.

And the Captain pointed at him, and he said, does Seaman Diller know your attack plan? I said, Captain, does everybody have to know my attack plan? And he said, well, only if you want it executed.

So here is our attack plan. And we want as many people, we want everyone, or as many people as possible, involved in the execution.

So how do they do that? If I am in industry and I have an idea of how I can solve one of these high-priority technology needs, what do I do? We have got a long-range Broad Agency Announcement

out; they can come in with white papers. We have received, we received over 300 white papers last year. And we are still in the process of evaluating them, because a lot of them came in late in the year.

But we have asked for 41 full proposals out of that white paper process. And we have received those, and we have funded 27 of those. So we are identifying private sector capabilities to close our capability gaps.

I will also mention, you know, the other aspect of our outreach is this five-year research and development plan. We tell everyone what we are going to be interested in doing research and development on in the next five years, so that they can make appropriate internal investment in their capabilities, and they can plan to support us when we are ready to go out with those, you know, with those solicitations over the next five years.

I believe Undersecretary Cohen mentioned the commercialization project that we started last year. Dr. Tom Celucci, who is a laser physicist by trade, has led the Directorate's relationship with business, and he has got the specific goal of rapidly commercializing products. He is committed to the outreach he needs with dozens of businesses. He has compiled a portfolio of about 300 businesses, with 2,000 technologies that are mapped to these capability gaps, that program managers can go to as they are planning their programs, and see what industry is already doing. And they are using that to good effect.

We have also got the SECURE program, System Efficacy through Commercialization Utilization Relevance and Evaluation. You do not have a good acronym, you do not have a good program. But SECURE is, the idea there is if you tell industry what you need, and you tell them what a reasonable conservative estimate of the market would be, they will invest their own research and development dollars in order to, in order to solve those problems.

Let me give you an example of how this has worked so far. We have, we got a demand from—this came out of some meetings that Secretary Chertoff had last summer with first responders. They felt like they needed a forensic camera that was capable of withstanding a blast, you know, for reconstruction and for law enforcement.

So in June of last year we put out an Operational Requirements Document. We published this Operational Requirements Document on the web. Over the next three months we got 25-plus responses from companies that were interested in providing a forensic camera. Most of those dropped out when they found that we were not going to fund that; that we were just highlighting a market and a capability need.

But a couple companies got it. And we have two examples here, two prototype examples that came in. And this is another. By December we had these prototypes in hand. In February at Aberdeen, we blew up a bus with these cameras installed in it, and we are evaluating the capability of those cameras to withstand the blast and to maintain the data, the visual data, on those, on what happened on that bus.

So by July we will do, we will have that evaluated. If there are corrections that need to be made to these technologies, we will

highlight those. TSA has committed to a pilot program to buy a number of these things, install them on buses, light rail, subways, and the infrastructure surrounding those kinds of things. And we expect that this will be a market release by fall. So that is an example of the commercialization effort, and it is functional.

Mr. PRICE. Thank you, sir. Mr. Rodriguez.

NON-FLAMMABLE GASOLINE AND LEVEE BREAK FIXES

Mr. RODRIGUEZ. Thank you very much. And I guess, similar to the Minority leader, I think he was talking about some of the projects in his area, and you were talking about how do we get something that is out there to the public as quickly as possible.

I know we at Southwest Research have produced a gasoline. In Iraq, whenever the explosions occur on the vehicles, the soldiers sometimes do not get killed, but they burn to death. And this is a gasoline that basically, when you hit it, it does not burn.

How do we move that along as quickly as possible? Or the project that you have here? I just had a levee break in Presidio, and 500 people got displaced. How do we get that item that you have there to hold up the water, you know, as quickly as possible?

Mr. BUSWELL. Well, the levee breach tool is just finishing. We have done a quarter-scale demonstration of that, and we are ready to do a full-scale.

And in parallel with that, we are holding meetings with emergency managers. We had a conference in New Orleans about a month ago to address that.

What is the business plan? Who is going to buy these? Where are we going to store them? How do we get them where we need them in a timely way? And you know, are there staging areas around the country? So we are trying to solve that problem with the state and local governments. Again, this is really important that we, you know, not just demonstrate this technology, but we come up with a way to get it out there.

VEHICLE-BORNE IMPROVISED EXPLOSIVE DEVICES

Mr. RODRIGUEZ. This was actually the dams on the Mexican side release water, and it did not even rain. That is what flooded our community. And so it is going to happen again. And so it is just a matter in terms of how to best do that. At least I know about that one now.

Let me ask you also, you mentioned the blast. We have research in the Pecos area where they have, in Iraq they were looking at the buses that were coming, well, the trucks that were coming in, exploding. And as the people came in, they ran a second one through there, and they were doing some of that research, also, you know. And you mentioned that explosive device in terms of areas that, as they do those studies, once again, how do we get it from there? And you mentioned the booklet that you have there, and people who get the information. That is critical for the communities to get it.

I have ports of entry, and if they do the same thing there—send a truck, and explode, and then as people come and gather they send a second one and explode again and kill a lot more people, you know. And then how do we react to that? And how do we deal with that?

I think we talked about, yesterday in that other hearing regarding something that, you know, the problem we had with the Inaugural here, how do we respond to situations like that with the research that we have?

Mr. BUSWELL. Well, I think the fundamental question is, and this is the purpose of our thirteenth integrated product team, where we are bringing in the state and local first responders to highlight these kinds of issues for us. And by connections through associations, the National Sheriffs' Association, the International Association of Chiefs of Police, Fire Chiefs, National Sheriffs' Association, and individual first responder leaders around the country. We are bringing those people together to inform this thirteenth integrated product team.

And that is a two-way, that is two-way communication. That is not, you know, we are not taking their information without feedback. We had a conference in Bellevue, Washington, at the end of February, where we brought together the first responder community. And they highlighted these very kind of issues. I mean, they gave us their top five, and we went off to work on them.

And one of the ones was the exact scenario that you highlighted: these vehicle-borne improvised explosive devices. And they highlighted the same issue that you are talking about.

We need to know what technology is in the pipeline so we can plan our concepts of operation, and we can plan our, you know, our procurement of these items. Because we cannot afford to bear inventory on items that we are not going to use every day.

Mr. RODRIGUEZ. Not only that, but nothing is worth having the technology and having the research, and not having it implemented when the need is there because no one is aware of it, or we are not sure how to pull it off. So the strategic plan is how to get that technology out there.

Mr. BUSWELL. And we have to create some creative, I think, approaches to, you know, pooling these kinds of resources among, among communities, among states.

Mr. RODRIGUEZ. And in that line, I know the Chairman talked a little bit in terms of the technology that is being devised from a cyber perspective. How do we make sure that people do not mess with it? I would hope you stay on top of that. And I know my time is over.

Mr. PRICE. I am going to return to that in my next round of questioning, let our witness pick up on that.

All right, Mr. Carter.

LIST OF CAPABILITY NEEDS

Mr. CARTER. Thank you, Mr. Chairman. And thank you for being here.

You have got an interesting job. Looking at your two publications that you just showed us, one of them is I guess a short-range plan, and one of them is a long-range plan.

Mr. BUSWELL. Sort of. One of them is really a list of capability needs. These are the capabilities that our customers, the operating components of homeland security, and we will add to this year the thirteenth page, the first responder needs; and the other is our long-range funding profile, our milestones, the kinds of things that

we think we are going to be delivering, and the things that we are going to start over the next five years.

PRIORITIZATION OF S&T EFFORTS

Mr. CARTER. Well, now, is that, that first plan, is that with input from the various departments? Because one of the things that I have a question about is how you prioritize on where you put your Science and Technology efforts, when you have got so many hats in this particular agency?

Mr. BUSWELL. Right.

Mr. CARTER. And is that part of the prioritization formula that you work with?

Mr. BUSWELL. It is. Let me talk about that a little bit. I think you have in front of you the 13 IPTs, right?

Each one of those, as you can see, is led by an operating component. So that at the top of each one of those diamonds is the lead or the co-lead of each of those, of each of those IPTs. And they tell us, it comes straight from them, what their priorities are.

Now, once that is compiled, once we have offered projects that close those capability gaps, then we take it to the Technology Oversight Group. The Technology Oversight Group is chaired by the Deputy Secretary of the Department; that includes the Undersecretary for Management, because that position is responsible for overseeing the acquisition of all of the components. And it does not mean anything unless the components acquire the technology.

And so the Undersecretary for Management is involved, and also the Undersecretary for NPPD, because of the broad preparedness aspect.

So that allows the Deputy Secretary insight into what the components are and have highlighted as their top priorities, and allows trades to be made across there. Perhaps the first unfunded priority in one of the IPTs is more important than one of the other funded priorities in the other IPT, and we can make those adjustments in where the funding goes at that point. And that is done as part of the budget preparation.

Mr. CARTER. So they basically say we need something to find X, anthrax. But they do not say how they want it to work. And you go over and put it out and say, okay, who has got a great idea on how to find anthrax?

Mr. BUSWELL. And we specifically want them to not tell us how to do this, because we want them to be highlighting capability needs, not capability solutions. Because part of our job is to look at the tradeoff among technologies and find out the best combination of ways to accomplish the mission that they have highlighted as——

SECURITY OF CAPABILITY INFORMATION

Mr. CARTER. And I understand your battle plan idea, and you gave a good example of that. But the question I would have is, are there going to be things that are in that request that are going to be things that you can keep secure? Ideas that you need to, in other words, they are not for publication?

Mr. BUSWELL. If you read this, this is a teaser. When you get to the, when you get to the real fundamental operational require-

ments, in some cases, yes. Those will be sensitive to the point where we will not be publishing those, other than in a, you know, a closed forum.

But most of our work is unclassified. I mean, it really is, we really are looking at unclassified kinds of things, because of the people that are going to have to use it. If you are going to distribute these things en masse to border patrol agents, TSOs, cops on the beat, firemen, you cannot be worried about security clearances for all of those people. We have to put together technologies that, you know, that can be used en masse. So we try to keep it unclassified.

Mr. CARTER. If I am running out of time, tell me. Would this go clear to the idea of satellite locations over borders and stuff like that?

Mr. BUSWELL. I will have to go back and—I do not know, I will be honest with you. I will take that one for the record. I am not sure what we have got as far as using satellites for those kinds of things. I will have to—

Mr. CARTER. I will have that question—

Mr. BUSWELL. Yes, I am just not sure what programs that we— we are not funding any Science and Technology, any satellite Science and Technology programs. But I am not sure what the Department has in place. So I will find that out and get back to you.

[The information follows:]

Question. Would S&T share the location of satellites over the border with State and local jurisdictions?

Response. The Science and Technology Directorate (S&T) does not have any satellite programs.

Mr. CARTER. Thank you, Mr. Chairman.

Mr. PRICE. Thank you. Mr. Farr.

CALIFORNIA HOMELAND SECURITY CONSORTIUM

Mr. FARR. Thank you, Mr. Chairman. Thank you for having this hearing.

I think that what we are experiencing on the civilian side is essentially what has been there, and we have not had much exposure to it on the military side, because a lot of these military technologies were not needed domestically. And now we are needing lots of, you know, lots of questions are being asked.

My specific question follows up on Mr. Rogers's issues about how to best—I mean, here we have sort of federal government needs. And with those needs we have buying power, and so everybody will rush to sell us something.

And it seems to me, one, you need to be coordinated in not just the federal community, but in the state community and local community, as well. You need to build these consortiums, which you have done.

I know we have one out in California, the California Homeland Security Consortium, which is a partnership of 23 academic, federal, state, and local government organizations and private sector firms, who are conducting approved field experiments in maritime security, cyber security, and critical infrastructure protection.

And we house that in the Naval Post-Graduate School in Monterey. And I wonder if you intend to continue to use S&T expertise of that Homeland Security Consortium at the Naval Post-Graduate

School for solutions on homeland security problems, like those in the maritime security and cyber security and critical infrastructure protection.

Mr. BUSWELL. Yes, sir, thank you for that question. We are. We have got a strong relationship with the Naval Post-Graduate School. We started a program two years ago to look at funding PhD students from Homeland Security at the Post-Graduate School. The idea was let us look at homeland security technology experts, not just in the Science and Technology Directorate, and specifically not in the Science and Technology Directorate, but across the Department. And see, you know, how would the Department benefit by some high-level education of those folks.

It did not work. We could not get volunteers to do that, and we could not—the components were essentially nonsupportive of the idea.

So we are now re-wickering that into something that might be more workable. It could be a Master's program that we are going to do at Post-Graduate School. But I am going out there with some of my team early in April to meet with the Provost and the President of the Post-Graduate School to see how we can best do that.

On the research side, this consortium that you mentioned is very interesting to us, especially in our new emphasis on first responder and emergency management capability across, across the country.

Monterey, with the Post-Graduate School, is a unique, has a unique position, I think to be an important pilot program for those kinds of things. The local government has identified some things that they are concerned about, and we are going to go and meet with them also, and see what we can do with the research capabilities of the Post-Graduate School. With the understanding that the students there who, you know, many of whom have just returned from Iraq, Afghanistan, and have operational experience in managing crises and understanding the kinds of things that make people, make people want to do bad things.

And we are going to use that as much as we can to run this pilot in Monterey. And I think, I am excited about it. I think it is going to be successful.

LIQUID DETECTION EFFORTS

Mr. FARR. One question. I go through TSA every week. How come, if we are so smart, we cannot take a bottle of water on board? You can take it on board, you just have to buy it inside the circle.

Mr. BUSWELL. I think it might be, I think there might be a conspiracy there among the water manufacturers, but I am not sure. [Laughter.]

Mr. FARR. Well, it has also to do with cosmetics and things like that.

Mr. BUSWELL. Exactly.

Mr. FARR. We heard, I heard that the technology is going to be able to, very quickly be able to not have to dump all that stuff; to be able to run it through screening.

Mr. BUSWELL. I think that is right. We are looking at—the existing technology that TSA is using in their Advanced Technology X-Ray Program we believe has the capability, with the right algo-

rithm and software combinations, to identify liquids. To be able to tell you this is a liquid that is of concern, that this is a liquid that we do not know what it is, and that this is a liquid that is okay to go.

We are not there yet. But we are doing a lot of evaluation at the Transportation Security Lab on new algorithms. We are preparing data packages that then we are providing to vendors that they can use in developing algorithms, and I think we are, we are going to get there.

In parallel, one of the things that we are doing is, in the innovation portfolio we are looking at, I mentioned MAGVIZ. It is a magnetic resonance capability. It works off of really medical kinds of magnetic resonance, where it will identify what a liquid is. And we are looking at—we have proven that it can do that. Now what we are looking at is, how do you display that to a TSO.

And you know, what we would like to do is be able to say this liquid is okay, it comes through on their screen as green. This one is a problem; you can make a homemade explosive out of this liquid, so we are not going to allow this on the plane. It shows up as red. This one, we are not sure what it is; it is not in our portfolio, it is not in our library of liquids, so it comes up as yellow and will require additional screening.

But we demonstrated that at the Albuquerque Airport this last year, and it was successful. So, and that is being run out of Los Alamos National Laboratory, and has a private partner—private sector partner, also.

So we have got a product possibility there.

Mr. PRICE. Thank you very much. Mr. Culberson.

PRIVATE SECTOR INVOLVEMENT

Mr. CULBERSON. Thank you, Mr. Chairman. Thank you very much for your testimony today.

I would like to ask Mr. Buswell about any unobligated balances in the past that agencies had. It has been my impression, and I know you are new on the job, and in previous years on the committee I have been frankly disturbed about the amount of money that has been spent in the Agency without a lot of tangible result. And I know you are working hard to correct that.

The private sector, of course, I would like, if I could, to first of all ask about, could you explain for the committee, give us a little better idea about how you are using competition and allowing the private sector to compete in a way that is objective and peer-reviewed, to ensure that the Agency is acquiring the very best technology at the very best price to the taxpayer? Remembering that we face record debt and deficit. I am sure you have got kids; we are all concerned, we want to make sure that every dollar we spend is spent wisely.

Mr. BUSWELL. Absolutely right. Okay, let me start from the beginning of the process to the point where if we have an idea for a project, the first thing that the program managers do is thorough market research, i.e. what is already being done? What can we leverage that is already existing, or is getting us to the point where we have a jumping-off point that is not creating something out of whole cloth? So that is the first thing.

And then they look at, they do an analysis of alternatives as to how we can go about that. Is it best done at a national laboratory? Is it best done in the private sector? Is it best done at a university? And that is reviewed by the supervisory level within the Directorate.

After that, once a decision has been made and our Office of Procurement Operations agrees that the approach is fair and is the best approach for, for the acquisition, we go—

Mr. CULBERSON. That is what I want to zero in on, is the decision. Who makes the decision, and how do you ensure that you are getting the best value for the dollar in a way that is objective and peer-reviewed?

Mr. BUSWELL. Well, the peer review, the analysis of alternatives is done by the program manager and reviewed by their supervisor. So we have division heads across the Directorate, six division heads who are senior executive level, and look at the analysis that was done for reasonableness. Is this a fair and reasonable approach to executing this program?

We get an independent look at that by a contracting officer, who also looks to see yes, does this, you know, does this meet the criteria of fair and reasonable.

And quite honestly, we do about 20% of our funding through inter-agency agreements with DOE labs, and about 45% is done competitively in industry. So the others, some are universities, and some are other federal agencies.

But the real question becomes where do you get the best value for the taxpayer dollar. And is that done by an inter-agency agreement with a national lab or another federal partner, or is that best done competitively.

My personal opinion is competition is always good. So if you can go to a competitive, you know, competitive award, you are always going to get the best value.

Mr. CULBERSON. It seems it is ultimately up to a single procurement officer, with a second opinion from, as you said, a—

Mr. BUSWELL. It is not a procurement officer. They are a technical expert, they are a subject matter expert on that particular technology. They make a recommendation to their boss; their boss then says yes, that makes sense to me. And then on the procurement side, they look at it for fair and reasonable, for a fair and reasonable assessment.

UNEXPENDED FUNDS

Mr. CULBERSON. And money that you do not spend, it rolls over to the next year?

Mr. BUSWELL. Sometimes we have an unobligated balance at the end of the year. We have had that. It has been shrinking over the last couple of years, and we have been really focused on getting money out the door, because nothing happens until, you know, until we have got money on contract.

But that carries over into the next year, and we execute that, as well.

Mr. CULBERSON. Forgive me if this has already been asked, Mr. Chairman. I have got two subcommittee hearings right on top of each other, so I was running a little behind.

But their committee instructed the Science and Technology Office to report back to us and tell us what you have been doing to attempt to reduce a significant amount of unextended obligations in your R&D accounts.

Have you already submitted that report to the committee? There was one report due at the first quarter of Fiscal Year 2009.

Mr. BUSWELL. Is this the contracting—

Mr. CULBERSON. The first quarterly brief to the subcommittee should occur after the close of the first quarter of Fiscal Year 2009.

Mr. BUSWELL. I will have to check. Two weeks, I am being told by my CFO, is the first one. So, that is right.

Mr. CULBERSON. And of course, we do not want you just shoveling money out the door. I will tell you, my impression is that over the years, that you have probably spent about \$6 billion since the creation of the Homeland Security Department.

When I first got on the subcommittee, I was dumbfounded that you did not have any products that you could even show for all the money that the taxpayers are invested. And you have got to remember, the P. Peterson Foundation headed up by David Walker estimates that every living American would have to write a check for about \$180,000 apiece to pay off existing unfunded liabilities of the United States. And that was as of last March; it has gotten a lot worse.

So it is very important that the money be spent wisely.

Mr. BUSWELL. Absolutely right. But it is also important, and it is important that we get it spent wisely in a timely manner. Because we do not get any technologies until we, until we start getting that money on contract.

I am committed to the best value for the taxpayer dollars, without question. And that is, you know, that is unequivocal.

But I want to make sure—and I also want to say that I am working really hard with the Office of Procurement Operations that reports to the Undersecretary for Management to make sure that we are doing these things the right way and we are doing them in a timely way.

Mr. CULBERSON. But will the report that you are going to give the committee in two weeks also talk to us about making sure the money that you have spent has been spent effectively?

Mr. BUSWELL. I do not know. Is that part of it?

No, that is not part of it. We will explain the obligation to spend under policies balanced by an extended budget.

Mr. CULBERSON. If you are only telling us that you have got it spent. Thank you, Mr. Chairman.

RESILIENT GRID PROJECT CYBER VULNERABILITIES

Mr. PRICE. Thank you. Mr. Buswell, I want to return briefly, and you can elaborate on this for the record if you wish, because I have another question I want to get to, and I think we are going to face some Floor votes here before too long.

But I do want to give you a chance to respond further to the earlier questions about the resilient electric grid project and the vulnerabilities of the smart grid technology. That is, the cyber aspect, which you had referred to, but not really elaborated.

Mr. BUSWELL. Right.

Mr. PRICE. What are these vulnerabilities, as you can briefly assess them? And how is the resilient grid project addressing the cyber aspect?

Mr. BUSWELL. I am not an expert on cyber security, and I did not stay at a Holiday Inn Express last night. So we will get you, I will get you a full answer on the smart grid aspects.

[The information follows:]

Question. What are the cyber security vulnerabilities of REG? How is the REG project addressing cyber security aspects?

Response. The REG technology is uniquely resistant to the vulnerabilities that make the existing power transmission technology susceptible to cascading power failures due to natural or manmade events which include cyber attacks. The current limiting nature of the REG technology reduces a power grid's vulnerability to cyber attacks and would allow existing and future power grids to be designed to mitigate the impact of cyber attacks.

But let me just tell you some of the things that we are doing, because the cyber security is a critical part of our portfolio.

DOMAIN NAME SECURITY

And it all starts with some of this domain-name system security. In other words, you know, the @.org kind of, .gov types of things. Are we sure, when we go to those kinds of websites or we are taking things from those kinds of websites, that it is who they really say they are. And that is one of the things that our cyber security folks are heavily involved in. The secure signer effort, you know, those kinds of things.

So the first part of, or the first aspect of cyber security is making sure that the person that you think you are talking to on the internet is actually who they say they are. And we are working hard on that.

We have actually delivered a couple of things. The Root kit detection technology, which looks at malicious software programs to take control of a computer operating system, which could be the kind of thing that you are talking about in a systems control application. In other words, can we take control of the electric grid operating system, and do nefarious things with that?

That root kit detection and mitigation technology has been developed. It was developed by a company in Maryland, and has been bought by MicroSoft. So MicroSoft is now incorporating that into their operating systems.

There is another similar active malware protection system that, again, increased security and reliability of the computers, that could be used to operate critical infrastructure. That has been, that was developed by a company in Virginia called Endeavor Systems, and has been purchased by McAfee. And they are incorporating that into their, into their security system.

So we have done a lot of work on cyber security at large, much of which applies to the security of critical infrastructure and the operating systems that go with that.

Mr. PRICE. Well, we would welcome a further submission on—

Mr. BUSWELL. Absolutely.

Mr. PRICE [continuing]. The way you are leveraging these general cyber security efforts to apply in particular to the electric grid.

[The information follows:]

Question. How is S&T leveraging its general cyber security efforts to apply in particular to the electric grid?

Response. S&T is conducting R&D to improve security for process control systems (PCS). PCSs control water supply, electrical power, gas and oil pipelines, and other distributed processes. The R&D seeks to advance interoperability with existing PCS systems. This interoperability will allow PCS systems to easily integrate new products into existing systems and enhance information sharing within the critical infrastructure sectors using PCS.

Mr. BUSWELL. Happy to do that. Yes, sir.

NBAF SAFETY ON MAINLAND

Mr. PRICE. Let me turn now to the National Bio- and Agro-Defense facility. Manhattan, Kansas, as you know, has been designated as the site for construction of NBAF. This follows the December publication of the NBAF final environmental impact statement or risk assessment.

Obviously, we take this risk assessment very seriously. The prospect of bringing such a highly infectious disease as Foot-and-Mouth to the United States mainland requires DHS to be very careful and deliberate; and the GAO, as you well know, has underlined that challenge in a report which we took careful note of in our last year's bill.

We restricted any funds for being obligated for construction of the NBAF, until the GAO had reviewed the DHS's risk assessment, in light of their earlier findings.

I understand that GAO work is ongoing with the Department, and that the DIS will be supplemented by such further information as they may need to, to reach a completion of the safety of doing this research on the mainland.

Let me just ask you, if the GAO finds that this environmental impact statement does not support DHS's conclusion that foot-and-mouth work can be done as safely on the mainland as it can on Plum Island, on an island location, how would you proceed concerning that research? And then I am interested, of course, in what kind of additional information you may think, you think may be necessary to determine the additional environmental, economic, security costs of a mainland site, as opposed to the island site?

Mr. BUSWELL. The first part of the question, what would we do, I am not in a position to answer that question at this point. I will go back and get you an Administration position on that.

[The information follows:]

Question. Administration position on NBAF choices should GAO recommend not building NBAF on the mainland?

Response. DHS appreciates the value of the GAO independent review of the NBAF Environmental Impact Statement risk assessment, and, once complete, will take the results of the GAO review into account in NBAF planning.

But as for the second part, I think we would not have selected Manhattan, Kansas as the site if we did not believe that there was sufficient work done to, for us to believe that that was a safe place to do it.

There are, we have to remember that Plum Island was built over 50 years ago. In the last 50 years, there has been a lot of bio-safety improvements done, and we handle a lot of nasty things in bio-security Lab 3 and 4, laboratories on the mainland. And we know how to do this safely.

And I am confident that the design, the operating procedures that we have put in place for NBAF will be successful. And we can, we can expect to succeed in protecting our agriculture from an inadvertent release of some of these diseases that could be devastating.

Mr. PRICE. Well, we are aware that that is your conclusion. And of course, up to a point, that is reassuring. But we are looking for much more, as is the GAO, than simply an assertion, in this regard.

And we are going to have to have, I think, the kind of scrutiny of this that it deserves. And so we will look forward to seeing this matter worked on diligently, and resolved within a reasonable timeframe.

Mr. BUSWELL. And we will be as open-kimono with the GAO as we can be. There are no secrets here. We will lay out to them exactly the research that was done, and the work that was done that allowed us to draw the conclusion that this was a safe place to site NBAF.

INFORMATION AVAILABILITY

Mr. ROGERS. As you have said, most of what you do is unclassified. And yet, we know that al Qaeda and others hack into our systems all the while, to find the vulnerabilities that we have. They do not need to be very diligent, because we print it in our publications, and it is on the web, and so on. And by necessity, you have to do this kind of work in order to get the private sector involved, among others.

Where is the happy medium here? Is there a way to do what we need to do, and yet not educate our enemies?

Mr. BUSWELL. Absolutely. I think, you know, as I said, if you look at this, this is a teaser. This does not tell you the level of detail that you would need to plan and conduct an attack on, on any one of these areas relevant to homeland security.

Mr. ROGERS. But it does tell you where we are weak, and where we have an Achilles heel.

Mr. BUSWELL. It tells you the areas that we are, that we are focused on, and where we think we need to improve, that is right. To the extent—and these are areas that we would like technology to help us in.

That is not to say that we have a vulnerability. We may be compensating with that vulnerability, for that vulnerability in other ways with additional manpower, with additional operating procedures that we could then avoid if we had technology that helped us.

So this is technology. And I, you know, I am very comfortable with the level of detail that we are going to here.

Now, when we get into some of the projects where we are looking at, you know, I gave the example of the homemade explosives, the liquids. The kinds of liquids that we are looking for, the amounts that we want to be able to detect, those sorts of details are the kinds of things that we do not want to publicize, and we will not publicize. We will keep those as secure with the vendors only, with vendors that can work with classified information.

CONTAINER SECURITY DEVICES

Mr. ROGERS. Now, let me ask you about the container security devices. We have been at this for how many years, four or five years, just at S&T. And I am told now that you are looking at an advanced container security device. Tell me what is going on.

Mr. BUSWELL. Let me talk about container security sort of writ large here.

One aspect of container security is a container security device. That would be a device that would lock the doors of a container, and would tell us if the doors were unlocked. That is one aspect of container security.

That would not tell us if somebody came into the side of a container. It would not tell us if something was in the container to begin with. So we are looking at all of those kinds of aspects of container security.

Let me talk about a couple of things that we are doing. We have a program where we are looking at—and let me also say that this container security technology and policy is all intertwined. And I think some of the, some of the non-progress that may have occurred early on in this program, before the last couple of years, really had to do with the hand-wringing over the policy versus the technology.

And what we decided to do is, look, if we provide the technology, it gives us, it allows us to start the policy discussions up here. Where if we do not have any technology, we are talking about policy discussions way down here.

So let me talk about—and there also has to be, without regulation there has to be a voluntary reason for shippers to do this. So they have to have some value added to implementing these technologies.

We are looking at a hybrid composite container, for example. Fifteen percent lighter than the steel containers, we can embed sensors in the walls of these containers that will tell us if the container has been breached. We can put sensors in the containers that will tell us if there is something nefarious in the container. And we are working on those sensors, as well.

So we are looking at connecting that to the Marine Asset Tracking Tag system that we are demonstrating right now between Yokohama, Japan, and the U.S. We have got a number of these things that are wireless and can communicate the status of the container across multiple bands: satellite, wireless, WiFi, cell phone, real time. So it will tell you this container has been opened, real time.

We are looking at the Advanced Container Security Device. And we are still working on the Container Security Device, and we think that we will have the testing done on that. We have got two vendors that have come in, and we will complete the testing of that by the end of this calendar year. And it will be available for market shortly thereafter.

But we still get back to the policy. Why should someone use this? It has to be of value to them. So if we can help them with their cargo-tracking capabilities; if not only is it telling you that this container is secure, but it is also telling you where your container is;

those are of interest to shippers. Those kinds of things are of interest to shippers.

Mr. ROGERS. Have you asked, just ask UPS to tell you how they do it?

Mr. BUSWELL. No, UPS and FedEx are really good at it. Walmart is really good at it. But they are not international, but they are not working in the volumes that we are talking about, and they are not working in the security environment that we are talking about. So there is some work to be done.

We think we are going to get there, but we have to work with CBP on the policy aspects of this in parallel with the technology development. Because the technology, you know, as we have said several times already in this forum, technology without implementation is of no use.

Mr. ROGERS. Thank you. Thank you, Mr. Chairman.

Mr. PRICE. Thank you. Mr. Rodriguez.

STRATEGIC PLANS

Mr. RODRIGUEZ. Thank you very much. And once again, thank you for being here with us.

On your chart, I know that the first one you mentioned, the information and management, are the importance of educating and getting that information across.

In speaking about that, when you look at border security and chemical, bio, and cyber security, do we have strategic plans that are available, that people can see in those specific areas? Do we have that?

Mr. BUSWELL. I think it varies from component to component. What they have published as far as their strategy goes, I mean, of course the Department has a strategic plan that we dovetail into. We are operating probably four layers below, you know, that strategy.

We take our, in these integrated product teams for example, in the information management, we are talking to the Intelligence and Analysis Branch of Homeland Security as to what their needs are. And they have a strategy as to how they want to compile information and get it to fusion centers—for example, the state and local folks—for use.

Mr. RODRIGUEZ. And in terms of not only the strategy, but in terms of also the things that I know, you know, we kind of look at who is bringing in the explosives, who is bringing in the bio. But the more natural things, on the biochemical for example, the TICs that come across that we have a serious problem with, that could basically, you know, quarantine all U.S. meat and create a serious problem. Do we look at those kind of things?

We have the Carrizo cane that creates a serious problem for border patrol and security on the border. Do we have a plan there to, you know, on those aspects on cyber security, to continue the importance of educating people in the private sector, and assuring that they will be cautious?

Mr. BUSWELL. There are—let me take them sort of one at a time.

The Carrizo cane, we are working hard on that with CBP. They have got some plans; we have got some experimental ideas that we are looking forward to starting soon. So that is one—

Mr. RODRIGUEZ. Let me know if I can help, because we need to get rid of as much of that stuff as we can.

Mr. BUSWELL. We agree. We agree. As far as the strategic plans in other areas, cyber, they are of varying maturity, I will say, across the government, across the entire government. Cyber is obviously something that there is a huge inter-agency effort on.

And we take our cues from their plans. So the investments that we make are, are advised by those plans, and advised by the highest-priority capability needs that those plans address.

So I would tell you that we do not invent the science that we do research on, we do not invent the areas. We take that from the customers.

CYBER INTRUSIONS

Mr. RODRIGUEZ. And on a more secure basis, on cyber for example, I know that when I was in Higher Education back in the Texas House, they did not tell us about the number of attempted rapes or things that happened on a university, because they wanted to keep it quiet.

The same for the private sector. I know that there is problems in the banking system with cyber. They are going to keep that quiet, because it is not good for the consumer to hear that.

How do we begin to work with the private sector to really see how serious the problem is? Because I know that it has doubled and quadrupled, and even doubled again in terms of the whole issue of cyber intrusions that have occurred.

Mr. BUSWELL. I am going to take that for the record, because I am not sure what we have across the government that talks about that.

But I think you are having a cyber hearing here in a little bit. And one of the witnesses will be the Program Manager, Doug Maughan, who runs our cyber program. And he is fully versed on these things.

So if I can defer to Doug at a future hearing, that would be terrific. But he is fully engaged.

[The information follows:]

Question. What is the magnitude of cyber intrusions in the private sector and how are we working with them on that?

Response. According to a case study published by the U.S. Cert in 2005 (http://www.us-cert.gov/control_systems/pdf/undirected_attack0905.pdf), cyber intrusions cost companies billions of dollars per year. The S&T Cyber Security R&D investment activities directly addresses a wide range of cyber attacks and vulnerabilities affecting both the Government and private sectors spanning malware detection, improved monitoring and reporting, and technologies to improve the security of existing Internet infrastructure. A prime example is S&T's Domain Name System Security (DNSSEC) initiative. DNS is a critical underpinning of today's Internet, responsible for mapping Internet Protocol (IP) numbers to domain names and without which the Internet would be unusable. Various types of DNS based attacks have been directed toward the private sector to successfully attack business-critical processes, prevent access to web sites, and compromise customer identities, accounts, and computers. Many DNS attacks can be prevented through the deployment of new security mechanisms for signing and validating DNS data. The DNSSEC initiative provides these solutions while driving their deployment, adoption, and use to help secure a crucial element of Internet infrastructure for both the private sector and Government. A DNSSEC Industry Coalition recently formed to work collaboratively to facilitate DNSSEC adoption.

Mr. PRICE. We will be having an Executive Session on cyber security later in the season. But in the meantime, what you can furnish for the record along these lines, we would—

Mr. BUSWELL. My pleasure.

Mr. PRICE [continuing]. Be very glad to see. I think we can get in the remaining questions here. The votes have been called. I will ask both questioners and answerers to proceed, very briefly though, starting with Mr. Carter.

FOLIAGE-PENETRATING RADAR

Mr. CARTER. Thank you, Mr. Chairman. Real quick, getting back to what my colleague from Texas was talking about, this Carrizo cane.

I know that one of the issues that has been out there that the Air Force and a bunch of other people have been trying to figure out, how to get foliage-penetrating radar to go through things like that cane, you know. I am not as sensitive as others; I just cut it down. It is a sensitive issue.

Do you have any idea what kinds of technology that they are looking at in particular for that, for penetrating that pretty dense cane and mesquite rush barriers along the Rio Grande River?

Mr. BUSWELL. I would, I am not sure that foliage-penetrating—we do not have a program in foliage-penetrating radar.

Mr. CARTER. If you do not have it yet, I think it is risky. I think you have got to get—

Mr. BUSWELL. Yes, sir, that is right. And as you said, there is a lot of work going on in the Department of Defense for those kinds of capabilities.

We would probably tend to leverage those investments that are much larger than anything that we could probably bring to bear. That is our strategy there.

As far as getting rid of that, you know, that nasty Carrizo cane, there is a combination effort of herbicide, and we have got an insect that will eat it. We have got a wasp that will eat the cane that we are planning on testing down there, you know, with CBP.

I read in the newspaper last night that there has been an injunction on doing anything against Carrizo cane. So we will—

Mr. CARTER. Well, we got more than our share of wasps down there. I hunt down in that area; we do not need any more wasps, thank you. [Laughter.]

Mr. CARTER. Thank you, Mr. Chairman.

Mr. PRICE. All right, Mr. Farr.

MITOC

Mr. FARR. Thank you. What I was interested in was MITOC program, essentially developed through the military and the Navy and used in, for the first time, kind of operational in the tsunami in India. And when they came back, they improved it. And then working with the private sector, field-trialed it in Kentucky. And I guess that is where the university has really taken it on as a center there.

Those are the kinds of things that I am really interested in seeing that we do that is an operable connection. And I know you are going out to Monterey. And I was reading your testimony that you

want to decrease the time for detection of a wide area of bio-aerosol release? The Navy lab out there has done remarkable experiments on this, that is essentially the Navy lab dealing with weather, because the Navy weather station is there.

Mr. BUSWELL. Right.

Mr. FARR. But you might check it out. It is right next to the campus of the——

Mr. BUSWELL. My pleasure. I have been there several times to METOC there at the——

Mr. FARR. So that is all the comment I had to make. Thank you for the hearing.

Mr. BUSWELL. Thank you.

Mr. PRICE. Thank you. And with that, we will go off to do our duty on the Floor. But we want to thank you for the good work you are doing, and for this helpful testimony this morning. I look forward to working with you as we put the budget together for the coming year.

Mr. BUSWELL. My pleasure. Thank you very much, Mr. Chairman.

Mr. PRICE. Thank you. And the Subcommittee is adjourned.

QUESTIONS FOR THE RECORD SUBMITTED BY

CHAIRMAN DAVID PRICE

Acting Under Secretary Bradley Buswell
Developing and Transitioning Homeland Security
Research Products Into Use

BioWatch

The Committee is aware that S&T is currently field-testing, in a limited capacity, the Bio-Agent Autonomous Networked Detector (BAND) technology. However, the Testing & Evaluation and Standards (T&E) component of S&T claims not to know any details of this testing, nor have access to any of the data.

Question: What is S&T doing to coordinate these testing efforts within the BioWatch program, and to eliminate this type of stove-piping with any other research projects, either now or in the future?

ANSWER: The S&T Directorate's Testing and Evaluation (T&E) and Standards component has access to all Bio-Agent Autonomous Networked Detector (BAND) test data. This data will be reviewed by the Office of Health Affairs if the BAND performer is selected to participate in the competitive field testing that is planned over the next year to select the technology to enter low-rate initial production for the BioWatch Gen 3 program.

There are multiple stages of test and evaluation (T&E) required to take a technology from the laboratory to a fully operational deployment. The three primary testing activities in an acquisition program must remain separate and independent to maintain the integrity of the results and the procurement.

Testing in a science and technology development project is technology demonstration. Technology demonstration is done to demonstrate that a technology or a system meets key design parameters. The system is measured against known inputs and circumstances to determine if it meets such parameters as: detection sensitivity and specificity, maximum number of false positives, operating temperature range, and mean detection time. This step is performed by the developer to establish the performance capabilities of the prototype system prior to transition to an operational entity.

The next stage of T&E is developmental test and evaluation (DT&E). This occurs when an acquisition is underway and the operating entity procuring the system operates the prototype in the field under real world conditions, but the test is overseen and conducted by trained technicians. This stage is necessary for the purchasing entity to verify the developer's performance claims and to determine any unforeseen operational issues that require the system to be refined, reengineered or improved prior to low rate initial production (LRIP).

Operational test and evaluation (OT&E) is the stage where validated production units are deployed in an extended pilot and operated purely by the end-users in the field. This stage, if successful, leads to full production and deployment since the system performance has been verified and now user interface issues can be addressed and overcome.

The S&T Directorate has multiple responsibilities in the T&E of homeland security technologies. This includes testing of technologies being developed or acquired by the Department and those being developed or acquired by third parties. S&T performers, under the oversight of their program managers, conduct technology

demonstrations for their technologies during the developmental stages of the project. In addition, the S&T Director of T&E and Standards is responsible for approving the T&E plans for acquisition programs of interest across the Department. The acquisition program's T&E plan includes both an independent evaluation of the technology and operational testing. The S&T Directorate must continue to maintain independence between the technology demonstration portion and the development of the DT&E and OT&E plans to maintain the integrity of the procurement process.

The Bio-Agent Autonomous Networked Detector (BAND) system testing is still in the technology demonstration stage. It should move soon to the acquisition phase where it will be subject to the test and evaluation master plan (TEMP), which will be approved by the Director of T&E and Standards and executed under his oversight.

Question: Please provide a table showing what projects S&T is involved in related to BioWatch for 2009 and planned for 2010. As part of this response, please include a brief description of the project and anticipated outcome, identify funding levels for each year, and include milestones for completion.

ANSWER: The projects under the Chemical and Biological Division's Surveillance and Detection Research and Development (R&D) Program are aimed at furthering the next generation of bio-detection capabilities and will benefit future BioWatch and other bio-detection systems. All project funding with a direct link to the Generation 3 BioWatch system ended in FY 2008, but there are some deliverables and milestones associated with the Generation 3 BioWatch Detection System Project that will occur during FY 2009.

Surveillance and Detection R&D Program – FY 2009: \$35.099 million; FY 2010 estimate: \$41.404 million. Develops next-generation detectors for biological threat agents, including fully autonomous detection capabilities for the third generation (Gen 3) BioWatch system. These detectors will operate with lower costs and faster detection times – thus significantly increasing the protected portion of the U.S. population. In addition, this program works to develop the assays (i.e., signatures or fingerprints of biological agents) needed to enable detectors to accurately recognize a biological agent. This project is also developing detect-to-protect systems specifically for use indoors.

BioWatch Generation 3 (Gen 3) Detection System Project – Develops the Gen 3 BioWatch detection system, including development of: (1) the Bio-Agent Autonomous Networked Detector (BAND), an automated, fully integrated "lab-in-a-box" that is capable of aerosol collection, molecular analysis, identification, and reporting of results with networking capability for real-time control of the entire sensor network; and (2) Deployable Aerosol Collection Systems (DACS), remotely programmable, automated samplers that can preserve viable samples for one to three days. The automated detection capabilities provided by BAND and DACS will significantly reduce BioWatch per unit operational costs, thereby allowing expanded and more frequent monitoring of the U.S. population. In FY 2008, the project initiated the commercialization phase of Gen 3 BioWatch detection systems. The S&T Directorate requested no funding for BAND beyond FY 2008; however, in FY 2009 the project will be prepared to transition the detection system and initial assays to OHA for the field test of Gen 3 BioWatch.

Bioassay - Near Term Project – Develops assays (fingerprint signatures of biological agents) employed within detectors to recognize biological agents, and provides bioinformatics resources and nucleic-acid signatures for use on commercial instruments. This effort develops bioassays for use in U.S. Government-deployed systems to provide an extremely high confidence that the detection warrants further action and investigation. These government-specific operational assays will allow Generation 2 and Generation 3 Biowatch to detect the top-twenty aerosolized biological threats identified in the 2008 BTRA. This project is also establishing a mechanism to independently evaluate and validate assays for first-responders and the private sector. In FY 2008, the project developed and transitioned assays to detect 10 biological threat agents and began the pilot evaluation of the Public Safety Actionable Assay (PSAA) process. The PSAA process should qualify biological

identification systems that an array of government and responder entities may use. In FY 2009, the project will transition characterized assays to OHA through CDC for use and support of the BioWatch laboratory network. In FY 2010, the project plans to transition the PSAA process to establish initial operational capability. In FY 2010, the project also plans to transition additional Gen 3 BioWatch characterized assays to OHA through CDC to support Gen 3 Biowatch assays.

BioAssays – Next Generation Project – Develops new approaches for detecting the broad range of possible future threats. The current strategy is to use basic biological building blocks – the subsystems that enable an agent to infect a person, to grow, and to multiply – as a way to identify future threats. This project is identifying fundamental building blocks, such as infectivity, virulence, and antibiotic resistance-mechanisms, and developing appropriate assays for them. The S&T Directorate will use these new assays and their associated detection platforms to create novel sensing technologies consistent with the national architecture. In FY 2008, the project began laboratory studies to provide an initial proof-of-concept for novel sensing technologies. The project also developed performance requirements, based on the performance characteristics of current operational systems and input from DHS customers, and identified a number of possible approaches for meeting those requirements. Because this is a difficult problem, the S&T Directorate must conduct research on a number of these approaches before determining which is the most likely to succeed. In FY 2009, this project will initiate multiple research efforts aimed at identifying the most promising approach for detecting a broad range of possible future threats. In FY 2010, this project plans to identify assays for use in conjunction with the concepts being developed by the Next Generation Biological Detection project.

Detect to Protect (DtP): Remote Sensors and Triggers and Confirmers Projects – Develops low-cost, bio-aerosol sensors and triggers to detect biological agents within one minute (acting as reliable 'bio smoke alarms') for protection of high-value facilities and their occupants. This project will provide commercially available detection systems that could enable transportation, entertainment, and other high-value facilities to monitor for airborne hazards and take low-regret precautions (e.g., turning off ventilation systems) to protect people by preventing mass exposure. In FY 2008, the project developed prototypes suitable for extended field-testing, with plans to subsequently transition the systems to the private sector through product commercialization. There is no funding requested for this project beyond FY 2008; however, in FY 2009, project will complete the final round of prototype evaluations in operational environments.

National BioSurveillance Integration System (NBIS) Project – Provides decision makers early identification of biological events of national significance, such as disease outbreaks, the potential use of biological agents, and emerging biohazards. The S&T Directorate supports OHA's operation of NBIS by providing subject matter expertise and developing modeling tools. NBIS acquires, integrates, analyzes, and disseminates information from existing human disease, food, agriculture, water, meteorological, and environmental surveillance systems and relevant threat and intelligence information. NBIS is currently developing a robust, domestic system that will assist with biosurveillance and provide a core, permanent, open-source biosurveillance capability. This project significantly improves information sharing and situational awareness for decision-makers and provides a common operating picture for all participating agencies to enable timely response to biological events. In FY 2008 through FY 2010, the S&T Directorate will provide subject matter expert (SME) support for bioinformatics, information technology systems, and NBIS operations. In FY 2009, the project will support model development to provide additional operating capability to the development and deployment of the Biosurveillance Common Operating Picture (BCOP) and to continue to provide subject-matter-expert support in bioinformatics and information technology systems. In FY 2010, the project plans to continue model development and platform enhancements to support an operational NBIS capability.

Next Gen Biological Detection Project – Starting in FY 2009, this project will develop technologies and systems to detect enhanced, emerging, and advanced biological threats. The project will explore universal detection technologies that do not require prior knowledge of the biological threat target, working to develop an automated, fully integrated, end-to-end (collection, identification, and reporting) system. This system will indicate the presence of a novel agent, provide rough quantification of the amount of that agent, and preserve

samples for further analysis. This project will both draw on and inform the BioAssay – Next Generation project described above. The S&T Directorate will initiate the Next Generation Detection project in FY 2009 with the solicitation of fundamental research in support of technology concepts, selection of performers, and initiation of laboratory studies to demonstrate technical feasibility. In FY 2010, the project plans to support the technology feasibility demonstration of chosen concepts.

Portable Bio Detector Project – Starting in FY 2009, this project will develop a hand-held biological detector/identifier in a spiral development process, beginning with a target to classify unknown samples as potential biological threats and culminating in approaches that identify (at species level) across an array of known agents. Target users are customs/border agents and responders. In FY 2009, the project will deliver several trade studies to assess the requirements to fully understand the required capabilities. In addition, based on the trade studies, a technology assessment will explore current technology and determine the best path forward. In FY 2010, the project plans to identify technology solutions for the rapid, on-site discrimination of potential biological agents and initiate development of concepts of operation for these technologies in target application environments.

Viable Bioparticle Capture Project – Develops an automated sampler compatible with laboratory analysis, sealed for safe handling of potential positives, providing preservation of sample viability for one to three days. The final system will augment BioWatch information by characterizing the viability of a threat during an attack and enable more definitive post-event characterization of bioterrorist events. Starting in FY 2009, the project will solicit technology concepts and select performers. In FY 2010, the project plans to identify concepts for improvements to deployed aerosol collection systems.

Multi-Application Multi-Plex Technology Platform – Develops a single technology platform in which assay cartridges may be changed based upon facility/agency specific needs. The project will ensure that different assay cartridges are validated for use by specific agencies. Assay cartridges can be immediately shipped to supporting agencies that have the same platform in order to provide surge capacity support for event mitigation. This technology will test for traditional agents, enhanced agents, emerging agents and advanced agents with the ability to perform up to 100 tests or detect 100 targets simultaneously within a single sample. The project started in FY 2009 and plans to conduct a technology feasibility demonstration in FY 2010.

Rapid Test Methods for High Volume Analysis project - Identifies key areas for improvement in laboratory analytical methods for high-throughput and on-site analysis of suspect food products. The overall project will target contamination concerns, including chemical, biological, and radiological contaminants that pose high risk to the American public or economy by undermining the safety of the agriculture/food infrastructure and supply. Investment in this area will enable more rapid detection of food contamination; provide prompt assessment of the scope of risk presented during a food contamination incident; support enhanced ability for epidemiological trace-back investigations, and will ultimately minimize the impact of food contamination events to both public safety and the economy. In FY 2010, the project plans to develop a systems study report identifying highest leverage investments.

Question: If the Autonomous Pathogen Detection System (APDS) being tested by OHA were to be evaluated as an unacceptable option for a full-scale BioWatch system, would that shorten the timeline for the test and evaluation and standards evaluation of the other systems, and the Low-Rate Initial Production phases?

ANSWER: The current plan is to release a request for proposals to solicit a full and open competition for bio-detection technologies for field testing against Bio Watch Generation 3 specification beginning in January 2010 – this includes Autonomous Pathogen Detection System (APDS). Technologies that pass the field test will go into low-rate initial production (LRIP) after a short engineering phase. The field test will determine if APDS or any other technology is acceptable for full operational testing. The timeline for the full operational testing will be driven by the engineering phase and production time to deliver LRIP units.

Regional Biocontainment Laboratories

Question: Please provide the Committee with an update on the status of S&T's coordination with the National Institutes of Health (NIH) regarding Regional Biocontainment Laboratories (RBLs). Have the RBLs presented the information S&T was waiting for to the Centers for Disease Control (CDC)? When does S&T expect to begin these coordination efforts? Have any more RBLs come "on-line" since last year?

ANSWER: The Regional Biocontainment Laboratories (RBLs) are infrastructure established by the National Institutes of Health (NIH), National Institute of Allergy and Infectious Diseases (NIAID). The S&T Directorate had discussions in spring 2008 with representatives of the RBLs to gain a better understanding of the capabilities they might offer. The S&T Directorate requested an estimate of potential charges for research efforts related to S&T Directorate activities. The S&T Directorate also requested that the laboratories make an additional estimate of the potential laboratory surge capacity they might represent in case of need in a substantial biological contamination event and associated cost, and to present that estimate to the Centers for Disease Control (CDC), which has the obligation to identify and maintain surge capacity for biological samples. In fall 2008, the S&T Directorate provided FOUO information (under a non-disclosure agreement) from the 2007 Laboratory Response Capability Assessment of the Integrated Consortium of Laboratory Networks (ICLN) to several RBL directors to inform their perspectives on potential sample analytical requirements in the event of a large-magnitude biological event. The S&T Directorate has not yet received a response. In the absence of a response, the S&T Directorate staff managing the ICLN assessed, based on the investment the CDC makes in the approximately 150 labs in its Laboratory Response Network, that the substantial institutional investment the RBLs sought to potentially provide surge capability is very high compared to the potential benefit. S&T Directorate provided this assessment to National Institute of Health, National Institute of Allergy and Infectious Diseases management staff in early April 2009.

The RBLs have not provided the estimate of potential surge testing support and associated costs to the appropriate CDC Laboratory Response Network staff, as identified by the S&T Directorate to their representatives. In the absence of a response, the S&T Directorate staff managing the ICLN assessed, based on the investment the CDC makes in the approximately 150 labs in its Laboratory Response Network, that the substantial institutional investment the RBLs sought to potentially provide surge capability is very high compared to the potential benefit. S&T Directorate provided this assessment to National Institute of Health, National Institute of Allergy and Infectious Diseases management staff in early April 2009.

The S&T Directorate's coordination with the National Institutes of Health (NIH) on the RBLs is complete. The S&T Directorate communicated its information regarding anticipated sampling and analysis needs for prototypical biological events to the RBLs to inform their perspectives and has directed them to communicate with CDC Laboratory Response Network management regarding potential services and costs. CDC holds responsibility for determining which laboratories will support its Laboratory Response Network.

As of last fall, seven of the 13 Regional Biocontainment Laboratories (RBLs) were still under construction. The RBLs are infrastructure established by NIH's National Institute of Allergy and Infectious Diseases (NIAID), and NIH NIAID would be best positioned to address the specific operational status of each RBL.

Chemical Programs

Question: Last year S&T notified the Committee that they were expecting to conduct a full-scale demonstration of an integrated CBRNEe detection system solution for the first time in April of 2009. Has that demonstration taken place? What are the future plans for this technology including any potential funding in the upcoming fiscal year 2010?

ANSWER: A number of demonstrations of the pilot integrated CBRNe detection system took place in 2008 and 2009. An operational pilot is deployed in the Los Angeles and Long Beach, CA, region that allows information from chemical and radiological sensors to be shared using open communication standards with a number of local government agencies in California, including: City of Los Angeles and Los Angeles County (sheriff, hazmat, fire, police, public health); City of Burbank Fire Department, City of Glendale and the City of Santa Fe Springs Fire Department. In addition, the system was operationally deployed for a number of special events in 2008 and 2009 in Los Angeles, Long Beach and Pasadena. Some of these events include the 2008 Golden Phoenix demonstration, 2008 Emmy Awards Ceremony, the 2009 Academy Awards Ceremony, the 2009 Rose Bowl Parade, the 2009 World Baseball Classic, and the 2009 Los Angeles Grand Prix.

Additional pilots are either under way or in the planning phase and will be implemented by the end of calendar year 2010. The pilot locations include Anaheim, Calif., Seattle, Wash, and an East Coast city to be determined (Baltimore, Md. or Boston, Mass.). The S&T Directorate is funding a large-scale Los Angeles regional exercise 'Golden Phoenix' that is tentatively scheduled for June 2010. The exercise provides for the evaluation of several integrated CBRNE project components (i.e., local, state, federal communications) and will produce data and metrics to help measure and demonstrate project successes. Many federal and state agencies are planning to participate in this exercise.

In addition to regional integration activities, the S&T Directorate is working with the DHS Domestic Nuclear Detection Office Chief Information Officer and the DHS Chief Information Officer to submit a CBRN Detection Information Exchange Packet Document (IEPD) that will be incorporated into the National Information Exchange Model (NIEM) to facilitate integration of CBRN detection information throughout DHS as well as support information exchange between other federal and local entities. A guidance document, including technical design concepts, open standards, concepts of operation, and lessons learned, will be made available to local, state and federal entities to serve as a template for future implementations.

Counter MANPADS

Question: What is the status of the research and development to test counter MANPADS devices on passenger air carriers. As part of this response, please update the Committee on the status of the evaluation of systems on cargo and passenger airlines that was previously scheduled to be concluded in the spring of 2009. In addition, please provide any other clarification on the upcoming timeline for development and testing of both in-air and other counter MANPADS systems, including an update on the Phase-3 testing of these systems.

ANSWER: The S&T Directorate is currently executing the final phase of the three-phase Counter-MANPADS program assessment. Phase III emphasizes three major objectives:

- 1) Conduct a suitability assessment on in-service cargo aircraft,
- 2) Conduct a suitability assessment on in-service passenger aircraft, and
- 3) Conduct live-fire tests to assess system capability to protect commercial transports.

All Federal Express flights for the cargo service evaluation portion of Phase III occurred before February 29, 2008. The S&T Directorate completed analysis of the cargo service evaluation data and will provide findings in a Phase III final report in late 2009. To fulfill the passenger service assessment portion of Phase III, the S&T Directorate is evaluating prototypes on three American Airlines passenger aircraft. The first flight took place in August 2008. The program's goal is to achieve between 5,000 and 7,000 flight hours by the end of June 2009.

The S&T Directorate also conducted live fire tests as part of Phase III. The two-and-a-half month test concluded in mid-December 2007 and analysts are reviewing the test results. The tests demonstrated the systems' capability to protect commercial transports from man portable air defense systems (MANPADS) and

to identify any anomalies in system performance. Live fire tests used the Aerial Cable Range at the White Sands Missile Range in New Mexico by firing real heat-seeking missiles at a target representing the infrared signature of a Boeing 747 aircraft. During the test, both systems experienced some anomalies and corrective actions have been identified. The S&T Directorate is assessing the corrective actions with a scheduled completion by July 2009.

The current in-service evaluation of the systems on cargo and passenger airlines will end by July of 2009. Because the Counter-MANPADS program was extended, the S&T Directorate will submit the final, comprehensive Phase III report in late 2009.

The Emerging Counter-MANPADS Technology (ECMT) program's task is to "evaluate emerging civil aviation defense technologies," and assess the suitability and interoperability of counter-MANPADS technologies, other than directed infrared countermeasures (DIRCM), for use in a civilian airport environment. Additionally, the program is to estimate life cycle costs (LCC). The program assessed three concepts: Northrop Grumman Space Technologies Skyguard ground-based high-energy laser concept; Raytheon Vigilant Eagle ground-based high-power microwave concept; and L3/Avisys decoy concept using a Doppler radar missile warning system.

The S&T Directorate completed the ECMT assessments in late 2008 and concluded that all three were at a low technology readiness level (TRL) as systems even though some of the components were at a high TRL. None of the concepts exist as complete systems and would require significant research, development, testing, and evaluation (RDT&E) to become complete systems. Significant civilian environment suitability issues remain for both ground-based concepts. Initial independent LCC estimates for the two ground-based concepts are in the range of \$25 billion to \$35 billion over ten years if implemented at the 35 major U.S. airports that account for 75% of passenger air travel. No LCC estimate could be made for the L3/Avisys concept because of the uncertainty of a new doppler radar design for use in the U.S. airspace.

No follow-on activities are planned.

Air Cargo

Question: Please provide an update on the status of the Air Cargo Explosives Detection Pilot Program (ACEDPP). Specifically, how will are the fiscal year 2009 appropriations being spent on this effort, and what funding will be required in fiscal year 2010? Please address S&T's future plans for the Cincinnati/Northern Kentucky International (CVG), and San Francisco International (SFO) airports.

ANSWER: Congress tasked the S&T Directorate to conduct a pilot program in collaboration with the Transportation Security Agency (TSA) to test new concepts of operation for screening a significant percentage of air cargo above current levels. This pilot became the Air Cargo Explosives Detection Pilot Program (ACEDPP). The S&T Directorate worked with three airports - San Francisco, Cincinnati and Seattle - to test different approaches to screening air cargo for explosives and stowaways.

The S&T Directorate provided TSA with the pilot's preliminary information derived from analytical data, analysis and conclusions in order to help TSA determine how to use new screening technologies and how to properly implement new explosives detection technology within the cargo handling systems established at major U.S. airports. This information will also inform decisions as TSA works toward the mandate of screening 100 percent of air cargo by 2010. The S&T Directorate prepared a final report and it is in clearance review with the Office of Management and Budget. We anticipate delivery of the report to the Committee in late spring 2009.

Though funding for the Air Cargo Explosives Detection Pilot Program (ACEDPP) ended in FY 2007, the S&T Directorate has other efforts to improve the efficiency and effectiveness of screening air cargo.

- In coordination with the TSA Office of Security Technology (OST) and in conjunction with Transport Canada, the S&T Directorate is working to develop a large bore metal detector. This technology will identify the metallic content of Improvised Explosive Devices (IEDS) when concealed in cargo that is non-metallic (such as fresh flowers). In early FY 2009, a contract was awarded to CEIA, Inc. and prototype systems will be delivered for laboratory and field testing mid-year.
- The S&T Directorate supports the development and field evaluation of high volume trace sampling systems and mass spectrometry systems for screening of air cargo. These efforts focus on improving trace sample collection capabilities for break bulk and palletized cargo and providing higher resolution trace detection instruments for reduced false alarm rates. Analysis of the sources of alarms and background trace signatures are also underway to provide an understanding of sources of alarms.
- The S&T Directorate is developing new training aids for canines to enhance their explosive detection on the new and emerging home made explosive (HME) threat. In addition, canine detection performance testing took place in the air cargo environment in 2008. Since then, TSA changed the certification standards and the S&T Directorate plans another assessment in FY 2010.
- The S&T Directorate is assessing state-of-the art Commercial Off-the-Shelf (COTS) and near COTS equipment to screen break bulk, palletized, and containerized air cargo.

Funding for the Air Cargo Explosives Detection Pilot Program (ACEDPP) ended in FY 2007. The President's budget requests \$13.45 million for the S&T Directorate's Air Cargo Program, which would fund additional efforts to improve the efficiency and effectiveness of screening air cargo. The major project within this program is the Air Cargo Project, which identifies and develops the next generation of air cargo screening systems to mitigate the threat of explosives placed in air cargo containers. Activities include developing technologies to enable 100-percent air cargo screening (including break-bulk screening) with reduced operational costs and a low false alarm rate. In FY 2010, the project plans to deliver validated air cargo screener training based on procedures and equipment, as well as assess state-of-the-art commercial-off-the-shelf (COTS) and near COTS equipment to screen break-bulk, palletized, and containerized air cargo.

Additional requested funds support the High Throughput Air Cargo Screening Project, which will accelerate current efforts to develop effective and operationally acceptable technologies to detect explosive materials within a wide range of perishable and non-perishable commodities in break-bulk, palletized, and containerized configurations. This technology will protect commercial airliners, as well as the Nation's supply chain and economy. The technology will: reduce reliance on human screeners to detect artfully concealed threats; provide automated equipment to screen air cargo to increase throughput; reduce the government's oversight costs; reduce the costs of industry compliance to air-cargo screening regulations; and provide additional layers of security to enhance and verify air cargo supply-chain integrity. In FY 2010, with additional funding, the project plans to begin the development of human-operator inspection and resolution tools.

Upon completion of Air Cargo Explosives Detection Pilot Program (ACEDPP) operations at San Francisco International Airport (SFO), all screening and cargo handling equipment was removed from the United Cargo Warehouse. The cargo handling system at the shared Northwest/Continental Cargo warehouse was reconfigured as an air cargo testbed, to allow for easy installation of screening technologies for operational data collection. The S&T Directorate subsequently used the reconfigured system to collect 90 days of operational test and evaluation data in the air cargo environment for an advanced x-ray technology (L-3's MVT-HR). The S&T Directorate is coordinating with TSA to identify alternative technologies to evaluate in the Northwest/Continental cargo warehouse using the testbed infrastructure.

The S&T Directorate, in cooperation with the TSA Canine Program, will also conduct homemade explosive (HME) training aid field assessments at airports around the country to include SFO. Researchers will evaluate the training aids in various airport venues, terminal, cargo, vehicle and aircraft to compare the current HME

source which has complicated handling requirements to commercial and government source non-hazardous HME training aids.

There are no current plans to for further use of Cincinnati/Northern Kentucky International (CVG) airport at this time.

The Future Attribute Screening Technology (FAST)

The Future Attribute Screening Technology (FAST) project seeks to automate behavior detection and screening by examining human behavior and attributes. The Committee is aware of some concerns, however, as to whether this program conflicts with a necessary level of privacy of the subjects involved.

Question: Would DHS plan on recording and/or storing any of the data collected by any FAST system?

ANSWER: The Future Attribute Screening Technology (FAST) project is a research and development (R&D) activity intended to develop and test whether certain behavioral or physiological indicators are associated with an individual's intent to cause or do harm to others. The FAST project will only keep and analyze data collected during experiments to judge the effectiveness of the system. The collected data will not be used outside of the R&D process. The DHS Privacy Office is already working closely with the S&T Directorate, the DHS Office of Civil Rights and Civil Liberties, and Office of General Council to address privacy aspects FAST. The S&T Directorate has an approved Privacy Impact Assessment in place guiding work on the project. Should FAST be successful as a primary screening system with the potential to transition to a DHS operational component, that DHS component will define what data is retained in conjunction with all applicable laws and the DHS Privacy Office.

Question: What steps has DHS taken to address any concerns of privacy issues regarding a FAST system? Have you consulted with outside groups on the issue?

ANSWER: The S&T Directorate works directly with the DHS Privacy Office, DHS Office of Civil Rights and Civil Liberties (CRCL), and Office of General Council to address privacy concerns regarding Future Attribute Screening Technology (FAST). The S&T Directorate has an approved Privacy Impact Assessment in place guiding work on the project. FAST is also the first S&T Directorate project that will undergo a Civil Rights and Civil Liberties assessment to ensure any issues are identified and adjudicated early in the project. This is voluntary and the S&T Directorate is working in conjunction with the CRCL office to develop this new assessment process.

The S&T Directorate established a working group in April 2009 consisting of national experts from academia, privacy and civil rights/civil liberties office representatives, U.S. Secret Service, local law enforcement, the Director of the International Center for Criminal Justice at the Harvard Law School, and Transportation Security Administration officials. The group discusses both the theory and potential application of Future Attribute Screening Technology (FAST) technologies as well as provides insights to legal and privacy issues. Additionally, the S&T Directorate's Human Factors Division will subject the FAST project to an upcoming Community Acceptance of Technology Panel to further explore potential privacy concerns. Community Acceptance of Technology Panels bring together representatives of industry, public interest, and community-oriented organizations to better understand and integrate community perspectives and concerns in the development, deployment, and public acceptance of technology.

Container and Advanced Container Security Devices

Question: The Advanced Container Security Device (ACSD) project is designed to develop a highly reliable and secure means of detecting tampering or other intrusion into cargo containers and the CSD project is supposedly designed to help field low cost, reliable sensors for use on such containers until the ACSD comes along. What is the current status of CSD development and plans to deploy the CSD, now that major private sector suppliers seem to have backed away from financing this effort?

ANSWER: In FY 2008, two vendors, Science Applications International Corporation (SAIC) and Georgia Tech Research Institute (GTRI), delivered 20 Container Security Device (CSD) prototypes, which the S&T Directorate evaluated and tested. Both prototypes showed promising results during testing. However, some deficiencies were discovered in functional operations, as well as in environmental operations. The S&T Directorate is working with the two vendors to address the deficiencies and to couple the devices with a global communications system known as the Marine Asset Tag Tracking System (MATTS), which is a separate development effort. During late FY 2009-early FY 2010, each vendor will submit an improved CSD for further testing. Upon completion of successful testing, the S&T Directorate will transition the CSD test and evaluation assessments and finalized specifications to DHS Customs and Border Protection (CBP) and DHS Policy.

Supply Chain Architecture Project

Question: Please explain how S&T works with CBP and international standards organizations (if relevant) to develop an architecture. What are the key milestones for this project, and its status, in terms of key deliverables?

ANSWER: The Supply Chain Security Architecture incorporates input and feedback provided by DHS Customs and Border Protection for the movement of cargo through the supply chain and various touch points, as well as the flow of respective data. It also includes relevant international standards as inputs. For example, the World Customs Organization (WCO) "Framework of Standards to Secure and Facilitate Global Trade," adopted in 2005, was used as a core standard during the development of the architecture. This Framework establishes standards that provide for supply chain security and the facilitation of goods being traded internationally. At least 45 other international standards from the International Standards Organization (ISO) and other standards bodies were included in the development of the Supply Chain Security Architecture.

The first phase, Maritime Supply Chain Security Architecture was completed in FY 2008. The second phase, Air Cargo Supply Chain Security Architecture will be completed in FY 2009. The key deliverable is a report documenting the flow of air cargo, how air cargo data is transmitted, and the requirements by which emerging security technologies will pass data. A demonstration and test will be conducted in May of this year using early Secure Carton prototypes to represent one example for how cargo flows and data is passed through the architecture. Feedback resulting from the demonstration will be incorporated into the final architecture.

Hybrid Composite Container

The Hybrid Composite Container technology would allow sensors to be embedded into the actual material of a shipping container. Composite container technology could provide increased detection capabilities for cargo at our ports, but more importantly, before they even arrive.

Questions: What has S&T done to engage the shipping industry with regard to the cost-effectiveness of the hybrid composite container both in terms of setting a price-point for the final product, and conducting evaluations of the cost-savings of the container as it is developed?

ANSWER: The S&T Directorate has engaged with APL (a wholly owned subsidiary of Singapore-based Neptune Orient Lines, a global transportation and logistics company engaged in shipping and related

businesses) and Maersk (a global liner shipping company) to discuss various Returns On Investment (ROI) analysis from an industry perspective. Both companies have expressed a keen interest in the composite container. The S&T Directorate is currently analyzing development production costs, life cycle costs, weight, space and fuel reduction cost-savings. The S&T Directorate will have a final ROI analysis for the Hybrid Composite Container upon the completion of testing in FY 2011.

Question: One of the highest hurdles of implementing this technology is acceptance and involvement with the shipping industry. How will S&T show that this is a commercially viable and cost-effective container? Do you have any plans for pilots or partnerships to prove that it is viable?

ANSWER: The S&T Directorate is working directly with industry to conduct a cost analysis comparing the composite container to conventional steel containers. It is anticipated that the business case will show that the composite container will have a longer life span, weigh less, and will have the added security benefits to outweigh any additional near term costs. The goal of the program is to keep within \$400 to \$600 in additional cost-per-container for research and development purposes. The S&T Directorate anticipates that these costs will also be offset by mass production economies of scale.

The S&T Directorate is currently negotiating with the Singapore Ministry of Home Affairs (MHA) on a cost-sharing project agreement. The Department of State has agreed to allow the S&T Directorate to use the Department of State's supply chain routes for pilot testing the composite container. These pilots would be part of second-phase testing. The S&T Directorate will conduct at least 100 global supply chain movements with fully functional hybrid container units.

Technology Clearing House

Within the recently submitted fiscal year 2009 Innovation spend plan, S&T listed multiple projects that seem to be duplicative of current efforts that are being funded by private companies, in particular, the Scalable Common Operational Picture Experiment (SCOPE) project.

Question: What is the formal process that S&T uses to ensure that technologies you invest in are not duplicative of ongoing efforts in both the federal government and private sector?

ANSWER: The S&T Directorate has formal programs and processes that limit duplication of efforts, and leverage the valuable skills, experience and resources of other government agencies and the private sector. This includes participation in formal interagency groups that work to coordinate research and development across federal, state, local and tribal governments as well as the private sector. The following table provides examples of participation by S&T Directorate divisions and offices in formal interagency coordination groups.

S&T Participation by Division/Office	
Chemical/Biological Division	
Federal	
	BioShield Biological Working Group
	BioShield Enterprise Executive Committee
	BioShield Executive Governance Board
	Chemical Security Analysis Center Interagency Steering Committee
	Diagnostics Working Group
	Environmental Anthracis Validated Sampling Plan Technology Working Group
	Environmental Chemical Laboratory Response Technical Working Group
	First Responder-Anthrax Vaccine Policy Group
	Integrated Consortium of Laboratory Networks

Joint Biological Point Detection System Working Group
Joint Science and Technology Office Proposal Review Panel
Non-Proliferation Arms Control Technical Working Group
Response and Restoration Sub Policy Coordination Committee
Other
Laboratory Response Network-American Public Health Laboratories Advisory Group
Command, Control & Interoperability Division
Federal
Comprehensive National Cyber Initiative Senior Steering Group
Communications and Outreach Committee
Cyber Security and Information Assurance Working Group
Cyber Security Principal Investigators
Cyber Security Quarterly Agency Review
Domain Name System Security Working Group
Emergency Communications Preparedness Center Clearinghouse Working Group
Emergency Response Council
Health Information Technology Standards Panel Technical Committee
Information Security Research Council
Interagency Board for Equipment Standardization and Interoperability
Policy and Plans Steering Group
Project 25 Compliance Assessment Governing Board
Secure Protocols Working Group
Spectrum Working Group
Technical Support Working Group (project coordination)
Technology Policy Council
Wireless Working Group
State and Local
All Hazards Consortium
Practitioner Steering Group
Human Factors/Behavioral Sciences Division
NSTC Subcommittee on Biometrics and Identity Management (Co-chair)
NSTC Subcommittee on Human Factors (Co-chair)
DOD Human Factors Engineering Technical Advisory Group (Executive Board)
NSTC Subcommittee on Domestic Improvised Explosive Devices
Strategic Multilayer Assessment Group, Joint Integration and Preparation of the Operational Environment
Socio-cultural and Behavioral Science Research Group
Radicalization and Violent Extremism Working Group
Biometrics and Identity Management Working Group
Inter-Agency and First Responder Programs Division (IAD)
Federal
Army Counter-IED Task Force
Capabilities Development Working Group
Capabilities Development Working Group Senior Steering Committee
Transportation Sector R&D Working Group
State and Local
FEMA Region I Regional Advisory Committee
FEMA Region I Regional Interagency Steering Committee

FEMA Region II Managers' Meeting
FEMA Region II Regional Advisory Committee
FEMA Region II Regional Interagency Steering Committee
FEMA Region III Regional Advisory Committee
FEMA Region III Regional Interagency Steering Committee
FEMA Region IV Regional Interagency Steering Committee
FEMA Region V Regional Advisory Committee
FEMA Region V Regional Interagency Steering Committee
FEMA Region VI Regional Interagency Steering Committee
FEMA Region VII Radiological Assistance Meeting
FEMA Region VII Regional Interagency Steering Committee
New Jersey Center for Public Health Preparedness Advisory Council
New Jersey Regional Homeland Security Technology Committee
Urban Area Security Initiative Working Group (New York City metropolitan area)
Urban Area Security Initiative Working Group (Northern New Jersey)
Other
Adjutants General Association of the United States Homeland Security Committee
National Guard Association

In addition, the S&T Directorate facilitates coordination with customers and technology providers across its divisions and offices. For example:

- The S&T Directorate's Transition Office coordinates with all S&T divisions to minimize duplication and ensure that the S&T Directorate is leveraging technology available in both the government sector and private sector. The Transition Office facilitates 13 customer-led Capstone Integrated Product Teams (IPTs) and has visibility into customer's capability gaps and technology needs. Two formal Capstone IPT reviews are conducted per year to provide visibility into the S&T Directorate's cross-functional programs and facilitate discussion on available DHS-external technologies/capabilities.
- The S&T Directorate has an Interagency and First Responder Program Division (IAD) to leverage other government technology efforts. IAD coordinates closely with the Transition Office and participates in the Capstone IPT reviews. With knowledge of customer technology needs identified through the Capstone IPT process, IAD coordinates with other government entities to explore and/or leverage alternative technologies available through other government entities.
- The S&T Directorate's Commercialization Office is responsible for the identification, evaluation and rapid commercialization of technology to meet the operational requirements of our customers. Since the Commercialization Office is part of the Transition effort, they have first hand knowledge of customer technology needs identified through the Capstone IPT process and the supporting S&T Directorate efforts. The Commercialization Office works closely with S&T divisions to ensure there is no duplication of effort and that S&T Directorate efforts are focused in only in areas where no rapid commercialization solution exists.

The 1401 Technology Transfer Program, which is also housed in the Transition Office, identifies and transfers Department of Defense (DoD) technology, items and equipment that can be used by the federal, state, tribal and local first responder community to support their role to protect and secure the homeland. The purpose of this program is to strengthen coordination and collaboration across DoD, DHS and the Department of Justice (DOJ) to improve the efficiency, effectiveness and consistency of the transfer of high-priority technology, items and equipment.

Question: Does S&T take the same care to justify continuing to invest in ongoing projects as it takes to decide whether or not to initiate a project? Please explain the formal process, if any, for vetting previously initiated and ongoing projects at S&T with work being done in the private sector and elsewhere in the federal government.

ANSWER: Yes, the S&T Directorate takes the same care to justify continuing to invest in projects as it does when determining whether to initiate a project. The S&T Directorate uses established processes and thorough internal and external reviews to justify the continuation of investment in ongoing projects as well as to initiate new projects.

For Transition efforts, S&T Directorate leadership conducts formal semi-annual reviews of current programs to ensure that technical development is progressing along previously agreed-upon milestones. S&T Directorate leadership also conducts regular reviews of new programs and continually reviews on-going programs in order to make informed decisions regarding continued funding.

For Research efforts, the S&T Directorate uses several approaches to evaluate its ongoing projects, not only to determine the appropriateness of continuing the project, but also to continue to look for synergies with other projects and to consider modifying elements of the effort if appropriate. Project and program managers evaluate their projects continuously, both in the review of the projects themselves (e.g., during reviews of monthly reports) and during interfaces with performers and with others in the research community. For evaluations by someone not directly involved in the day-to-day management of the projects, Division heads conduct informal reviews of each program and project throughout the year. Formal program reviews with portfolio directors and other senior members of the S&T Directorate's staff are also held semi-annually.

For Innovation efforts, the Homeland Security Advanced Research Projects Agency (HSARPA) holds comprehensive programmatic and technical project reviews twice a year and regular project status reviews to assess progress to established goals for each project in its portfolio. During a project review, program managers are required to relate all specific project elements to interim and final project goals in terms of cost, risk, and schedule. Great care is taken to assess and prioritize the HSARPA program based on technical merit, mission relevance, and department priorities. Some projects continue as others are reduced in budget and scope or terminated.

The S&T Directorate has several programs and processes in place to vet previously initiated and ongoing projects.

For Transition efforts, the S&T Directorate performs comprehensive market analysis and technology scans in addition to leveraging, whenever possible, the valuable skills, experience and resources of the private sector. The S&T Commercialization Office, which resides within the Transition Office, has improved the S&T Directorate's relationship with the private sector through its various outreach initiatives and the creation of a detailed repository of technologies, capabilities and products available in the private sector that have the potential to address DHS high-priority technology needs. The Commercialization Office works closely with S&T divisions and leverages its knowledge of the DHS functional, department level requirements and technology needs when conducting its public relations and outreach activities.

The 1401 Technology Transfer Program, which is also housed in the Transition Office, identifies and transfers Department of Defense (DOD) technology, items and equipment that can be used by the federal, state, tribal and local first responder community to support their role to protect and secure the homeland.

The Long Range Broad Agency Announcement (BAA) identifies strategic topics of interest to DHS's mission and is the principal vehicle to outreach for white papers and full proposals in the private sector and university community. Submissions are assessed based on the overall best value to the government and identify areas where expertise and technologies exist in the private sector.

For Research efforts, the S&T Directorate maintains close liaison throughout the research community to vet projects both before they are initiated and during their execution. The S&T Directorate has a multi-faceted approach to ensure S&T stays informed of the state of the research being conducted by federal agencies, labs, universities, and industry and then uses that knowledge during periodic program reviews to ensure appropriate integration, cost sharing, and potential combination or canceling of projects.

The S&T Directorate coordinates closely with the White House's Office of Science and Technology Policy (OSTP) through the National Science and Technology Council (NSTC), with members on 30 of its committees, subcommittees and working groups. This provides valuable interaction and visibility into the needs and activities of other federal agencies. For example, S&T's Program Executive Officer for Counter Improvised Explosive Devices [PEO (C-IED)] is the co-chair of the NSTC Domestic Improvised Explosive Devices (D-IED) subcommittee, which includes representatives from seven cabinet-level departments with interest in IEDs and serves to coordinate research efforts in that area. In December 2008 the D-IED subcommittee published a joint document entitled *Research Challenges in Combating Terrorist Use of Explosives in the United States*.

Through its Office of National Laboratories, the S&T Directorate maintains a special relationship with the Department of Energy (DOE) and National Nuclear Security Administration (NNSA) laboratories and works very closely with other federal laboratories (such as those of DOD, NASA and NOAA). These labs are well known for knowing the state of the art of emerging science – and often for conducting the leading-edge science themselves. Regularly scheduled meetings are held with the laboratories at multiple levels, from laboratory directors to principal investigators, to ensure free flow of information and support effective integration of efforts. The DOE and NNSA labs have provided the S&T Directorate access to databases of their research efforts and the S&T Directorate is working with other federal agencies to improve our sharing of access to information.

The Office of University Programs maintains 12 university Centers of Excellence (COEs). These universities stay up to date in their areas of expertise and, through routine interactions with the S&T Directorate, allow us to benefit from that knowledge.

The S&T Directorate also reaches out to research communities through conferences and symposia. This includes publishing documents that show our interests, including our *High-Priority Technology Needs* and our *Basic Research Focus Areas*. Our very active SBIR program allows us to engage with small businesses, often the place where highly innovative work is done. To catch items that we might otherwise miss, the S&T Directorate also has a small contract with a company to do technology scouting.

For Innovation efforts, each HSARPA project is managed by a program manager that works with the scientific community related to the technical and operational approaches of their project(s). All actively contribute to the scientific community by either authoring publications, chairing panels, or attending conferences and symposia that expose them to a broad base of cutting edge science and technology in industry, academia, and government. In addition, HSARPA program managers interact with their basic research and transition division counterparts, sharing knowledge and observations about related activities in the private sector and government. During project status reviews, the program director and senior program advisors advise program managers on existing technologies, new approaches or developments in the field and strategies to consider when executing their projects.

HSARPA also subscribes to an international technology scouting service, targeting the most recent technical approaches and applications to our most difficult challenges. HSARPA uses public announcements such as Requests For Information (RFIs) and Broad Area Announcements (BAAs) as a means to learn about and consider technical approaches and solutions from private industry, academia and government that relate to a specific research challenge. These vehicles are normally used to initiate new programs, but are more frequently used to consider new or more recent discoveries than when the program first started.

Inclusion of Stakeholders

Question: What steps has S&T taken to promote its desire to receive input from private technology developers? The Committee notes the establishment of initiatives such as the Small Business Innovation Research (SBIR) program, but how are these efforts being promoted so that more users are aware of them?

ANSWER: The S&T Directorate has taken a number of steps to reach out to and receive input from the private sector. For example:

To further develop contact with the private sector, the S&T Commercialization Office (established in October 2008) has published four books, including *Requirements Development Guide*, *Developing Operational Requirements (Versions I and II)* and *Harnessing the Valuable Experience and Resources of the Private Sector for the Public Good*, and launched the SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) Program. SECURE is an innovative public-private partnership, which has already yielded the development of two fully deployable products in less than five months, funded by the private sector. To date, the Commercialization Office through its private sector outreach efforts (using its "Full Response Package" process) has met with or provided briefs to more than 25,000 business executives and maintains information on more than 300 firms and more than 2,000 technologies/capabilities/products that are closely aligned to S&T Directorate-customer high-priority technology needs. The Commercialization Office's private sector outreach efforts extend to regular meetings with small, medium and large businesses. A concerted effort to engage minority, disadvantaged and HUB Zone groups is ongoing and documented in our *S&T Private Sector Outreach Statistics Report*, which is updated regularly.

The DHS Small Business Innovation Research (SBIR) Program uses its website to engage the private sector to submit topic recommendations (<https://www.sbir.dhs.gov/uploadrecommendation.asp>). The community is invited to submit a one-page abstract providing the following information: (1) name, organization and contact information; (2) what special contributions to an area might be; and (3) why S&T SBIR should consider this area as a potential topic area. Topic recommendations submitted from the community are shared with S&T divisions at the time that the internal call for topics is made.

The S&T Directorate also uses the Long Range Broad Agency Announcement (BAA) 09-05 to identify strategic topics of interest to our mission.

The S&T Directorate participates in three Homeland Security S&T Stakeholders Conferences each year, with one conference being held in Washington, D.C., one in a Western state, and one at a location convenient to an international audience. These conferences focus on the future of the S&T Directorate while highlighting the innovative research efforts that DHS has underway in the U.S. and around the world to make the nation safer. Attendees from the private sector, academia, and all levels of government learn about opportunities for partnership with S&T for science and technology research. All of the senior leadership of the S&T Directorate speak during these events. Key program managers and other staff of the S&T Directorate are broadly represented throughout the S&T Stakeholders Conference East, and attendees have extensive opportunities for formal and informal interaction with Directors, Division Heads, and Program Managers from the S&T Directorate. A critical component of the conference is the time available for intensive discussion between attendees and S&T Directorate personnel at all levels, to share ideas and information, including opportunities throughout the conference to congregate in small groups for focused conversations on specific issues. The conferences feature speakers from the operating components of DHS, First Responder organizations, Capitol Hill professional staff, and representatives of organizations partnering with the S&T Directorate. There is a significant international component to all the S&T Stakeholders Conferences.

The Small Business Innovation Research Program (SBIR) Director actively participates in national, regional, state, and local SBIR conferences and workshops throughout the country in an effort to promote the DHS SBIR

Program. For example: (1) an SBIR Tutorial, highlighting the features of the DHS SBIR Program, is presented at each of the biannual S&T Stakeholders Conferences; (2) the DHS SBIR Program Director participates in the monthly DHS Small Business Vendor Outreach Sessions that provide the small business community with an opportunity to discuss their capabilities and learn of potential procurement opportunities; and (3) the DHS SBIR Program Director participates in each of the National SBIR Conferences (Connecticut in the Fall of 2008; Nevada in the Fall of 2009).

In addition, the SBIR Program Office maintains a website (<http://www.sbir.dhs.gov>) which provides detailed information about the DHS SBIR Program. The DHS SBIR Program website is also linked on many federal agency SBIR websites, as well as many commercial SBIR vendor sites. Further, the S&T Directorate SBIR Program Office maintains an electronic mailing list (currently more than 1,400 addresses subscribed), which is exercised periodically and when a solicitation is released (two times per year).

Question: What efforts has S&T made to include mass transit systems and communities to evaluate what types of technologies and capabilities are needed, before approaching these sites with demonstration and pilot opportunities?

ANSWER: Through the DHS Office of Infrastructure Protection's (IP) National Infrastructure Protection Plan (NIPP) framework, the S&T Directorate engages with the Sector Specific Agencies (SSA), Government Coordinating Councils (GCC) and Sector Coordinating Councils (SCC) to identify capability gaps and research and development requirements. Through the NIPP process, each sector generates Sector Annual Reports (SAR), in which they list and prioritize these capability gaps. The S&T Directorate considers customer capability gaps through the Capstone Integrated Product Team (IPT) process. The IPT process is the centerpiece of the S&T Directorate's product transition portfolio, which functions in mission-critical areas to identify customers' needs and enable and transition near-term capabilities for addressing them. These Capstone IPTs engage DHS customers, acquisition partners, S&T Directorate technical division heads, and end users as appropriate in our product research, development, transition and acquisition activities. The S&T Directorate draws on the knowledge and expertise of the members of the IPTs throughout the technology development process, from project proposal through transition of the technology solution to the customer. In this manner, mass transit systems, communities, localities and owner/operators are involved in technology identification, development and evaluation through the NIPP and Capstone IPT processes, in particular the Transportation IPT and the Infrastructure Protection IPT.

The S&T Directorate works closely with the Transportation Security Administration (TSA), the Sector Specific Agency for the Transportation Sector, to address capability gaps specific to mass transit systems. TSA reaches out to stakeholders nationwide and gathers technology capability gaps from the mass transit and passenger rail community. TSA solicits formal feedback from the Mass Transit Sector Coordinating Council and the Transit Security and Policing Peer Advisory Group, as well as through workshops with transit agencies related to specific categories of technology. Safety and Security Roundtables and Transit Security Grant Program outreach events have allowed TSA to compile additional input from transit agencies on technology development needs. TSA compiles capability gaps and submits them to the S&T Directorate through the IPT process. The S&T Directorate ultimately leverages all of these interactions to develop an understanding of key requirements of mass transit stakeholders. Additionally, the S&T Directorate works through TSA to directly engage stakeholders on a project-specific basis to refine capability gaps, conduct project planning, and measure the progress of ongoing efforts to ensure that research, development, testing and evaluation efforts undertaken by the S&T Directorate address the identified stakeholder requirements.

Within the Infrastructure Protection IPT, several efforts are being conducted in close coordination with mass transit stakeholders:

- **Bay Area Rapid Transit (BART) mitigation strategy:** In partnership with BART and Lawrence Livermore National Laboratory (LLNL), conducting small-scale blast experiments and computational analysis to design a mitigation strategy to protect a key vulnerability identified in the BART system.
- **Brick Tunnel Analysis:** In partnership with LLNL and U.S. Army Corp of Engineers – Engineering Research and Development Center (ERDC), conducting blast testing and computational analysis to characterize the behavior of brick constructed tunnels under explosive loads for a key mass transit stakeholder.
- **Blast Analysis Tools:** In partnership with LLNL, ERDC and the Technical Support Working Group (TSWG), developing fast-running numerical models to enable infrastructure owners and operators to estimate the effects of explosive events on critical assets and assess the effectiveness of mitigation measures. Current work is focused on tunnels, bridges, dams, and complex urban environments. The tunnel analysis tool will include data from in-depth analyses of tunnel structural vulnerability to explosives devices conducted in close partnership with seven U.S. mass transit agencies.

The mass transit community is also heavily involved in a project within the S&T Innovation Portfolio:

- **Resilient Tunnel Project:** The S&T Directorate is developing inflatable tunnel plugs with the potential to protect critical transportation tunnels from fire, flooding, and other hazards. Early on in this project, the S&T Directorate engaged TSA, Washington Metro Area Transit Authority (WMATA), and the Port Authority of New York and New Jersey (PANYNJ) to identify the performance and operational requirements that have guided project development. These organizations remain heavily engaged in the day-to-day project development and plan to provide locations for prototype deployment. As the project matures, the S&T Directorate is working with TSA to engage more mass transit owners and operators in order to develop strategies to employ this technology across the sector.

Question: Has S&T developed any technology investments or projects that were initially proposed by a small business owner or private developer? Please give examples with a history of funding of these projects.

ANSWER: Yes. To develop technology solutions for DHS capability gaps, the S&T Directorate continues to make funding investments in projects proposed by small businesses and private developers. One example is with Innovative Wireless Technologies (IWT) a small business funded by the S&T Directorate to develop an Unattended Ground Sensor (UGS) distributed mesh network ad hoc capability. IWT performed a successful engineering test this year and upgrades are in place for operational testing later this year. The SBInet Program Office and Boeing are both very interested in going forward with IWT's UGS' if the operational testing is successful. A second S&T Directorate funded small business is Global Technical Systems. This company developed the Fusion Command™ technology, a sensor integration, command and control, and tactical scene awareness application designed to automate the detection and tracking of targets of interest. It is currently deployed as part of a test bed at a U.S. Border Patrol station supporting the S&T Directorate technology development and providing an operational capability to station field agents. It was also deployed as part of a three month demonstration investigating maritime scene awareness on the Great Lakes.

Another example where S&T Directorate is making an investment in an effort proposed by a small business is with Boston MicroSystems. This company is designing and testing a silicon carbide MEMS array for proof of concept explosives detection. A fourth S&T Directorate funded small business is Ironkey which developed the world's most secure USB flash drive. The Ironkey is now in Phase II of the S&T Directorate pilot with more than 500 users. Other representative small businesses funded by the S&T Directorate include: GammaTech, *Model Checking Software Binaries*; Komoku, *Copilot – A High Assurance and Independent Security Auditor*;

Adventium, Embedded Firewall for Robust Protection of Mission Critical Operations; Secure64, Automating the Chain of Trust – Secure Interzone Key Management for Large Scale DNSSEC Deployments (SCOTTY); PCH, BGP Routing Integrity Checker and Prefix-List Filter Generation Tool; PCH, INOC-DBA, VoIP Network Security; Secure Decision, Visualization Toolkit for NetFlow Analytics; Digital Bond, Passive Security Log Generation for Control Systems; and InGuardians, Virtual Machine Detection and Escape.

The Long Range Broad Agency Announcement (BAA) is another helpful tool that identifies strategic topics of interest to DHS's mission and is the principal vehicle to outreach for white papers and full proposals in the private sector and university community. Submissions are assessed based on the overall best value to the government.

In addition to the projects and methods above that the S&T Directorate uses to make technology investments in projects that were initially proposed by a small business owner or private developer, the S&T Directorate effectively uses the SBIR Program to not only conduct outreach to the small business community, but also to use innovation ideas proposed by small businesses for technology solutions/products through all phases of the Program (Phase I, Phase II, and Phase III). One example is the Readiness Optimization SBIR Phase III project by Human Bionics LLC. (*SBIR Phase III projects are funded with non-SBIR funds.*) It uses a form of neurotraining known as "brain music" to determine if it will improve the operational readiness of our Nation's front lines, including Federal Air Marshals and First Responders.

Other SBIR Phase III examples include: a project by Physical Optics Corporation to develop a low-power, handheld biodetection device; a project by Vista Research to develop innovative radar algorithms to mitigate clutter effects and lower the false alarm rate; a project by Toyon Research Corporation to develop algorithms for cameras that remove camera shake and jitter effects and automatically detect and track targets; a project by Intelligent Optical Systems, Inc. to develop the Light Emitting Diode Incapacitator (LEDI) technology as a less-lethal means to compel compliance on aggressive, violent, self-destructive, and/or dangerous individuals by temporarily obstructing vision and potentially causing disorientation; a project by Engineering Science Analysis Corporation to develop the Safe Quick Undercarriage Immobilization Device (SQUID) technology as a less-lethal vehicle stopping method to mechanically stop an offending vehicle without causing serious injury to the vehicle occupants, bystanders, law enforcement officers, and/or property; and a project by iControl to complete development of a Marine Asset Tag Tracking System (MATTS) and conduct a series of development tests.

With SBIR Phase I and Phase II funding, the S&T Directorate has invested in several small businesses to develop new technology to meet DHS needs. Examples include: two Phase II projects piloting technologies with the S&T Directorate CIO – HB Gary's Enterprise Botnet Extraction and Response project and Milcord's Botnet Analytics Appliance (BNA) project; three Phase II projects developing technologies for a low cost underwater threat detection system: Applied Physical Science Corporation, BioSonics Inc., and FarSounder Inc; two Phase II projects developing technologies for a distributed buoy vessel detection system: Advanced Acoustic Concepts Inc., and LewTech Company Inc.; and one Phase II project by Lynntech to develop a technology to detect human targets in open water. The S&T Directorate also has SBIR projects that use existing technology in new applications. These projects are being leveraged in larger S&T Directorate programs. Examples include an SBIR Phase I effort with Bio-Behavior Analysis Inc. and a Phase II effort with Veridical, both using commercial technology in new applications to detect intent. Work from both of these efforts will be leveraged and will feed into the S&T Directorate's Office of Innovation's Future Attribute Screening Technology (FAST) Program.

The projects described above are representative of the projects that the S&T Directorate funds to leverage the technical contribution from the small business and private developer community. The S&T Directorate funds projects from this community using both SBIR and non-SBIR funds. Funding for these projects is shown in the tables below:

Representative Small Business and Private Developer Projects Funded by the Science and Technology Directorate		
S&T Division Managing the Project	Company	Amount of S&T Funds
Borders and Maritime Security Division	Innovative Wireless Technologies <i>Forest, VA</i>	\$ 909,000
	Global Technical Systems <i>Virginia Beach, VA</i>	\$ 796,000
Explosives Division	Boston MicroSystems <i>Woburn, MA</i>	\$ 825,000
Command, Control and Interoperability Division (Cyber Security Thrust Area)	Ironkey <i>Los Altos, CA</i>	\$1,335,096
	GrammaTech <i>Ithaca, NY</i>	\$ 538,111
	Komoku <i>Columbia, MD</i>	\$1,286,629
	Adventium <i>Minneapolis, MN</i>	\$ 870,013
	Secure64 <i>Greenwood Village, CO</i>	\$1,000,804
	PCH <i>San Francisco, CA</i>	\$ 449,967
	PCH <i>San Francisco, CA</i>	\$ 599,983
	Secure Decisions <i>Northport, NY</i>	\$ 617,092
	Digital Bond <i>Sunrise, FL</i>	\$ 475,000
	InGuardians <i>Washington, DC</i>	\$1,159,419
	Human Factors Behavioral Sciences Division	Human Biomics LLC <i>Purcellville, VA</i>
Chemical and Biological Division	Physical Optics Corporation <i>Torrance, CA</i>	\$ 99,993 SBIR Phase I \$669,000 SBIR Phase III
Borders and Maritime Security Division	Vista Research Corporation <i>Sunnyvale, CA</i>	\$ 99,960 SBIR Phase I \$999,996 SBIR Phase II \$3M from SBInet Program Office for SBIR Phase III
	Toyon Research Corporation <i>Goleta, CA</i>	\$100,000 SBIR Phase I \$750,000 SBIR Phase II
	Intelligent Optical Systems <i>Torrance, CA</i>	\$ 99,999 SBIR Phase I \$770,000 SBIR Phase II \$395,000 SBIR Phase III
	Engineering Science Analysis Corporation <i>Tempe, AZ</i>	\$100,000 SBIR Phase I \$750,000 SBIR Phase II \$750,000 SBIR Phase III
	iControl <i>Palo Alto, CA</i>	\$ 96,945 SBIR Phase I \$877,020 SBIR Phase II \$2.3M SBIR Phase III
	Command, Control and Interoperability Division (Cyber Security Thrust Area)	HBGary, Inc. <i>Bethesda, MD</i>
Mifcord LLC		\$100,000 SBIR Phase I

Representative Small Business and Private Developer Projects Funded by the Science and Technology Directorate		
S&T Division Managing the Project	Company	Amount of S&T Funds
	Waltham, MA	\$750,000 SBIR Phase II \$ 50,000 additional S&T funds on the SBIR Phase II (<i>in process</i>)
Borders and Maritime Security Division	Applied Physical Sciences Corporation Groton, CT	\$ 74,274 SBIR Phase I \$749,998 SBIR Phase II
	BioSonics, Inc. Seattle, WA	\$100,000 SBIR Phase I \$750,000 SBIR Phase II
	FarSounder, Inc. Warwick, RI	\$ 99,940 SBIR Phase I \$750,000 SBIR Phase II
	Advanced Acoustic Concepts Hauppauge, NY	\$ 99,989 SBIR Phase I \$749,996 SBIR Phase II
	LewTech Company, Inc. Fort Wayne, IN	\$ 99,905 SBIR Phase I \$749,763 SBIR Phase II
	Lynntech, Inc. College Station, TX	\$100,000 SBIR Phase I \$ TBD SBIR Phase II in negotiation
	Bio-Behavior Analysis, Inc.(St. Louis, MO)	\$ 99,987 SBIR Phase I
Human Factors Behavioral Sciences Division	Veridical Bozeman, MT	\$ 99,981 SBIR Phase I \$ TBD SBIR Phase II in negotiation

Question: Please provide for the Committee a list of the funds spent on promoting awareness and communication with the private sector over the last three fiscal years (FY 06 – FY 08), and list what specifics efforts have been taken to achieve better visibility.

ANSWER: Outreach to potential performers, including the private sector, is an integral part of how the Science and Technology Directorate (S&T) does business. The funds are spread throughout the Directorate's work.

The S&T's Corporate Communications Division (CCD) conducts outreach through S&T Stakeholder's Conferences, which invite industry to come learn about the Directorate, its research activities, and how we conduct business. The CCD also produces weekly stories on S&T accomplishments to an opt-in email newsletter list. The newsletter currently has 14,000 subscribers.

The S&T's operating divisions perform outreach to the private sector throughout the year. The Chemical and Biological Division held a conference specific to chemical/biological risk analysis. The Command, Control, and Interoperability Division hosted an event targeting critical incidence response. University Programs held a conference of principals and working researchers in the Center of Excellence enterprise. All outreach events inform the private sector and other research communities about S&T's research mission and priorities.

The S&T produces documents, distributes them to the public at conferences, and makes them available on our website. These documents communicate the research areas of interest to the S&T and how to do business with the Directorate and DHS components. These documents include:

- *High Priority Technology Needs (May 2007 and June 2008);*
- *Requirements Development Guide;*
- *Developing Operational Requirements (Versions I and II);*
- *Harnessing the Valuable Experience and Resources of the Private Sector for the Public Good; and*
- *Five Year Research and Development Plan Fiscal Years 2008-2013.*

The S&T's Commercialization Office's private sector outreach efforts extend to regular meetings with small, medium and large businesses, including a concerted effort to engage minority, disadvantaged and HUBZone groups. Our regularly updated *S&T Private Sector Outreach Statistics Report* provides more information. Additionally, the Commercialization Office published on its websites seven DHS-generated, DHS-vetted detailed operational requirements documents (ORDs). The ORD's sparked significant response from interested private sector firms seeking additional information on possible partnership opportunities with DHS. The Commercialization Office also launched the SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) Program. SECURE is an innovative public-private partnership, which has already yielded the development of two fully deployable products in less than five months that were funded through the private sector. To date, the Commercialization Office, through its private sector outreach efforts (using its "Full Response Package" process), met with or provided briefs to more than 25,000 business executives. The Office also maintains information on more than 300 firms and more than 2,000 technologies/capabilities/products that align to S&T Directorate-customer high-priority technology needs.

Broad Agency Announcements (BAA) and the Small Business Innovation Research (SBIR) Program achieve further directed outreach for S&T. The widely distributed BAAs that accompany a request for white papers and proposals include information about the areas of research the Department is interested in pursuing. There are national, regional, state and local SBIR conferences and workshops throughout the country that S&T Directorate representatives participate in to promote the DHS SBIR and BAA announcements. These events often have accompanying kickoff conferences to better engage the private sector and other research communities. The Office of SAFETY Act Implementation also conducts a wide range of workshops, presentations, and events to publicize the SAFETY Act to organizations working on technology with counter-terrorism applicability.

Outreach also occurs every time an S&T official speaks or presents at a conference or participates in a technology workshop. It occurs when public meetings are held to discuss major construction projects like NBACC and NBAF. Outreach to the private sector is an integral part of the every day function of a large part of S&T and is funded from sources across both the Management and Administration and the Research, Development, Acquisition, and Operations appropriations.

In support of the *Homeland Security Act of 2002* (P.L. 107-296, Sections 302, 305, 307, 308, and 313) the Corporate Communications Division (CCD) of the Science and Technology Directorate conducts the bulk of the Directorate's outreach activities. Recent examples include a stakeholders conference focused on partnerships designed to solicit ideas and concepts from the private sector ("Partnering for a Safer Nation"), a stakeholders conference focused on the needs of first responders ("First Responder Frontiers"), and a stakeholder's conference for the PacAsia region ("Scientific Research for Homeland Security") to engage our international partners. Additional conferences included an event specific to chemical/biological risk analysis (Chemical and Biological Division), an event targeting critical incidence response (Command, Control, and Interoperability Division), and a conference of principals and working researchers in the center of excellence enterprise (University Programs).

CCD provides weekly stories on the S&T Directorate's accomplishments to an opt-in email newsletter list currently with 14,000 subscribers.

The Directorate exhibited in 60 exhibits in 18 states with at least one event in each of the 10 FEMA regions. It prepared 159 distinct and specific briefings in support of a very broad range of speaking opportunities.

The directorate entered into a formal cooperative agreement for the production of *Hi-Tech War on Terror* (DVD copy may be attached) which achieved significantly higher than normal ratings on the National Geographic Channel.

In support of the SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) Program, CCD and the Commercialization Office have published four books that facilitate the development of a requirements development capability, including *Requirements Development Guide*, *Developing Operational Requirements (Versions I and II)* and *Harnessing the Valuable Experience and Resources of the Private Sector for the Public Good*. The Commercialization Office has met with or provided briefs to over 25,500 persons and maintains information on over 300 firms and over 2,000 technologies, capabilities, products closely aligned to the high priority technology needs of S&T Directorate. The Commercialization Office's private sector outreach efforts extend to regular meetings with small, medium and large businesses, including a concerted effort to engage minority, disadvantaged and HUBZone groups. The Commercialization Office has also published on its websites seven DHS-generated, DHS-vetted detailed operational requirements documents (ORDs) with significant response from interested private sector firms seeking additional information on possible partnership opportunities with DHS.

The Office of SAFETY Act Implementation provides a wide range of workshops and presentations to groups and events to publicize the SAFETY Act to organizations working on technology with counter-terrorism applicability.

Border Inspection Technology Projects

Question: Please describe any tangible benefits that the Hidden Compartment Inspection Device and Under Vehicle Inspection projects have produced for CBP and Border Patrol inspection, or will produce over the next fiscal year. Please also describe how the results of such projects transition to operational form.

ANSWER: The Hidden Compartment Inspection Device will enable law enforcement agents to non-intrusively detect, from greater stand-off ranges, anomalies and/or voids hidden behind walls and other barriers. This technology will allow officers to have a greater situational awareness regarding unexplained entities, anomalies, and/or voids thus supporting intelligence and interdiction missions. In FY 2008, the S&T Directorate developed a prototype device through a Phase II S&T Small Business Innovation Research (SBIR) project. The S&T Directorate plans to further assess and develop the prototype in FY 2009, demonstrate it in a lab environment in FY 2010, demonstrate it in an operational environment in FY 2011, and transition it to our customer in FY 2011.

The S&T Directorate formulates and establishes projects based on relevant science and technology capability gaps identified by our operational component customers (i.e. CBP, ICE, TSA etc) during S&T's Integrated Product Team (IPT) process. As part of establishing a project to develop a technology to address those capability gaps, the S&T Directorate and the customer component(s) sign a Technology Transition Agreement (TTA) to establish a commitment to support the S&T Directorate's investment through the project's completion. This process assists component customers in establishing their out-year funding requirements because once a successful project is transitioned, it is up to the operational components to acquire and sustain the technology through its life cycle.

International Agreements

Question: Please detail for the Committee the anticipated projects that will take place in partnership with the German Federal Ministry for Education and Research (BMBF).

ANSWER: Based on previous discussions with colleagues from the German Federal Ministry for Education and Research (BMBF), the International Cooperation Programs Office (IND) anticipates initial cooperation in the following areas: visual analytics/pattern recognition, cargo security,

chemical/biological/radiological/nuclear detection, explosives detection, and human factors issues such as radicalization.

The first cooperative activity will be in the area of visual analytics. The new research area of Visual Analytics is the result of the rapid proliferation of increasingly complex data. One central challenge is to filter the most important information from these large amounts of data. Only a combination of technologies in the fields of data analysis and visualization can enable effective access to and interpretation of otherwise unmanageable quantities of data. The cooperative Visual Analytics (pattern recognition) project is expected to have applications in the field of infrastructure networks (i.e., the early recognition of incidents, real-time reaction in the event of an incident). The DHS customers for this activity are: the Federal Emergency Management Agency, Intelligence and Analysis Directorate, U.S. Secret Service, and Immigration and Customs Enforcement.

The second cooperative activity will be a cargo security workshop to be held in Bremen, Germany in September. One objective is to consider innovative logistics technologies for tracking and tracing cargo. This event is in the early planning stages.

In addition, IND is working with our BMBF counterparts to schedule a bilateral session for this summer/early fall when the counterparts for chemical, biological, radiological and nuclear (CBRN) detection, explosives detection, and human factors can meet, discuss ongoing programs, priorities and requirements, and identify cooperative activities in these areas of common interest.

Basic Research

Question: Universities in the S&T Centers of Excellence program provide a wide assortment of basic research that applies to agencies across the Department. What specific coordination efforts are there between those components and the research institutions to provide a focus for the research that would be most applicable?

ANSWER: The S&T Directorate's University Program (UP) has a well-established process to link the work of the Centers of Excellence (COEs) to the DHS components. Each COE aligns with an S&T Directorate Division. Divisions align with customers and stakeholders through the integrated product team (IPT) process. Through this connection, the S&T Directorate communicates customer needs to the COEs and COE capabilities to customers. This alignment allows coordination between the COEs, S&T Divisions, and S&T Directorate customers, which include DHS components.

For example, the S&T Directorate's Chemical and Biological Division, the DHS Office of Health Affairs and its partner agencies are working intensely to bring a range of COE capabilities from at least five COEs to bear on H1N1 virus questions, including modeling the epidemiology of the disease spread; evaluating the economic consequences of the disease and potential responses; and providing tools to manage, analyze and visualize massive amounts of data. This rapid response effort could only be productive where all of the parties know what COE capabilities are available and all work together to get appropriate applications and analyses into the hands of decision-makers quickly.

Additionally, UP invites S&T Directorate customers and stakeholders to its annual University Network Summit.

Question: Specifically, what basic research efforts that S&T is involved in can be applied to the work that FEMA does regarding disaster response?

ANSWER: The Center for Preparedness and Critical Event Response (PACER) and the Natural Disasters, Coastal Infrastructure and Emergency Management (NDCIEM) Center of Excellence (COE) are specifically

aligned with the S&T Directorate's Infrastructure Geophysical Division (IGD) to address FEMA and related agencies' research needs. The COE for Risk and Economic Analysis of Terrorism Events (CREATE) and Center for the Study of Terrorism and Responses to Terrorism (START) also conduct research of interest to FEMA on disaster response, specifically community resilience and risk assessment.

The primary areas of COE research that benefit FEMA include:

PACER (John Hopkins University): PACER's mission is to improve the Nation's preparedness and the ability to respond in the event of a high consequence natural or manmade disaster and to alleviate the event's effects by developing and disseminating best scientific practices. Examples of specific projects include:

- Conduct research for FEMA to identify and integrate promising modeling and simulation tools into FEMA National Preparedness Directorate's (National Exercise Simulation Center) NESC. This project will also provide a modeling and simulation catalogue that facilitates the accomplishment of NESC goals.
- Conduct research for the FEMA National Incident Management System (NIMS) Integration Center Compliance and Technical Assistance Branch to develop a rigorous performance assessment program based on preparedness goals and requirements.
- Examine critical decision-making factors prior to a catastrophic event and develop a roadmap identifying where to allocate resources to improve decision making across jurisdictions during a mass evacuation.
- Develop training tools for first responder leadership that address preparation for and response to crises and catastrophic events, specifically emphasizing the importance of fully integrating homeland security considerations into first responder culture, and the role of research and science.
- Developed EMCAPS (Electronic Mass Casualty Assessment and Planning Scenarios), a web-based shareware applet designed based on DHS planning scenarios to calculate and predict a surge in casualties at the local level.
- Developed award-winning Large Scale Pandemic model, which simulates the spread of infectious disease using both biological and sociological data. This realistic model will inform policy makers as it allows for the design and testing of optimal policies in the event of an infectious disease outbreak such as Pandemic Influenza.
- Developed deployable wireless sensor network compatible with first responder communication software that supports real-time monitoring of first responders.
- Identified the technology gaps that hinder the first responders' ability to effectively respond to large-scale incidents and disasters.

NDCIEM (University of North Carolina at Chapel Hill and Jackson State University): Focus on advancing the understanding of natural hazard resilience and transferring that knowledge into action, resulting in reduced loss of life or injury and lessened damages to the built and natural environment. Examples of specific projects include:

- Advance state of the art coastal wave and surge modeling to accurately represent coastal hazards for FEMA National Flood Insurance Program studies and emergency management preparedness.
- Integrate coastal wave and surge models with hydrologic and meteorological models to create a comprehensive modeling system that can predict inland and coastal flooding during hurricanes and other severe storms to guide emergency management response prior to, during and after storm events.
- Examine the quality and effectiveness of state and local hazard mitigation plans required under the Federal Disaster Mitigation Act (DMA) of 2000, including their ability to speed the wise expenditure of FEMA's hazard mitigation grant program and pre-disaster grant program funds.
- Assess the dynamics of coastal landforms (e.g., barrier islands, wetlands, dunes) and develop design guidance for their protection or restoration.
- Develop a practical methodology for hazard identification, risk assessment, impact analysis, and cost-benefit analysis and a training program for local and state officials in the use of the methodology.

- Examine differences in risk perceptions between citizens and decision makers, across geographic locations, and demographic groups; use findings to provide tailored approaches to improve preparedness and response.
- Develop enhanced models to more effectively plan regional transportation infrastructure improvements for disaster scenarios, and to test, evaluate and manage evacuations. The findings will also inform the temporal declaration of evacuation orders and the implementation of proactive evacuation measures such as phased evacuations and contraflow.
- Conduct research to better understand inter-organizational coordination in disasters and suggest ways to use ad hoc knowledge networks more effectively in disaster response.
- Evaluate models and strategies to make supply chains become more efficient and resilient such as multi-supplier strategies, supplier redundancy, risk sharing contracts and robust information management strategies.
- Conduct research to help officials do a better job of coordinating incidents that are multi-organizational and/or multi-jurisdictional by identifying skills, cultural features and social relationships that can foster effective improvised action. This project will design and test a training program in collaborative management and leadership for community and state officials involved in managing hazards and disasters.

Additionally, UP has developed a liaison relationship with FEMA to directly integrate FEMA into UP activities. A FEMA liaison works part time with UP to ensure FEMA coordination and collaboration with the COEs and education programs. Finally, FEMA has also directly funded modeling efforts at three COEs – PACER, CREATE and START.

Question: Is there any basic research conducted through university programs financed through other government agencies outside of DHS that S&T has been able to successfully coordinate with to further their homeland security mission?

ANSWER: Yes, the S&T Directorate has coordinated university programs with other federal agencies, including the National Science Foundation, U.S. Department of Health and Human Services, U.S. Department of Agriculture, Department of Defense and Department of Justice. These agencies provided funds to the Centers of Excellence (COEs) to conduct directed research. The Office of University Programs and the S&T Directorate have worked closely with the DHS components and other federal agencies to ensure that directed funds complement related research projects at the COEs and other federal research labs and facilities.

Centers of Excellence

Question: For the record, please highlight for the Committee the estimated funding for each Center of Excellence in fiscal year 2010. For those COEs that are not receiving funding, please explain why.

ANSWER: Please see the table below for the projected funding for each Center of Excellence.

Center of Excellence	FY 2010 President's Budget Request
Center for Advancing Microbial Risk Assessment (CAMRA)	-
Center Of Excellence for Risk & Economic Analysis of Terrorism Events (CREATE)	\$3,180,000
Center of Excellence for Command, Control and Interoperability	\$3,180,000
Center of Excellence for Maritime Island & Extreme/Remote Environmental Security	\$3,180,000

Center of Excellence	FY 2010 President's Budget Request
Center of Excellence for Explosives Detection, Mitigation, and Response	\$3,180,000
Center of Excellence for Border Security and Immigration	\$3,180,000
Center of Excellence for Foreign Animal & Zoonotic Disease Defense (FAZD)	\$3,180,000
Center of Excellence for Food Protection & Defense (NCFPD)	\$3,180,000
Center of Excellence for National Consortium for the Study of Terrorism and Responses to Terrorism (START)	\$3,180,000
Center of Excellence for Natural Disasters, Coastal Infrastructure and Emergency Management	\$3,180,000
Center of Excellence for the Study of Preparedness and Catastrophic Event Response (PACER)	\$3,180,000
Center of Excellence for Transportation Security	\$3,180,000
TOTAL:	\$34,980,000

In FY 2010, the S&T Directorate is not requesting additional funds for the Center for Advancing Microbial Risk Assessment (CAMRA). CAMRA was fully funded prior to FY 2010, with the intention of allocating funding to projects over several years. CAMRA will continue to use that funding in FY 2010.

Question: What, if any COEs, will re-compete in 2009 and 2010? How long do you anticipate this process will take and when will decisions be reached. Please address each competition separately.

ANSWER: Four Centers of Excellence (COE) will be in re-competition in 2009 and 2010. The S&T Directorate will re-compete:

- The food protection and defense COE, currently led by the University of Minnesota, in 2009; award by end of 2009.
- The foreign and zoonotic disease defense COE, currently led by Texas A&M University, in 2009; award by the end of 2009.
- The risk and economic analysis COE, currently led by the University of Southern California, in 2009; award in 2010.
- The terrorism and responses to terrorism COE, currently led by the University of Maryland, in 2010; award in 2011.

In general, competitions for COEs, whether new or re-competed, take about 10 months to 1 year to complete, depending on the complexity of the competition, i.e., whether there is a white paper pre-application period, the number of applicants and partners and the complexity of negotiations. For the four competitions mentioned above:

- The food protection and defense COE and foreign and zoonotic disease defense COE: The S&T Directorate's University Program (UP) began the re-competition process for two centers, food protection and defense, currently led by the University of Minnesota, and foreign and zoonotic disease defense, currently led by Texas A&M University in December 2008. The application period for these COEs closed in January 2009; extramural expert reviews took place in late April and early May 2009. UP will conduct internal relevancy reviews, site visits, negotiations and awards during the summer and early fall of 2009, with awards anticipated before the end of 2009.
- The risk and economic analysis COE: UP will initiate the re-competition for the risk and economic analysis COE, currently led by the University of Southern California in summer 2009. We anticipate that the funding announcement for this COE will be posted on www.FedBizOps.gov and www.grants.gov in July or August 2009, and will close in September or October 2009, followed by

external reviews, internal reviews, site visits, negotiations and award. We anticipate a new award in Spring 2010.

- The terrorism and responses to terrorism COE: UP will initiate the re-competition for the studies of terrorism and responses to terrorism COE, currently led by the University of Maryland in spring or summer of 2010. The entire process of solicitation, external reviews, internal reviews, site visits, negotiation and award is expected to take 10 months to one year. The new COE should be awarded by May-June 2011.

Question: Regarding the recent announcement of a new DHS Center of Excellence at Purdue University of Indiana and Rutgers University: The announcement implied that this Center will handle data management and interpretation tasks, please detail the anticipated projects that you expect to take place at this Center. What involvement will US-VISIT, e-Verify, or any of the other DHS data collection and Biometric identification components have in the projects taking place here.

ANSWER: The S&T Directorate's University Program (UP) announced Purdue and Rutgers as co-leads for the new Command, Control, and Interoperability Center of Excellence (C2I COE) on March 24, 2009 in the Federal Register. UP is currently developing detailed work plans with Purdue and Rutgers, which will denote specific project goals, milestones, and deliverables. Research at both Universities and their collaborating partners will be adaptable to a wide range of homeland security challenges. The role of this COE is primarily to pioneer new data analysis and visualization theories and methods. Research products will provide a future "rapid response" capability to quickly analyze and visualize diverse and disparate bodies of data, including, but not limited to, cyber security, immigration, natural disasters and public health.

Purdue, as Visualization Sciences Co-Lead, will create innovative and effective integrated data and visual analytic environments – frameworks, methods, and software – that advance the start-of-the-art in analyzing massive, heterogeneous, incomplete or temporally evolving homeland security data for anticipating, detecting and responding to DHS mission needs. Purdue's research will address three basic pillars:

- 1) Visually Adapted Analytical Techniques: Creating actionable environments for planning, decision making, and information explorations. These capabilities, which should be driven by the human decision maker's perceptual and cognitive abilities, will enable disparate, multi-type data to be readily integrated and analyzed
- 2) Advanced Computing and Mathematical Foundations: Integrates visual reasoning, hypothesis-driven analysis, and modeling and simulation of data-intensive events. These capabilities are critical to the extraction of information, knowledge, and wisdom from diverse data sets; and
- 3) Interactive Visual Analysis and Decision-making Environments: Enables humans to meet the challenges of increasingly complex retrospective, prospective and predictive tasks associated with diverse, constantly evolving homeland security missions.

Rutgers, as Data Sciences Co-Lead, will study methods to produce integrative, semantic analysis of dynamic, heterogeneous multimedia data in support of homeland security efforts. Rutgers will frame its research to address three fundamental challenges facing homeland security decision makers in the face of ever-increasing amounts of data:

- 1) Insufficient scalability of current methods for organizing, storing and retrieving information will not scale.

- 2) Potential inapplicability of current methods for expressing the need for information and evaluating the results in the future, as greater information spaces will demand different and better guidance for search.
- 3) The resultant decline in the ability of both experts and non-experts to retrieve and extract useful information in real time.

The data analysis and visualization research and capabilities developed at the Command, Control, and Interoperability Center of Excellence (C2I COE) will be applicable to a wide range of homeland security data, including, but not limited to, cyber security and forensics, immigration, natural disasters, sensor integration and public health. The C2I COE aligns with S&T Directorate Command, Control, and Interoperability Division. The Division aligns with customers and stakeholders such as US-VISIT and e-Verify through the integrated product team (IPT) process. Through this connection, the S&T Directorate communicates customer needs to the COE and COE capabilities to customers. This involvement allows coordination between the C2I COE, the S&T Directorate, and S&T Directorate customers.

Additionally, the C2I COE is already engaging with the Border Security and Immigration COE at the University of Arizona to apply its tools to biometric identification, which will be extended to other COEs (e.g., explosives, maritime). The S&T Directorate looks forward to continuing our coordination with the National Protection and Programs Directorate (NPPD) and the U.S. Citizenship and Immigration Services (USCIS) to leverage the work of the C2I COE into the ongoing efforts of US-VISIT and e-Verify.

First Responders

S&T has told the Committee in recent years that it has attempted to increase the input of first-responders into the technology and development process through a separate Integrated Product Team (IPT).

Question: Has S&T seen any measureable success from this increase?

ANSWER: The S&T Directorate is in the process of forming a First Responder IPT dedicated to serving the technology needs of first responders. The first responder technology topics that have been published in the S&T Directorate brochure were identified through numerous interactions (still ongoing) with the Federal Emergency Management Agency (FEMA) and many emergency management representatives of the local and state communities. The S&T Directorate first-responder engagement efforts include:

- **Project Responder:** The S&T Directorate engaged the first responder community representatives from across the nation in a workshop environment over two years, which has captured the top priority needs of the community. This activity has been very successful, and the S&T Directorate completed an update to our original Project Responder report in late 2008.
- The S&T Directorate is also actively involved with the Interagency Board (IAB) and several other organizations that represent the interests of the first responder community including the National Emergency Management Association (NEMA), the International Association of Fire Chiefs (IAFC), and the International Association of Fire Fighters (IAFF). The S&T Directorate also works closely with localities across the nation: Seattle, Anaheim, Cincinnati, New York and Chicago to name a few, and are able to capture and validate first responder needs as well as to identify common theme areas of interest for the responders.
- Additionally, the Infrastructure/Geophysical Division has a career fire lieutenant on staff (1/2 time) to provide subject-matter-expertise and advise on efficacy of various pursuits for responders.

Also, in FY 2010, the S&T Directorate plans to establish a budget to support the First Responder IPT to ensure the highest priority technology needs are identified and are addressed in our research and development work

Demonstrations and Pilot Programs

The engagement of end-users in demonstrations and pilot programs is a critical component of the development process for a technology. These events ensure that S&T's customers assisted in the maturation of a project and serve as a check so that S&T is not developing a product without a practical use, or investing a lot of time and funding in something that will just sit on the shelf.

Question: Has S&T been successful at getting the necessary cooperation from stakeholders to perform demonstrations on a regular basis?

ANSWER: Yes, the S&T Directorate has been successful at getting the necessary cooperation from stakeholders to perform demonstrations on a regular basis.

Question: What pilots and/or demonstrations, across all portfolios, does S&T have scheduled for the upcoming year that involve localities?

ANSWER: Please see the following table.

Name	Pilot/Demo Description	Local Partners	Date	Portfolio
Resilient Tunnel	Scaled Pressurized Testing of Tunnel Plug -- Demonstrate the ability of a second generation tunnel plug to withstand water pressures in a scaled tunnel environment	West Virginia University, Morgantown, WV	June 2009	Innovation
Wide Area Surveillance	Wide Area Surveillance Spiral I Demonstration -- demonstrate a 100 megapixel, 360 degree field-of-view persistent surveillance capability at Logan International Airport	Massachusetts Port Authority	TBD	Innovation
Future Attribute Screening Technologies (FAST)	FAST Primary Screening -- Conduct an operational demonstration using a simulated real-world event requiring human behavioral screening.	Cambridge, MA local law enforcement	September 2009	Innovation
Explosives Standoff Detection	Integration and demonstration of explosives standoff detection technology.	Kennewick, WA Police Department	FY 2009	Transition

Name	Pilot/Demo Description	Local Partners	Date	Portfolio
Critical Infrastructure Inspection Management System (CIIMS) Knowledge Management Tools, Collaborative Information Sharing, Threat Dissemination Standards	Demonstrate an infrastructure inspection management tool which allows law enforcement aviation units to perform inspections of CI. Aviation module is being modified for ground patrol use in Los Angeles	Maryland State Police (Aviation Command) and Los Angeles Police Department	FY 2009	Transition / Command Control and Interoperability Division
Hostile Intent Training Simulation	Develop course curriculum and supporting computer-based simulation technology to train validated behavioral indicators of deception and intent detection during screening and interviewing interactions at mass transit portals, to include tailoring the current course curriculum for state and local law enforcement by incorporating law enforcement-specific examples and vocabulary and piloting a tailored course with the Las Vegas Metropolitan Police Department (LVMPD) in 2009.	Las Vegas Metropolitan Police Department (LVMPD)	2009	Transition / Human Factors
Facility Restoration Demonstration	The Science and Technology Directorate's (S&T) Chemical and Biological Division (CBD) is collaborating with Los Angeles World Airports (LAWA) as part of a DHS-funded project to develop guidance, strategies and decision analysis tools for use in the cleanup of a major U.S. airport after an incident involving a chemical warfare agent release.	The partner airport in this project is Los Angeles International Airport (LAX). LAX is working closely with four Department of Energy National Laboratories to develop and exercise such guidance. The project brings together major stakeholders that also include: Los Angeles City and County Fire Departments, Los Angeles County Public Health Office, California Department of Environmental Protection, California National Guard 9th Civil Support Team, US Environmental Protection Agency, Federal Bureau of Investigation, US Customs and Border Protection and the Transportation Security Administration.	October 19-21, 2009	Chemical Biological Division

Name	Pilot/Demo Description	Local Partners	Date	Portfolio
Integrated CBRNE Detection System	S&T is sponsoring the Golden Phoenix Exercise, a series of table top exercises in FY09 and a final on the ground demonstration planned for May 2010. This exercise has now been merged with Golden Guardian, a California State Exercise. The Golden Phoenix Exercise will be used to demonstrate and test the ICBRNE Detection Demonstration pilot system as well as exercise the interagency concept of operations developed in conjunction with this pilot program.	California	May 2010	Transition / Chemical Biological Division
Advanced Container Security Device	Test and evaluate ACSD prototype systems in operational settings	SAIC – San Diego, CA; Maine Secure Composites, Orono, ME; Georgia Tech Research Institute, Atlanta, GA	2009	Transition / Borders and Maritime Security Division
Unattended Ground Sensors	Complete system testing of Unattended Ground Sensors (UGS) testbed on the southern border	<ul style="list-style-type: none"> - CBP, Douglas, AZ; - Innovative Wireless Technologies (IWT), Forest, VA; - McQ, Inc, Fredericksburg, VA; - MPS Techline of PA, Inc., Willow Grove, PA; - MIT/LL, Lexington, MA; 	2009	Transition / Borders and Maritime Security Division
Port and Coastal Radar Improvement Project	Conduct a radar test and evaluation that could provide a future technology feed into the USCG's Interagency Operations Center acquisition program.	<ul style="list-style-type: none"> - Long Island Power Authority (LIPA), Uniondale, NY; - Plum Island Animal Disease Center (PIADC), Plum Island, NY; - USCG Sector Command Center, New Haven, CT; - Noblis, Inc., Falls Church, VA; - Pennoni Assoc. Inc., Vineland, NJ; - LVS Inc., Wading River, NY; - Sensor Technologies Incorporated (STI), Red Bank, NJ; - US Army Communications, Electronic Research and Development Center (CERDEC), Ft. Monmouth, NJ 	2009	Transition / Borders and Maritime Security Division

Name	Pilot/Demo Description	Local Partners	Date	Portfolio
Tripwire Technologies	Engineering test of prototype system	<ul style="list-style-type: none"> - CBP Tucson Sector, Tucson, AZ; - Williams Electric Co., Ft. Walton Beach, FL; - Alpine Electric Co., El Paso, TX; - Sensor Technologies Incorporated (STI), Red Bank, NJ; - Emx, Inc., Melbourne, FL; - Night Vision & Electronic Sensors Directorate (NVESD), Ft Belvoir, VA; - Naval Research Lab (NRL), Washington, DC; - Sandia National Laboratory (SNL), Albuquerque, NM 	2010	Transition / Borders and Maritime Security Division
Port Security Test Bed in LA Long Beach, CA.	Installation and check-out of initial sensor technologies into the Port Security Test Bed	<ul style="list-style-type: none"> - USCG – LA, Long Beach, CA; - SPAWAR, San Diego, CA 	2009	Transition/Borders and Maritime Security Division
Northern Border Test Bed (NET-B)	Install and prove out the baseline capabilities of Northern Border Test Bed (NET-B)	<ul style="list-style-type: none"> - Systems and Processes Engineering Corp (SPEC), Austin, TX; - Advanced Technology Systems (ATS) Public Safety, McLean, VA; - NS Microwave, Spring Valley, CA; - Murnane Construction, Plattsburg, NY; - Robert M. Sutherland, P.C. Surveyor, Plattsburg, NY; - PrimeLink, Plattsburg, NY; - Champlain Telephone Co., Champlain, NY; - Treeman Tree Service, Inc., Dannemora, NY; - Leon Rabideau Excavation, Mooers, NY - CBP Swanton Sector HQ, Swanton, VT; - CBP Station Champlain, Champlain, NY; - CBP Station, Messena, NY; - Digital Design and Imaging Service (DDIS), Inc., Falls Church, VA; - MPS Techline of PA, Inc., Willow Grove, PA; - Innovative Wireless Technologies (IWT), Forest, VA; - BAE Systems - Burlington, MA - MIT/LL, Lexington, MA; - Night Vision & Electronic Sensors Directorate (NVESD); Ft Belvoir, VA 	2009	Transition / Borders and Maritime Security Division
Container Security Devices (CSDs)	Operationally test Container Security Devices (CSDs)	Georgia Tech Research Institute (GTRI) Atlanta, GA	2009	Transition / Borders and Maritime Security Division

Name	Pilot/Demo Description	Local Partners	Date	Portfolio
M-Lock	Marine Asset Tag Tracking Demo in Cargo environment	iControl Inc, Santa Clara, CA; Consolidated Freight Shipping, Detroit, MI; Southwest Airlines, Detroit, MI	2009	Transition / Borders and Maritime Security Division
Tunnel Detection	Advanced ground penetrating radar - Full Scale demonstration	Lockheed Martin Advanced Technology Laboratory, Cherry Hill, NJ, CBP/LSS/OIT, CBP/OIOC, OBP Tucson Sector	22-Jul-09	Innovation / Borders and Maritime Security Division
Multi-Band Radio (P25 Interfaces)	Lab T&E and Demonstration - Currently identifying long-term pilot sites	Institute for Telecommunications Sciences (Boulder, CO), New York Police Department, New York City Office of Emergency Management, Port Authority of New York and New Jersey, Fire Department of New York, New York City Department of Information Technology and Telecommunications, Michigan Emergency Medical Services, Boise (Idaho) Fire Department, Kentucky 41st Civil Support Team, Murray State University	Varies over the course of FY 2009 and FY 2010	Transition / Command Control and Interoperability Division
Regional Operations Platform Pilot (ROPP) (Wireless Broadband Productization)	Integrate existing platforms, enhanced visualization tools, and other data sets to allow participating states' systems to interoperate and exchange data with each other, regardless of the particular platform or application in use	Alabama, Florida, Kentucky, Mississippi, Tennessee, Texas, and Virginia, as well as observers from Georgia	FY 2009	Transition / Command Control and Interoperability Division
Botnet Detection and Mitigation	Malware detection/mitigation technologies - experimental deployment on S&T LABNET and Defense Research and Engineering Network (DREN)	Washington, DC	2009	Transition / Command Control and Interoperability Division
Web*DECIDE - Finance Sector Exercise Tool	Web*DECIDE distributed simulation - first deliverable and incremental demonstrations	Various Locations (depending on stakeholder participation)	Semi-annual starting April 2009	Transition / Command Control and Interoperability Division
Internet Route Monitoring	Prefix Hijack Alerting System - detection of Internet routing attacks and misconfigurations	Various locations (depending on stakeholder participation)	January 2009 into 2010	Transition / Command Control and Interoperability Division
Cyber Forensics - Various projects	Cyber Forensics to support law enforcement (Federal, State, Local)	Various Locations (depending on stakeholder participation)	Late 2009 into 2010	Transition / Command Control and Interoperability Division
Regional Technology Integration Initiative (RTII)	Anomaly detection and mitigation technology	Seattle, WA and surrounding cities	July 2009- June 2010	Transition / Command Control and Interoperability Division
Linking the Oil and Gas Industry to Improve Cyber Security (LOGIC)	Demonstration and analysis of Safety Instrumented System (SIS) in operational O&G environment	Coordination with industry, Washington DC	Mid-2010	Transition / Command Control and Interoperability Division

Name	Pilot/Demo Description	Local Partners	Date	Portfolio
Knowledge Management Tools, Collaborative Information Sharing, Common Operating (COP) Data Fusion Technologies	Examines information management processes at a fusion center to help determine information sharing and dissemination requirements.	Maryland Coordination and Analysis Center	FY 2010	Transition / Command Control and Interoperability Division
GeoPredict - Knowledge Management Tools, Collaborative Information Sharing, Cross Target threat Awareness	Deploy variants of a DoD geospatial predictive analytics tool to three fusion centers. The tools will be modified to allow predictive analysis of CI/KR protection and gang activity.	New Jersey Fusion Center, Los Angeles Fusion Center	FY 2009	Transition / Command Control and Interoperability Division
Regional Information Sharing and Collaboration (RISC) - Knowledge Management Tools, Knowledge Frameworks, Integrated Data Processing and Analysis	Establish and pilot digital image exchange specifications for the NLETS Image Sharing Program (NISP) that enable state and local law enforcement personnel to query and retrieve driver's license photos across state lines via the NLETS network.	Lehigh Valley Police Department, PA; Bethlehem PD, PA; New Jersey State Police, Seattle WA PD, Phoenix AZ ACJC	FY 2010	Transition / Command Control and Interoperability Division
Law Enforcement Information Framework (LEIF) - Knowledge Management Tools, Knowledge Frameworks, Integrated Data Processing and Analysis	Web-based and mobile incident analysis and collaboration technology for front-line law enforcement and counter-terrorism personnel. In operational use by agents.	A Joint Powers Agency (JPA) to share information among justice agencies throughout San Diego and Imperial Counties, California (a few examples include: San Diego Harbor Police, Escondido Police Department, National City Police Department)	FY 2010	Transition / Command Control and Interoperability Division
Virtual City - Knowledge Management Tools, Knowledge Frameworks, Integrated Data Processing and Analysis	Integrate multiple data sources (Automated License Plate Reader, CCTV, etc) into the City of Beverly Hills' Geospatial Information System (GIS)	City of Beverly Hills Police Department	FY 2010	Transition / Command Control and Interoperability Division
Staff Toolkit for Rapid Incident Prediction and Evaluation (STRIPE) - Knowledge Management Tools, Collaborative Information Sharing, Cross Target threat Awareness	Geospatial predictive analytics is a force multiplier for law enforcement intelligence in combating terrorism, gangs, and conventional criminal activity before an event occurs. As a central resource for intelligence led policing, it helps target gang leadership, locate gang recruiting, and intervene in planning for crimes.	Louisiana State Analytical Fusion Exchange (La-SAFE)	FY 2009	Transition / Command Control and Interoperability Division

Name	Pilot/Demo Description	Local Partners	Date	Portfolio
Privacy Technology	The research will evaluate a state or urban area fusion center's information sharing policy guidelines for products developed using Federal, State, local and private sector data, develop prototypes that evaluate if Federal, State, local or private sector policies impact information sharing by a Fusion Center and assess the ability of accountable systems to provide greater policy compliance at lower cost, with more streamlined and efficient information flow.	Boston Fusion Center	FY 2009	Transition / Command Control and Interoperability Division
Identity Management	The Department of Homeland Security (DHS) Science & Technology (S&T) Directorate has established an identity management test bed to evaluate various identity and access control architectures and technologies for the homeland security community, to develop proof-of-concept solutions, and to conduct pilot experiments.	OCIO Monterrey, CA	FY 2009	Transition / Command Control and Interoperability Division
Virtual State - Knowledge Management Tools, Knowledge Frameworks, Integrated Data Processing and Analysis	Demonstrate the effectiveness of distributing streaming video in response to school incident.	State of Alabama Office of Homeland Security	FY2010	Transition / Command Control and Interoperability Division
Forensic Analysis Tools Program, GPS Forensics Project	Demo of the capabilities of the GPS device Forensic Logical Analysis tool to Miami Dade Police Department	Miami Dade Police Department, Florida	FY 2010	Transition / Command Control and Interoperability Division
Intelligent Randomization in Scheduling (IRIS) Project	Potential involvement by Los Angeles World Airport police in IRIS pilot at LAX – using the developed algorithm to randomize general airport security scheduling	Los Angeles, California	FY 2010	Transition / Command Control and Interoperability Division

Question: How does S&T solicit input from localities, such as transit systems, on the types of technologies that they are interested in developing?

ANSWER: Through the DHS Office of Infrastructure Protection's (IP) National Infrastructure Protection Plan (NIPP) framework, the S&T Directorate engages with the Sector Specific Agencies (SSA), Government Coordinating Councils (GCC) and Sector Coordinating Councils (SCC) to identify capability gaps and research and development requirements. Through the NIPP process, each sector generates Sector Annual Reports

(SAR), in which they list and prioritize these capability gaps. The S&T Directorate considers customer capability gaps through the Capstone Integrated Product Team (IPT) process. The IPT process is the centerpiece of the S&T Directorate's product transition portfolio, which function in mission-critical areas to identify customers' needs and enable and transition near-term capabilities for addressing them. These Capstone IPTs engage DHS customers, acquisition partners, S&T technical division heads and end users as appropriate in our product research, development, transition and acquisition activities. The S&T Directorate draws on the knowledge and expertise of the members of the IPTs throughout the technology development process, from project proposal through transition of the technology solution to the customer. In this manner, mass transit systems, communities, localities and owner/operators are involved in technology identification, development and evaluation through the NIPP and Capstone IPT processes, in particular the Transportation IPT and the Infrastructure Protection IPT.

The S&T Directorate works closely with TSA, the Sector Specific Agency for the Transportation Sector to address capability gaps specific to mass transit systems. TSA reaches out to stakeholders nationwide and gathers technology capability gaps from the mass transit and passenger rail community. TSA solicits formal feedback from the Mass Transit Sector Coordinating Council and the Transit Security and Policing Peer Advisory Group, as well as through workshops with transit agencies related to specific categories of technology. Safety and Security Roundtables and Transit Security Grant Program outreach events have allowed TSA to compile additional input from transit agencies on technology development needs. TSA compiles capability gaps and submits them to the S&T Directorate through the IPT process. The S&T Directorate ultimately leverages all of these interactions to develop an understanding of key requirements of mass transit stakeholders. Additionally, the S&T Directorate works through TSA to directly engage stakeholders on a project-specific basis to refine capability gaps, conduct project planning, and measure the progress of ongoing efforts to ensure that research, development, testing, and evaluation efforts undertaken by the S&T Directorate address the identified stakeholder requirements.

Within the Infrastructure Protection IPT, several projects are being conducted in close coordination with mass transit stakeholders:

- **Bay Area Rapid Transit (BART) mitigation strategy:** In partnership with BART and Lawrence Livermore National Laboratory (LLNL), conducting small-scale blast experiments and computational analysis to design a mitigation strategy to protect a key vulnerability identified in the BART system.
- **Brick Tunnel Analysis:** In partnership with LLNL and ERDC, conducting blast testing and computational analysis to characterize the behavior of brick constructed tunnels under explosive loads for a key mass transit stakeholder.
- **Blast Analysis Tools:** In partnership with LLNL, ERDC and the Technical Support Working Group (TSWG), developing fast-running numerical models to enable infrastructure owners and operators to estimate the effects of explosive events on critical assets and assess the effectiveness of mitigation measures. Current work is focused on tunnels, bridges, dams, and complex urban environments. The tunnel analysis tool will include data from in-depth analyses of tunnel structural vulnerability to explosives devices conducted in close partnership with seven U.S. mass transit agencies.

The mass transit community is also heavily involved in a project within the S&T Directorate Innovation Portfolio:

- **Resilient Tunnel Project:** The S&T Directorate is developing inflatable tunnel plugs with the potential to protect critical transportation tunnels from fire, flooding, and other hazards. Early on in this project, the S&T Directorate engaged the Transportation Security Administration (TSA), Washington Metro Area Transit Authority (WMATA), and the Port Authority of New York and New Jersey (PANYNJ) to

identify the performance and operational requirements that have guided project development. These organizations remain heavily engaged in the day-to-day project development and plan to provide locations for prototype deployment. As the project matures, the S&T Directorate is working with TSA to engage more mass transit owners and operators in order to develop strategies to employ this technology across the sector.

National Bio- and Agro- Defense Facility (NBAF)

Question: Has DHS conducted additional studies, besides the EIS, to determine the additional environmental, economic, and security costs of constructing the NBAF on the U.S. mainland? In particular, has DHS considered the heightened security costs, such as the need for increased perimeter security, associated with being located on the mainland?

ANSWER: Yes. The S&T Directorate conducted the following additional studies in support of the site selection process: site cost analysis, site characterization study and the Plum Island Closure and transition cost study. These studies are available on the National Bio and Agro-defense Facility (NBAF) website www.dhs.gov/nbaf. The information from these studies was used by the S&T Directorate to evaluate strengths and weaknesses of each site alternative against the mission criteria (proximity to research for the NBAF mission, proximity to workforce, acquisition/construction, operation and community acceptance). In addition, the S&T Directorate conducted a security assessment (Threat and Risk Assessment) to determine the threats and vulnerabilities to the NBAF at each of the site locations. The S&T Directorate found that the NBAF Environmental Impact Statement (EIS) and the Threat and Risk Assessment presented very little differentiation between the sites. All of these factors, along with the EIS and NBAF Risk Assessment, were taken into account in the site selection process and final site recommendations.

Yes. The site cost analysis took into account the required security needed for both the NBAF construction and operations at each of the six alternative sites. Regardless of the final site chosen, the S&T Directorate will implement robust physical security measures for the NBAF including dual layered perimeter fencing, access control, and monitoring systems. The costs will be updated as more detailed security requirements are developed during the site specific design.

Question: Some have claimed that the added distance between a laboratory and the mainland that an island offers would provide an extra layer of protection. Could you provide the Committee with an explanation for why the NBAF is better suited for the mainland?

ANSWER: The recommendation to select a mainland site for the National Bio and Agro-defense Facility (NBAF) by the NBAF Steering Committee was based on several factors. The site evaluation criteria were key to the recommendation and they were: proximity to research for NBAF mission; proximity to workforce; community acceptance; and acquisition, construction, and operation of the facility. The lack of significant differentiation between a mainland or island site in the environmental impact statement (EIS) and the Threat and Risk Assessment (TRA) further reduced the need to build on an island. Also, the World Organization for Animal Health (OIE) – the international organization that determines a country's foot and mouth disease (FMD) status – indicated it would not follow its prior declaration of the United States as an FMD free nation if a future outbreak occurs on an island. Finally, the Manhattan, KS site was deemed to have more strengths and fewer weaknesses when evaluated against the selection criteria.

The S&T Directorate issued a Record of Decision (ROD) for the NBAF EIS in January 2009 explaining the rationale for why a mainland site was chosen. The ROD was on the proposed site, construction, and operation of the facility and can be found on the NBAF website www.dhs.gov/nbaf. A summary is included below.

The National Environmental Protection Act (NEPA) regulation requires federal agencies to examine the impacts of proposed actions before decisions are made on such actions. The proposed action was the construction and operations of the NBAF. As part of its site selection analysis, the S&T Directorate conducted two separate risk assessments to determine if FMD work can be safely conducted on the mainland. The Health and Safety Risk Assessment was conducted as part of the NBAF EIS to address both the probability and consequences of potential adverse events for each of the alternative sites. A separate TRA was completed to identify and evaluate the potential security risks (threats, vulnerabilities, and consequences). Both of the risk assessments were reviewed by subject matter experts to analyze the results and to assure that the approach and methodology were sound. The results of both of these risk assessments along with the four mission criteria were then used to assign final site ratings, which resulted in a final ranking of preferred sites at which to construct and operate the NBAF.

To ensure that the Health and Safety risk assessment covered the worst case scenarios, the approach and methodology was based on the National Academy of Sciences (NAS) Committee letter report (April 2008) which provided important considerations for developing a risk assessment for operating a high-biocontainment laboratory. These considerations were: 1) What could go wrong (sequence of events that could cause an infectious pathogen to escape the laboratory, set-up a chain of transmission, and cause infection disease in the surrounding community?); (2) What are the probabilities of such a sequence of events?; (3) What would be the consequences of such a sequence of events (e.g. the impacts of a release including transmission of disease, morbidity, and mortality)?

The major concern for NBAF analysis is the potential for outbreaks of disease in livestock, wildlife and humans. Three pathogens were then chosen to bound the hazards, accidents and consequences for the NBAF: Foot and Mouth Disease Virus, Rift Valley Fever Virus and Nipah Virus. Foot and Mouth disease is a Foreign Animal disease that does not impact humans while Rift Valley and Nipah are zoonotic diseases that impact human life. The accidents analysis in the Health and Safety risk assessment considered eight scenarios for evaluation including spill/uncontrolled release of pathogens, lab acquired infection, loss of an infected animal, release of contaminated wastes, large room or facility fire, over-pressure event from deflagration, natural phenomena events (seismic or high wind with no fire), and aircraft crash into the facility. Conservative viral pathogens were used in the model and exceeded the planned amounts that would be used at NBAF. The Gaussian plume model was chosen because it conservatively models downwind concentrations of hazardous constituents (biological pathogens) from an unlikely accidental release. It should be noted that other government agencies have used the Gaussian Plume model to provide estimates of potential down-wind concentrations of biological materials resulting from release.

The Health and Safety risk assessment results for the mitigated risk were shown to be extremely low given appropriate attention to the design, construction, and operation of the NBAF and was independent of site. Most of the accidents were calculated to result in a release ranging from 1 in 10,000 operating years to 1 in 1 million operating years. Two accidents (loss of animal/insect) and release of infected waste were calculated to result in a release ranging from 1 in 100 operating years to 1 in 10,000 operating years. At the mainland sites, only the significant accidents of a large fire or an over-pressure event are considered to have the potential for resulting in an infection after a release. The risk of a release from these accidents was minimal, ranging from 1 in 10,000 years to 1 in 1 million operating years.

The S&T Directorate did note that the potential impact of pathogen release would be slightly less at the Plum Island Site, due in part to there being less opportunity for the pathogen to become established and spread. The economic impact of an outbreak of FMD virus, primarily from potential foreign bans on United States livestock, could result in a loss in the range of \$2.8 billion in the Plum Island region to \$4.2 billion in the Manhattan, KS region over an extended period of time. Regardless of site location, the potential for economic losses for a worse case scenario is non-trivial and the S&T Directorate determined that the difference in impacts from accidental releases between Plum Island and any of the mainland sites were negligible.

The results of the Health and Safety Risk Assessment were reviewed by three separate review teams that had uniquely qualified subject matter experts. The review teams consisted of an External Review group from outside of the S&T Directorate; an internal review from within DHS and the United States Department of Agriculture (USDA); and a Steering Committee to review the risk assessment methodology, EIS and risk results, and to evaluate strengths and weaknesses to develop final recommendations to the agency officials. It should also be noted that the review process included public and stakeholder review and input as part of the NEPA/EIS process. Over 5,000 comments were received from the Draft EIS and considered prior to the final EIS being published. Numerous public meetings were held as part of the EIS process to allow for comments to be provided.

External reviews from experts at the Massachusetts Institute of Technology (MIT), Johns Hopkins and Gryphon agreed that the overall risk assessment analysis was appropriate and reasonable. The review confirmed that aerosol calculations represented a reasonable, conservative and well-thought approach to determining the hazards associated with potential accidental releases. It was also noted that conservative estimates of viral pathogen quantities were modeled and that the Gaussian plume model was suitable as a representation of the probability that an area at a given distance away from the NBAF would be affected, and to what extent, by an accidental release.

In addition, the risk assessment, EIS, and other supporting documents were reviewed by the internal DHS and USDA team. The DHS and USDA review teams had expertise in risk assessment, bio-containment safety and security, operations, EIS reviews and FMD research. The internal review team conducted thorough reviews of the EIS and risk assessments throughout the document development phase, including the Scoping phase, Draft EIS and Final EIS documents.

A senior level Steering Committee, comprising career federal employees from DHS and USDA, with extensive expertise in biocontainment design, construction, and operations; laboratory facility site selection; risk assessment; and modeling, biosafety and biosecurity, FMD research and other high consequence bioagents. The Steering Committee reviewed the EIS, Health and Safety Risk Assessment, Threat and Risk Assessment, and other supporting documents such as the site cost analysis and site characterization study.

Based on the results of their review, the Steering Committee concluded that the EIS and TRA offered very little differentiation between the sites. The risk assessment stated that the risk of release of a biological pathogen from the NBAF was independent of where the NBAF was located since the range of accidents could happen at any of the alternative sites. The Steering Committee concluded that the likelihood of a release of a pathogen was very low, given appropriate attention to the design, construction, and operation of the NBAF with an array of safety controls. The Steering Committee further determined that the risk of release of any identified pathogen proposed for study within the NBAF could be mitigated by implementation of operational protocols, rigid security measures, and adherence to the U.S. government biosecurity guidelines.

The Steering committee concluded that the range of cost impacts for all six sites (\$2.8 - \$4.2 billion) is within the same order of magnitude because this number is largely based on the potential loss of trade status until the U.S. is again declared FMD-free. The Steering Committee also reviewed the TRA (security assessment) and determined that the insider threat is the biggest threat to the NBAF and independent of site. The committee also concluded that there are no significant differentiators between the site alternatives with respect to potential "land-based", "airborne", or "waterborne" attack given the known threats identified by the TRA. The attractiveness of the sites as targets and specific threats identified by the threat analysis are considered to be mitigated by appropriate security measures. The environmental impacts analyzed in the EIS and the site specific threats were all very similar and that there were only minor differentiators that could be found.

It was determined that the key differentiator among the sites was the original four evaluation criteria: proximity to research for NBAF mission, proximity to workforce, acquisition/construction/operation, and community acceptance. Because this facility is intended to be the Nation's preeminent research facility for foreign animal

disease and zoonotic disease research, the site's proximity to research capabilities that can be linked to NBAF mission requirements was emphasized among the four evaluation criteria.

Based on an evaluation of all the alternatives, the Steering Committee determined that the Manhattan Campus Site clearly possessed more strengths and fewer weaknesses than any other alternative and best met the purpose and need to site, construct and operate the NBAF. Specifically, its location near Kansas State University (KSU) provides site proximity to existing research capabilities that can be linked to NBAF mission requirements. Additionally, the site's proximity to the KSU College of Veterinary Medicine, KSU College of Agriculture and the Biosecurity Research Institute is relevant to the NBAF mission and a significant strength. The EIS demonstrated that construction and operation of the NBAF at the Manhattan Campus Site would be environmentally acceptable as almost all environmental impacts fell into the "no impacts to minor impacts" category. As stated in the EIS and agreed to by the Steering Committee, the risk of release of a pathogen was independent of where the NBAF was located. The Manhattan Campus Site alternative demonstrated very strong community acceptance from local, State, and federal officials and stakeholders. Additionally, the consortium offered a substantial, unconditional off-set package, including use of the KSU Biosecurity Research Institute. Having NBAF on a mainland site such as the Manhattan Campus Site will facilitate the use of diagnostic capabilities.

An additional factor was the new information received from the World Organization for Animal Health (OIE). The OIE is responsible for determining a Nation's FMD status, which impacts that country's ability to export meat. Recent discussions and a subsequent written letter from OIE affirmed that the United States FMD free status would be impacted if a release occurred at either a mainland or island location. OIE stated that the national impact of an outbreak is more related to how authorities respond to the incursion rather than where the outbreak occurs. It should be noted that this is a departure from the previous OIE ruling on United States FMD free status after 1978 Plum Island FMD virus release.

Question: Has DHS examined whether Plum Island's location is a significant factor in the recruitment and retention of staff?

ANSWER: The S&T Directorate has not conducted a formal study or survey, but has received feedback from candidates for jobs at the Plum Island Animal Disease Center (PIADC) that indicate their unwillingness to accept a job at PIADC due to the location and the antiquated research conditions at the facility. As stated in the National Bio and Agro-defense Facility (NBAF) Record of Decision in January 2009, DHS concluded that Plum Island's lack of proximity to medical schools, veterinary schools, and BSL 3 to BSL 4 laboratories with mission related areas did not meet the purpose and need to site, construct and operate NBAF at Plum Island. This lack of proximity would significantly limit establishing long-term enduring research capabilities on Plum Island and impacts its abilities to attract top scientists needed to sustain future research capabilities for foreign animal diseases and zoonotic diseases.

Question: How does S&T envision the NBAF will fit into the current load of research that S&T supports on biological diseases and threats? Will the NBAF be wholly complementary of all of the research currently conducted through the University Programs, or will it supplant some of that research?

ANSWER: The S&T Directorate's Chemical and Biological Division supports targeted advanced development and basic research on foreign animal disease countermeasures (vaccines and diagnostics). This research and development currently focuses primarily on foot-and-mouth disease (FMD) programs conducted at the Plum Island Animal Disease Center (PIADC) in close coordination with colleagues in the U.S. Department of Agriculture (USDA) Animal Research Service (ARS) and Animal and Plant Health Inspection Service (APHIS). The work at National Bio and Agro-defense Facility (NBAF) will expand beyond the current level

of work being done on FMD countermeasures to include additional FMD work and other foreign animal and zoonotic diseases.

NBAF and its associated program requirements, including planning for activities beyond the current PIADC mission, are and have been a part of the long term S&T Directorate strategic and research plans. This includes ongoing inter-agency discussions in the context of the National Science and Technology Council (NSTC) Foreign Animal Disease Threats Subcommittee, which is co-Chaired by representatives from the USDA ARS and the S&T Directorate.

Research conducted at the National Bio and Agro-defense Facility (NBAF) will be a continuation of the countermeasure work currently being conducted at the Plum Island Animal Disease Center (PIADC) and will address other zoonotic diseases that are not currently being addressed. NBAF research will not supplant any work at the DHS Centers of Excellence (COE) and in fact there will be new opportunities for COEs and other universities to conduct joint research projects with the DHS and U.S. Department of Agriculture staff at NBAF. The university COE focused on foreign animal and zoonotic diseases is currently undergoing peer reviewed re-competition for FY 2010 and beyond. When the recipient of the COE is named, the S&T Directorate's Chemical and Biological Division will work with the lead institution to finalize a research plan that complements programs currently ongoing at PIADC, and those planned for NBAF.

Question: Please provide the Committee the latest timeline for site prep and construction of the selected NBAF site, the closure of the old laboratory, sale of Plum Island, and the necessary remediation work.

ANSWER: The S&T Directorate will begin preparing the National Bio and Agro-Defense Facility (NBAF) site for construction in late FY 2010 with the expectation that the facility will be ready for occupancy in 2015. Transition from the Plum Island Animal Disease Center (PIADC) to NBAF is expected to begin in 2015 and be completed by 2017. Closure would be in 2017 and be performed from 2017 to 2018. A more detailed schedule of the PIADC and Plum Island demolition and disposal, remediation, and closure will be dependent upon the timing of the sale of Plum Island.

Test & Evaluations and Standards

Question: Has S&T encountered any resistance from other agencies while you attempt to implement the oversight of the T&E division on any DHS procurement initiatives? Provide us some examples, and what has been your recourse if you run into a situation like this?

ANSWER: No. The Department and the S&T Directorate's Test & Evaluation, and Standards Division (TSD) created the Test and Evaluation (T&E) Council and promulgated acquisition policy. The Department's Acquisition Program Management Division co-chairs the T&E Council. All components actively participate in the T&E Council. The T&E Council is crucial in establishing relationships with T&E personnel throughout the Department and developing DHS T&E policy. The Department's Acquisition Directive 102-01 (interim) documents TSD's role in the acquisition process. The Directive signifies the most important single event in the Department's T&E evolution. The Directive requires all Level 1 and non-delegated Level 2 acquisition programs to comply without exception and establishes the Director of Operational Test and Evaluation (DOT&E) as a member of the Acquisition Review Board (ARB) led by the Deputy Secretary. The TSD and DOT&E provide T&E oversight for all major acquisition programs that have gone before an ARB during FY 2009 and provide an independent view of the status of the test program to the senior Department leadership. TSD is successfully expanding its reach to all Level 1 and non-delegated Level 2 programs.

Question: Do your efforts appear to have the full support of the incoming Department leadership?

ANSWER: Yes.

Management

Question: Please list all S&T political employees who received bonuses in 2008. Include the position, office, and bonus amount.

ANSWER: Science and Technology Directorate political employees did not receive any bonuses in 2008.

Question: Please list all S&T SES bonuses provided in 2008 by position, office, and bonus amount.

ANSWER: Please see the following table.

S&T SES Bonuses -2008		
Position	Office	Amount
Deputy Under Secretary	Office of the Under Secretary for S&T	\$22,451
Division Head	Command, Control & Interoperability	\$14,984
Division Head	Infrastructure and Geophysical	\$12,739
Division Head	Chemical and Biological	\$12,985
Director	Innovation/HSARPA	\$17,686
Division Head	Human Factors	\$18,381
Division Head	Explosives	\$9,647
Director	Strategy, Policy and Budget	\$24,360

Question: Please list by office and pay grade level the number of non-SES employees who received a bonus or quality step increase (qsi) in 2008, the total bonus/qsi expenditures for the particular office and pay grade, and the total number of employees in the office and pay grade.

ANSWER: Please see the following table.

Office	Pay Plan	Grade	Award Type	Award Amount
Office of the Under Secretary	GS	15/10	Bonus	4,470.00
Total Employees/Awards by Grade		1		4,470.00
	GS	14/01	Bonus	2,941.00
Total Employees/Awards by Grade		1		2,941.00
Office of the Chief of Staff	GS	11/01	NA*	-
Total Employees/Awards by Grade		1		-
Office of Research	ST	00/00	Bonus	6,340.00
	ST	00/00	Bonus	4,755.00
Total Employees/Awards by Grade		2		11,095.00
	GS	15/02	Bonus	2,383.00
Total Employees/Awards by Grade		1		2,383.00
Office of Research/Office of National Labs	GS	15/10	Bonus	2,980.00
	GS	15/08	QSI	-
	GS	15/06	QSI	-
	GS	15/06	Bonus	4,036.00

Office	Pay Plan	Grade	Award Type	Award Amount
	GS	15/06	Bonus	2,691.00
	GS	15/04	Bonus	2,537.00
	GS	15/03	Bonus	3,690.00
	GS	15/01	NA*	-
Total Employees/Awards by Grade		8		15,934.00
	GS	14/09	Bonus	3,725.00
	GS	14/07	Bonus	3,304.00
	GS	14/06	Bonus	3,212.00
Total Employees/Awards by Grade		3		10,241.00
Office of Research/University Programs	SL	00/00	Bonus	4,755.00
Total Employees/Awards by Grade		1		4,755.00
	GS	15/04	Bonus	3,806.00
	GS	15/04	Bonus	3,806.00
	GS	15/01	Bonus	3,460.00
Total Employees/Awards by Grade		3		11,072.00
Office of Innovation/HSARPA	ST	00/00	Bonus	4,593.00
	ST	00/00	Bonus	3,170.00
	ST	00/00	Bonus	4,728.00
Total Employees/Awards by Grade		3		12,491.00
Total Employees/Awards by Grade	GS	15/10	Bonus	2,807.00
Total Employees/Awards by Grade		1		2,807.00
	AD	00/00	Bonus	8,000.00
	AD	00/00	Bonus	8,000.00
	AD	00/00	Bonus	6,000.00
	AD	00/00	Bonus	8,000.00
	AD	00/00	Bonus	7,000.00
	AD	00/00	Bonus	6,000.00
	AD	00/00	Bonus	7,000.00
	AD	00/00	Bonus	3,000.00
	AD	00/00	Bonus	2,000.00
Total Employees/Awards by Grade		9		55,000.00
Office of Transition	ST	00/00	Bonus	4,608.00
Total Employees/Awards by Grade		1		4,608.00
	GS	15/10	Bonus	4,470.00
	GS	15/10	Bonus	4,470.00
	GS	15/05	NA*	-
	GS	15/05	Bonus	3,921.00
	GS	15/01	Bonus	3,460.00
	GS	15/01	QSI	-
Total Employees/Awards by Grade		6		16,321.00
	GS	09/01	Bonus	1,443.00
Total Employees/Awards by Grade		1		1,443.00
Operations Analysis Division	GS	15/10	Bonus	4,470.00
	GS	15/07	Bonus	4,151.00
	GS	15/06	Bonus	2,691.00
	GS	15/04	Bonus	2,537.00
Total Employees/Awards by Grade		4		13,849.00

Office	Pay Plan	Grade	Award Type	Award Amount
	GS	01/01	NA*	-
Total Employees/Awards by Grade		1		-
Corporate Communications Division	SL	00/00	Bonus	4,755.00
Total Employees/Awards by Grade		1		4,755.00
	GS	15/06	Bonus	4,036.00
Total Employees/Awards by Grade		1		4,036.00
	GS	14/08	Bonus	3,627.00
	GS	14/05	Bonus	4,433.00
	GS	14/05	Bonus	3,333.00
	GS	14/02	Bonus	4,039.00
Total Employees/Awards by Grade		4		15,432.00
	GS	12/01	Bonus	2,093.00
Total Employees/Awards by Grade		1		2,093.00
	GS	03/01	NA*	-
Total Employees/Awards by Grade		1		-
Business Ops, Services & Human Capital	GS	15/10	Bonus	5,960.00
	GS	15/10	NA*	-
	GS	15/07	Bonus	5,151.00
	GS	15/07	Bonus	4,151.00
	GS	15/07	QSI	-
	GS	15/06	Bonus	5,036.00
	GS	15/06	QSI	-
	GS	15/05	Bonus	5,221.00
	GS	15/04	Bonus	3,806.00
	GS	15/04	Bonus	3,806.00
	GS	15/04	Bonus	2,537.00
	GS	15/04	Bonus	3,806.00
	GS	15/04	Bonus	2,537.00
	GS	15/01	Bonus	2,306.00
Total Employees/Awards by Grade		14		44,317.00
	GS	14/07	Bonus	2,306.00
	GS	14/06	Bonus	3,529.00
Total Employees/Awards by Grade		2		5,835.00
	GS	13/04	Bonus	2,738.00
	GS	13/03	Bonus	2,655.00
	GS	13/01	Bonus	2,489.00
Total Employees/Awards by Grade		3		7,882.00
	GS	12/05	Bonus	2,372.00
Total Employees/Awards by Grade		1		2,372.00
International Programs Division	SL	00/00	Bonus	6,000.00
Total Employees/Awards by Grade		1		6,000.00
	GS	15/06	Bonus	3,339.00
	GS	15/04	Bonus	3,806.00
	GS	15/02	Bonus	3,623.00
Total Employees/Awards by Grade		3		10,768.00
	GS	14/04	Bonus	4,235.00
	GS	14/01	QSI	-

Office	Pay Plan	Grade	Award Type	Award Amount
Total Employees/Awards by Grade		2		4,235.00
	GS	12/06	Bonus	2,442.00
	GS	12/02	NA*	-
	GS	12/02	Bonus	2,163.00
Total Employees/Awards by Grade		3		4,605.00
	GS	04/01	NA*	-
Total Employees/Awards by Grade		1		-
Interagency Programs Division	ST	00/00	Bonus	4,755.00
Total Employees/Awards by Grade		1		4,755.00
	GS	15/10	NA*	-
	GS	15/09	Bonus	5,782.00
	GS	15/08	QSI	-
	GS	15/04	Bonus	3,806.00
Total Employees/Awards by Grade		4		9,588.00
Special Programs Division	GS	15/10	Bonus	4,470.00
	GS	15/10	Bonus	4,470.00
	GS	15/05	Bonus	3,921.00
Total Employees/Awards by Grade		3		12,861.00
Strategy, Policy and Budget Division	GS	15/08	Bonus	3,500.00
	GS	15/07	Bonus	5,051.00
	GS	15/06	Bonus	3,500.00
	GS	15/06	QSI	-
	GS	15/05	Bonus	5,221.00
	GS	15/04	Bonus	3,537.00
	GS	15/04	Bonus	4,306.00
	GS	15/04	Bonus	2,537.00
	GS	15/03	QSI	-
	GS	15/03	Bonus	3,690.00
	GS	15/02	Bonus	4,765.00
Total Employees/Awards by Grade		11		36,107.00
	GS	14/08	Bonus	2,918.00
	GS	14/05	Bonus	3,333.00
	GS	14/04	Bonus	4,235.00
	GS	14/03	Bonus	2,591.00
	GS	14/03	Bonus	2,091.00
	GS	14/01	Bonus	3,541.00
	GS	14/01	Bonus	2,941.00
	GS	14/01	Bonus	1,961.00
Total Employees/Awards by Grade		8		23,611.00
	GS	12/06	Bonus	1,628.00
	GS	12/01	Bonus	4,493.00
Total Employees/Awards by Grade		2		6,121.00
	GS	11/04	Bonus	1,921.00
	GS	11/01	Bonus	1,164.00
Total Employees/Awards by Grade		2		3,085.00
	GS	09/09	Bonus	2,028.00
	GS	09/01	Bonus	1,500.00

Office	Pay Plan	Grade	Award Type	Award Amount
Total Employees/Awards by Grade		2		3,528.00
	GS	08/07	Bonus	1,045.00
	GS	08/04	Bonus	2,037.00
	GS	08/02	NA*	-
Total Employees/Awards by Grade		3		3,082.00
	GS	04/01	NA*	-
Total Employees/Awards by Grade		1		-
Test & Evaluation and Standards Division	GS	15/10	Bonus	4,470.00
	GS	15/10	Bonus	5,960.00
	GS	15/08	QSI	-
	GS	15/05	Bonus	1,366.00
	GS	15/03	Bonus	3,690.00
Total Employees/Awards by Grade		5		15,486.00
	GS	14/04	Bonus	3,735.00
Total Employees/Awards by Grade		1		3,735.00
Command, Control and Interoperability Div	ST	00/00	Bonus	4,755.00
Total Employees/Awards by Grade		1		4,755.00
	GS	15/10	Bonus	5,000.00
	GS	15/10	Bonus	4,470.00
	GS	15/10	Bonus	4,470.00
	GS	15/10	Bonus	4,470.00
	GS	15/09	Bonus	4,382.00
	GS	15/07	Bonus	4,151.00
	GS	15/06	Bonus	4,036.00
	GS	15/05	Bonus	3,921.00
	GS	15/05	Bonus	3,921.00
	GS	15/05	Bonus	3,921.00
	GS	15/04	Bonus	3,806.00
Total Employees/Awards by Grade		11		46,548.00
	GS	14/10	Bonus	3,823.00
	GS	14/01	Bonus	2,941.00
	GS	14/01	Bonus	2,941.00
	GS	14/01	Bonus	2,941.00
Total Employees/Awards by Grade		4		12,646.00
	GS	12/08	QSI	-
Total Employees/Awards by Grade		1		-
	GS	11/08	Bonus	1,436.00
Total Employees/Awards by Grade		1		1,436.00
	GS	09/01	Bonus	1,552.00
Total Employees/Awards by Grade		1		1,552.00
Infrastructure & Geophysical Division	ST	00/00	Bonus	4,755.00
Total Employees/Awards by Grade		1		4,755.00
	GS	15/08	Bonus	4,267.00
	GS	15/07	Bonus	4,151.00
	GS	15/04	QSI	-
	GS	15/04	Bonus	4,506.00
	GS	15/04	Bonus	3,806.00

Office	Pay Plan	Grade	Award Type	Award Amount
Total Employees/Awards by Grade		5		16,730.00
Explosives Division	ST	00/00	Bonus	4,755.00
	ST	00/00	Bonus	6,000.00
Total Employees/Awards by Grade		2		10,755.00
	GS	15/10	Bonus	5,960.00
	GS	15/09	Bonus	5,842.00
	GS	15/06	Bonus	5,336.00
	GS	15/06	Bonus	4,536.00
	GS	15/06	Bonus	2,691.00
	GS	15/05	Bonus	5,221.00
	GS	15/05	Bonus	2,614.00
	GS	15/01	Bonus	3,960.00
Total Employees/Awards by Grade		8		36,160.00
Chemical and Biological Division	ST	00/00	Bonus	4,755.00
	ST	00/00	Bonus	6,340.00
	ST	00/00	Bonus	2,870.00
	ST	00/00	Bonus	6,340.00
	ST	00/00	Bonus	3,170.00
Total Employees/Awards by Grade		5		23,475.00
	GS	15/10	Bonus	2,980.00
	GS	15/10	Bonus	2,980.00
	GS	15/09	Bonus	4,470.00
	GS	15/08	Bonus	2,845.00
	GS	15/08	Bonus	2,845.00
	GS	15/07	Bonus	4,151.00
	GS	15/06	Bonus	4,036.00
	GS	15/05	Bonus	2,614.00
	GS	15/04	Bonus	2,537.00
	GS	15/04	Bonus	2,537.00
	GS	15/04	Bonus	3,806.00
	GS	15/03	QSI	-
	GS	15/02	Bonus	2,383.00
	GS	15/01	Bonus	3,106.00
	GS	15/01	Bonus	3,106.00
	GS	15/01	NA*	-
Total Employees/Awards by Grade		16		44,396.00
	GS	14/10	Bonus	2,549.00
	GS	14/02	Bonus	1,013.00
Total Employees/Awards by Grade		2		3,562.00
Borders and Maritime Security Division	ST	00/00	Bonus	4,755.00
Total Employees/Awards by Grade		1		4,755.00
	GS	15/10	Bonus	4,470.00
	GS	15/10	Bonus	2,980.00
	GS	15/09	Bonus	4,382.00
	GS	15/06	Bonus	4,036.00
	GS	15/06	Bonus	2,691.00
	GS	15/05	Bonus	2,614.00

Office	Pay Plan	Grade	Award Type	Award Amount
	GS	15/04	Bonus	3,806.00
	GS	15/03	Bonus	4,920.00
Total Employees/Awards by Grade		8		29,899.00
	GS	13/03	Bonus	885.00
Total Employees/Awards by Grade		1		885.00
Human Factors Division	ST	00/00	Bonus	3,170.00
Total Employees/Awards by Grade		1		3,170.00
	GS	15/10	Bonus	4,470.00
	GS	15/09	Bonus	4,382.00
	GS	15/07	Bonus	5,534.00
	GS	15/06	Bonus	2,691.00
	GS	15/06	NA*	-
	GS	15/04	Bonus	3,806.00
	GS	15/01	Bonus	3,460.00
	GS	15/01	QSI	-
	GS	15/01	Bonus	3,460.00
Total Employees/Awards by Grade		9		27,803.00
	GS	14/07	Bonus	3,529.00
	GS	14/02	Bonus	3,039.00
	GS	14/01	Bonus	3,921.00
Total Employees/Awards by Grade		3		10,489.00
Plum Island Animal Disease Center	GS	15/10	Bonus	4,470.00
	GS	15/06	Bonus	4,219.00
	GS	15/02	Bonus	3,737.00
Total Employees/Awards by Grade		3		12,426.00
	GS	14/10	Bonus	2,664.00
	GS	14/06	Bonus	3,584.00
	GS	14/05	Bonus	1,161.00
	GS	14/03	Bonus	1,093.00
	GS	14/01	Bonus	3,074.00
Total Employees/Awards by Grade		5		11,576.00
	GS	13/08	Bonus	2,139.00
	GS	13/07	Bonus	3,122.00
	GS	13/06	Bonus	3,835.00
	GS	13/05	QSI	-
	GS	13/01	Bonus	2,601.00
Total Employees/Awards by Grade		5		11,697.00
	GS	12/09	Bonus	1,847.00
	GS	12/07	Bonus	1,750.00
	GS	12/06	Bonus	2,552.00
	GS	12/05	Bonus	1,653.00
	GS	12/04	Bonus	1,604.00
	GS	12/04	Bonus	2,406.00
	GS	12/02	Bonus	2,261.00
	GS	12/01	Bonus	2,188.00
	GS	12/01	Bonus	1,458.00
Total Employees/Awards by Grade		9		17,719.00

Office	Pay Plan	Grade	Award Type	Award Amount
	GS	11/02	Bonus	1,257.00
Total Employees/Awards by Grade		1		1,257.00
	GS	09/08	Bonus	1,240.00
	GS	09/07	Bonus	1,207.00
Total Employees/Awards by Grade		2		2,447.00
	GS	07/03	Bonus	877.00
Total Employees/Awards by Grade		1		877.00
	WS	04/05	Bonus	1,803.00
Total Employees/Awards by Grade		1		1,803.00
	WL	06/04	Bonus	1,526.00
	WL	06/02	Bonus	1,414.00
Total Employees/Awards by Grade		2		2,940.00
	WG	06/05	Bonus	1,439.00
	WG	06/05	Bonus	1,439.00
	WG	06/03	Bonus	1,337.00
	WG	06/02	Bonus	1,285.00
	WG	06/01	NA*	-
Total Employees/Awards by Grade		5		5,500.00
Transportation Security Laboratory	GS	15/10	Bonus	4,470.00
	GS	15/10	Bonus	2,980.00
	GS	15/10	Bonus	4,470.00
	GS	15/10	Bonus	2,980.00
	GS	15/09	Bonus	5,805.00
	GS	15/08	Bonus	4,240.00
	GS	15/08	QSI	-
	GS	15/08	Bonus	2,827.00
	GS	15/07	Bonus	2,750.00
	GS	15/07	Bonus	5,501.00
	GS	15/07	Bonus	2,750.00
	GS	15/06	Bonus	4,011.00
	GS	15/06	Bonus	1,337.00
	GS	15/06	Bonus	2,674.00
	GS	15/05	Bonus	4,396.00
	GS	15/02	Bonus	1,184.00
Total Employees/Awards by Grade		16		52,375.00
	GS	14/10	Bonus	1,767.00
	GS	14/10	Bonus	2,533.00
	GS	14/10	Bonus	1,267.00
	GS	14/10	Bonus	2,533.00
	GS	14/09	Bonus	1,234.00
	GS	14/09	Bonus	2,468.00
	GS	14/09	Bonus	2,468.00
	GS	14/09	Bonus	4,202.00
	GS	14/09	Bonus	2,468.00
	GS	14/08	Bonus	1,202.00
	GS	14/07	Bonus	1,169.00
	GS	14/07	Bonus	1,169.00

Office	Pay Plan	Grade	Award Type	Award Amount
	GS	14/07	Bonus	3,507.00
	GS	14/06	Bonus	2,273.00
	GS	14/06	Bonus	1,137.00
	GS	14/06	Bonus	2,273.00
	GS	14/05	Bonus	3,312.00
	GS	14/05	Bonus	4,412.00
	GS	14/02	Bonus	1,007.00
	GS	14/02	Bonus	3,020.00
Total Employees/Awards by Grade		20		45,421.00
	GS	13/08	Bonus	2,034.00
	GS	13/07	Bonus	989.00
	GS	13/07	Bonus	2,968.00
	GS	13/07	Bonus	1,979.00
	GS	13/06	Bonus	962.00
	GS	13/06	Bonus	962.00
	GS	13/05	Bonus	2,803.00
	GS	13/04	Bonus	907.00
	GS	13/03	Bonus	3,508.00
	GS	13/03	Bonus	1,759.00
Total Employees/Awards by Grade		10		18,871.00
	GS	11/07	Bonus	2,082.00
	GS	11/05	Bonus	1,967.00
	GS	11/04	Bonus	1,273.00
	GS	11/03	Bonus	1,734.00
Total Employees/Awards by Grade		4		7,056.00
	GS	09/06	Bonus	558.00
	GS	09/06	Bonus	558.00
	GS	09/05	Bonus	542.00
Total Employees/Awards by Grade		3		1,658.00
	GS	08/03	Bonus	923.00
Total Employees/Awards by Grade		1		923.00
Environmental Measurement Laboratory	GS	15/10	Bonus	4,470.00
	GS	15/08	Bonus	4,460.00
	GS	15/07	Bonus	5,739.00
	GS	15/06	QSI	-
	GS	15/04	Bonus	3,978.00
Total Employees/Awards by Grade		5		18,647.00
	GS	14/08	Bonus	1,764.00
	GS	14/07	Bonus	3,689.00
	GS	14/06	Bonus	3,996.00
	GS	14/06	Bonus	4,086.00
Total Employees/Awards by Grade		4		13,535.00
	GS	13/10	Bonus	1,627.00
	GS	13/09	Bonus	2,197.00
	GS	13/08	Bonus	3,209.00
	GS	13/05	Bonus	2,948.00
	GS	13/05	Bonus	3,448.00

Office	Pay Plan	Grade	Award Type	Award Amount
Total Employees/Awards by Grade		5		13,429.00
	GS	12/10	Bonus	948.00
	GS	12/09	Bonus	3,271.00
	GS	12/08	Bonus	899.00
	GS	12/07	Bonus	875.00
	GS	12/06	Bonus	851.00
	GS	12/02	Bonus	2,261.00
Total Employees/Awards by Grade		6		9,105.00
	GS	11/10	Bonus	791.00
	GS	11/10	Bonus	2,373.00
	GS	11/08	Bonus	2,251.00
Total Employees/Awards by Grade		3		5,415.00
	GS	09/10	Bonus	654.00
	GS	09/04	Bonus	1,659.00
Total Employees/Awards by Grade		2		2,313.00
	GS	08/10	Bonus	1,776.00
Total Employees/Awards by Grade		1		1,776.00
	GS	07/08	Bonus	1,521.00
Total Employees/Awards by Grade		1		1,521.00
	GS	06/10	Bonus	481.00
Total Employees/Awards by Grade		1		481.00

* NA = person was not eligible for an award or QSI and did not receive one.

Question: Please provide for the record a table that shows all funds expended by S&T political employees for travel in 2008. Include name of individual traveling, purpose of travel, location(s) visited, and total cost.

ANSWER: Please see the following table.

Traveler	Purpose	Location	Cost
Jay Cohen	Speak at Coast Guard's 7th Annual Innovation Expo	NEW ORLEANS,LA	\$623.30
Jay Cohen	Attend Australia Bilateral Mtg; Meet with Australian Homeland Security Official; Speak at 2007 ITEA Conference in Kauai, HI	HONOLULU,HI SYDNEY,AUS CANBERRA,AUS SYDNEY,AUS ISLE OF KAUAI,HI	\$6,342.58
Jay Cohen	Speak and attend International Stakeholders Conference	LONDON,GBR PARIS,FRA	\$4,268.83
Jay Cohen	Meeting with National Science Foundation and ceremony on Antarctic; MOU Signing in Wellington, NZ, and attend S&T Conference in Los Angeles, CA	CHRISTCHURCH,NZL LOS ANGELES,CA	\$4,531.59
Jay Cohen	Attend meetings with French officials at the French Homeland Security Institute	PARIS,FRA	\$3,208.87
Jay Cohen	Attend BHEF Winter 2008 Meeting	MIAMI,FL	\$1,329.88
Jay Cohen	Speak at the OSI Forum on Projects on Defense and Economic Security in the Wider Caribbean Conference	CARTAGENA,COL	\$1,966.35
Jay Cohen	Meet with CEO Xconomy and visit MIT Lincoln Labs	BOSTON,MA	\$598.95
Jay Cohen	Attend meetings at EML and NY Port Authority	MANHATTAN,NY	\$230.95

Jay Cohen	Speak at Navy League Dinner in Kings Bay, GA	KINGS BAY NSB,GA	\$707.45
Jay Cohen	Speak at SPIE Defense and Security Symposium	ORLANDO,FL	\$845.58
Jay Cohen	Meeting with Israeli Homeland Security Officials	TEL AVIV.ISR	\$68.50
Jay Cohen	Site Visit NREL/NOAA	DENVER.CO	\$1,094.08
Jay Cohen	Site Visit to Los Alamos National Laboratory	SANTA FE,NM	\$858.93
Jay Cohen	Attend meetings with Director of Petrochemical Transportation Security Ctr of Excellence at Texas Southern University and Speak at Azalea Symposium in Norfolk, VA	HOUSTON,TX NORFOLK,VA	\$1,161.67
Jay Cohen	To attend the UK-US Homeland Security Science and Technology Treaty Bilateral Meeting	LONDON,GBR	\$2,230.67
Jay Cohen	Attend USCG Academy Presentations, Attend Tech Fair with Congresswoman Gifford in Tucson, AZ	NEW LONDON,CT TUCSON,AZ	\$1,320.29
Jay Cohen	Site Visit/Meetings at The National Institute For Hometown Security with Congressman Rogers	LEXINGTON,KY	\$849.71
Jay Cohen	Attend All Hands Meeting at Plum Island	OLD SAYBROOK,CT	\$394.95
Jay Cohen	Meet with Israel Homeland Security Officials	TEL AVIV.ISR	\$5,406.55
Jay Cohen	Speak at MORS Symposium at USCGA in Groton, CT	GROTON,CT	\$986.68
Jay Cohen	Site Visit at Penn State Lab Electro Optics Center	STATE COLLEGE,PA	\$1,171.95
Jay Cohen	Speak at US Fleet Forces Commander's Conference	SAN DIEGO,CA	\$674.45
Jay Cohen	Visit Lab with US Knight from USDA	WINNIPEG,CAN	\$1,855.80
Jay Cohen	Attend Commissioning of the HTS Cable in Long Island, NY	ISLANDIA,NY	\$416.44
Jay Cohen	Attend Bilateral meetings in Stockholm	STOCKHOLM,SWE	\$5,027.16
Jay Cohen	Attend Inaugural Event for DHS National Center of Excellence for Maritime, Island and Port Security	NEWARK,NJ	\$821.52
Jay Cohen	Speak at Pacific Operations S&T Conference. Attend meetings at Kodak in Rochester, NY	HONOLULU,HI ROCHESTER,NY	\$3,023.69
Jay Cohen	Site Visit Pirbright Laboratory to review research on Foot & Mouth Disease with USDA U/S Knight	LONDON,GBR	\$1,890.57
Jay Cohen	Speak at S&T Conference in Ft. Leonard Wood.	FT. LEONARD WOOD,MO	\$1,146.70
Jay Cohen	Attend University of Texas El Paso Ribbon cutting with Congressman Reyes	EL PASO,TX	\$896.35
Jay Cohen	Attend meetings with Senator Collins at University of Maine, Bangor, and Bath, ME	PORTLAND,ME	\$1,327.58
Jay Cohen	Attend Ribbon Cutting Ceremonies at Centers of Excellence in NC and AZ	CHAPEL HILL,NC TUCSON,AZ	\$2,020.63
Jay Cohen	Participate in Filming of demo with ConEd in New York. Speak at Future Security Conference in Karlsruhe; meet with homeland security officials in Berlin	MANHATTAN,NY STUTT GART,FRG BERLIN,FRG	\$4,278.78
Jay Cohen	Meet with Homeland Security Officials in Burbank, CA and Ketchikan, AK	LOS ANGELES,CA KETCHIKAN,AK	\$1,860.49
Jay Cohen	Attend Levee Breach Demo in Stillwater, OK	OKLAHOMA CITY,OK	\$29.95
Jay Cohen	LOCAL TRAVEL	LOCAL TRAVEL	\$18.00
Jay Cohen	LOCAL TRAVEL	LOCAL TRAVEL	\$35.00
Jay Cohen	LOCAL TRAVEL	LOCAL TRAVEL	\$10.00
Jay Cohen	LOCAL TRAVEL	LOCAL TRAVEL	\$59.67
Jay Cohen	LOCAL TRAVEL	LOCAL TRAVEL	\$81.00
Jay Cohen	LOCAL TRAVEL	LOCAL TRAVEL	\$32.00
	Total for Jay Cohen		\$65,704.09
Lesley Randolph	NONE	NONE	NONE

Total for Lesley Randolph			\$0.00
Caroline Whitfield	Attend Australia Bilateral Meetings	SYDNEY,AUS CANBERRA,AUS SYDNEY,AUS CHICAGO,IL	\$4,984.65
Total for Caroline Whitfield			\$4,984.65
Michael B. Smith	To attend SpecOps East 2007 Warfighter Symposium & Expo	CHARLOTTE,NC	\$1,026.82
Michael B. Smith	To attend technology meetings at GELTech Solutions, Jupiter FL	WEST PALM BEACH,FL	\$775.68
Michael B. Smith	Attend 1st Responder Exercise-Northeastern event at Monmouth University Rapid Response Institute	FT. MONMOUTH,NJ	\$64.72
Michael B. Smith	Visit NETC and receive briefings	FREDERICK,MD	\$73.72
Michael B. Smith	Meet with the Adjutant General of Delaware	WILMINGTON,DE	\$125.64
Michael B. Smith	Attend and present panel at West Coast Stakeholders' Conference	LOS ANGELES,CA	\$1,498.94
Michael B. Smith	Attend 2008 Annual Chemical and Biological R&D Technologies Conference	SAN ANTONIO,TX	\$1,496.34
Michael B. Smith	Meet with FEMA Region II Administrator; Meet with Ft. Monmouth Community Force Protection Council	FT. MONMOUTH,NJ	\$65.22
Michael B. Smith	Attend SMART "ULSS" Forum	PITTSBURGH,PA	\$696.78
Michael B. Smith	Visit FEMA Region V Administrator/staff	CHICAGO,IL	\$937.44
Michael B. Smith	Present S&T Overview to Wayne Co PA Director of Emergency Mgt. Present STEM briefing at Honesdale PA High School	SCRANTON,PA	\$326.69
Michael B. Smith	Attend Strengthening Mid Atlantic Region for Tomorrow (SMART)States' House of Representatives Speakers Conference	PHILADELPHIA,PA	\$236.06
Michael B. Smith	Attend Eastern Division International Association of Fire Chiefs Conference	PA	\$679.07
Michael B. Smith	Attend meeting with Executive Director of World Cares Center	MANHATTAN,NY	\$34.00
Michael B. Smith	Give presentations at WI Homeland Security Council and WI NG Headquarters	MADISON,WI	\$962.23
Michael B. Smith	Attend 2008 Emergency Management Conference	BERGEN COUNTY,NJ	\$598.30
Michael B. Smith	Attend 2d Annual Cross-Border Public Health Preparedness Conference at WV University	MORGANTOWN,WV	\$461.28
Michael B. Smith	Attend PSA-USTRANSCOM CIP meeting	CHICAGO,IL	\$1,129.68
Michael B. Smith	Attend AMTRAC meeting at TSL	ATLANTIC CITY,NJ	\$99.94
Michael B. Smith	Attend Wisconsin Security Research Consortium 2008 Resource Rendezvous in Madison WI	MADISON,WI WI MADISON,WI	\$1,308.44
Michael B. Smith	Attend PA Emergency Management Conference	STATE COLLEGE,PA	\$625.20
Michael B. Smith	Attend National Guard Association of the United States 130th Annual Conference	BALTIMORE CITY,MD	\$883.12
Michael B. Smith	ePortation technology demonstration, Balt/wash airport	BALTIMORE CITY,MD	\$60.53
Michael B. Smith	Attend 2007 USCG Innovation Exposition	NEW ORLEANS, LA	\$1,094.24
Michael B. Smith	Three presentations to the student body	NEW MONMOUTH, NJ	\$63.21
Michael B. Smith	Rapid Research Institute review of FEMA region II	NEW MONMOUTH, NJ	\$67.09
Michael B. Smith	Site visit to west coast ops. area	SACRAMENTO, CA	\$1,309.62
Michael B. Smith	Tech meeting at GELtech Solutions	JUPITER, FL	\$27.25
Michael B. Smith	Attend Precision Airdrop Technology Conference & Demo	YUMA, AZ	\$1,395.05
Michael B. Smith	LOCAL TRAVEL	LOCAL TRAVEL	\$108.24

Michael B. Smith	LOCAL TRAVEL	LOCAL TRAVEL	\$42.68
Michael B. Smith	LOCAL TRAVEL	LOCAL TRAVEL	\$51.09
Michael B. Smith	LOCAL TRAVEL	LOCAL TRAVEL	\$152.69
Michael B. Smith	LOCAL TRAVEL	LOCAL TRAVEL	\$30.67
Michael B. Smith	LOCAL TRAVEL	LOCAL TRAVEL	\$50.04
Michael B. Smith	LOCAL TRAVEL	LOCAL TRAVEL	\$18.30
Michael B. Smith	LOCAL TRAVEL	LOCAL TRAVEL	\$33.34
Michael B. Smith	LOCAL TRAVEL	LOCAL TRAVEL	\$58.28
Michael B. Smith	LOCAL TRAVEL	LOCAL TRAVEL	\$59.39
Michael B. Smith	LOCAL TRAVEL	LOCAL TRAVEL	\$42.68
Michael B. Smith	LOCAL TRAVEL	LOCAL TRAVEL	\$33.95
Michael B. Smith	LOCAL TRAVEL	LOCAL TRAVEL	\$24.80
Michael B. Smith	LOCAL TRAVEL	LOCAL TRAVEL	\$59.89
Michael B. Smith	LOCAL TRAVEL	LOCAL TRAVEL	\$16.00
Michael B. Smith	LOCAL TRAVEL	LOCAL TRAVEL	\$40.40
Michael B. Smith	LOCAL TRAVEL	LOCAL TRAVEL	\$89.64
Michael B. Smith	LOCAL TRAVEL	LOCAL TRAVEL	\$33.95
Total for Michael B. Smith			\$19,068.33
Anthony Correale	To attend conference for international programs	QUEBEC,CAN	\$2,209.74
Anthony Correale	Counter Terrorism Training	FT. GEORGE G. MEADE,MD	\$726.16
Anthony Correale	LOCAL TRAVEL	LOCAL TRAVEL	\$23.00
Anthony Correale	LOCAL TRAVEL	LOCAL TRAVEL	\$93.00
Anthony Correale	LOCAL TRAVEL	LOCAL TRAVEL	\$105.00
Anthony Correale	LOCAL TRAVEL	LOCAL TRAVEL	\$91.00
Anthony Correale	LOCAL TRAVEL	LOCAL TRAVEL	\$50.15
Anthony Correale	LOCAL TRAVEL	LOCAL TRAVEL	\$57.58
Anthony Correale	LOCAL TRAVEL	LOCAL TRAVEL	\$141.75
Total for Anthony Correale			\$3,497.38
Bradley Buswell	Attend NDIA Innovative Technologies Conference (Trip Cancellation Fee)	LOS ANGELES,CA	\$27.25
Bradley Buswell	Site Visit to Federal Law Enforcement Training Center with Under Secretary S&T	JACKSONVILLE,FL	\$788.20
Bradley Buswell	Site Visit NREL/NOAA	DENVER,CO	\$835.33
Bradley Buswell	Speak at Annual Arizona Nontechnology Conference	PHOENIX,AZ	\$1,683.25
Bradley Buswell	LOCAL TRAVEL	LOCAL TRAVEL	\$40.00
Total for Bradley Buswell			\$3,374.03
TOTAL			\$96,628.48

Question: Please list the number, by office and pay grade level, of all S&T employees hired non-competitively in fiscal year 2008.

ANSWER: Please see the following table.

2008 Non-Competitive Appointments			
Office	Pay Grade Level	Number	Authority
Innovation/HISARPA	AD Term	3	Section 307(b)(6), Homeland Security Act

2008 Non-Competitive Appointments			
Office	Pay Grade Level	Number	Authority
Innovation/HSARPA	ST Career	1	5 USC 3325
Research	ST Career	2	5 USC 3325
Office of the Under Secretary	ST Career	1	5 USC 3325
Transition	ST Career	1	5 USC 3325
Human Factors	ST Career	1	5 USC 3325

Contracts

Question: Please provide for the record, the number of noncompetitive contracts S&T has entered into in fiscal year 2008, what is anticipated in 2009 and 2010, and an explanation as to why a non-competitive contract was chosen. As part of this response, please clearly delineate other transactional agreements and those purchases made from the GSA approved listings.

ANSWER: The Office of Procurement Operations (OPO) awarded 34 new, non-competitive contracts in Fiscal Year (FY) 2008. These contracts were awarded because only one source was deemed capable of providing the supply or service, and no other type of supply or service could satisfy agency requirements, in accordance with Federal Acquisition Regulation (FAR) 6.302-1.

To date in FY 2009, OPO has awarded 18 new non-competitive contracts on behalf of the S&T Directorate. Of the 18 non-competitive actions, all actions are expected to be contracts; none are other transactions or GSA orders.

To date, DHS has not gathered forecast information for new non-competitive contracts anticipated in FY 2010; that data will be gathered in the fourth quarter of FY 2009 and made available in October 2009. The OPO Contracting Officer, upon receipt of the procurement documentation, may determine that a contract originally anticipated to be a sole source may or should be awarded competitively under the GSA schedules. Additionally, non-competitive actions over \$500,000 must be approved by the OPO Competition Advocate; actions over \$10 million must be approved by the OPO Director/Head of Contracting Activity; and actions over \$50 million must be approved by the DHS Chief Procurement Officer (CPO).

FAR Part 6 provides seven exceptions to the use of full and open competition:

- Only one responsible source; and no other supplies or services will satisfy agency requirements
- Unusual and compelling urgency;
- Industrial, mobilization; engineering, developmental, or research capability; or expert services;
- International agreement;
- Authorized or required by statute;
- National security; and
- Public interest.

Question: In total, how much of your awards are competitive? Please answer in dollar amount and percentage.

ANSWER: In Fiscal Year (FY) 2008, the Office of Procurement Operations competitively awarded 158 contracts on behalf of the S&T Directorate. The 158 actions had a total dollar value of \$163,840,329, which is 94.7 percent of the contracts awarded for the S&T Directorate in FY 2008.

Question: Update and submit, through the most recent month available, the list provided in last year's hearing record (2009, Part 2, pages 654-661) regarding Sole Source Contracts. Organize by contractor, purpose, appropriation account, dollar award, full performance value, contract start date, contract end date, and reason for sole-source.

ANSWER: The table that follows lists new, sole source contracts initiated in FY 2008.

CONTRACTOR	PURPOSE	APPROPRIATION ACCOUNT	TOTAL OBLIGATION (DOLLAR VALUE)	TOTAL AMOUNT (FULL PERFORMANCE VALUE)	START DATE	END DATE	REASON NOT COMPETED
JOHNSON CONTROLS, INC.	Funding for a preventive maintenance agreement of the card key reader P1500 security system.	Laboratory Facilities	\$4,251	\$4,251	07/01/2008	06/30/2009	Only One Source - Other
DYNO NOBEL INC.	Funding to purchase ammonium nitrate based and nitroglycerin based commercial explosives for TSL Operations.	Laboratory Facilities	\$5,268	\$5,268	06/04/2008	08/03/2008	Unique Source
PERKINELMER LAS, INC	Funding for a preventive maintenance service agreement for the Liquid Scintillation Analyzer Model 2250CA-Tri Carb.	Laboratory Facilities	\$5,421	\$5,421	06/18/2008	06/30/2009	Only One Source - Other
AMERICAN ASSOCIATION FOR LAB	Funding for In-House Training.	Test and Evaluation	\$6,530	\$6,530	06/27/2008	09/26/2008	Only One Source - Other
SUPERIOR COMMUNICATIONS, INC.	Funding to purchase a radio system for the Department of Homeland Security (DHS) National Biodefense Analysis and Countermeasures Center (NBACC).	Laboratory Facilities	\$11,461	\$11,461	09/11/2008	09/11/2009	Follow-on contract
SUFFOLK COUNTY OF	Funding to provide training classes to Plum Island Animal and Disease Center (PIADC) from Suffolk County Fire Academy.	Laboratory Facilities	\$14,575	\$14,575	06/10/2008	09/30/2008	Only One Source - Other
NATIONAL ACADEMY OF SCIENCES	Membership to the National Academies' Division on Engineering and Physical Sciences to support the activities of the Federal Facilities (FFC).	M&A Business Operations	\$20,000	\$20,000	07/16/2008	07/16/2009	Unique Source
ENSIGN-BICKFORD AEROSPACE & DEFENSE COMPANY	Funding to acquire manufactured Primasheet 1000 and Primasheet 2000 explosives for effect testing and evaluation of explosives detection systems.	Laboratory Facilities	\$24,528	\$24,528	06/04/2008	09/02/2008	Unique Source
Environmental Mutagens Society-Default Location	Funding for the Environmental Mutagens Society-Homeland Security Symposium.	Chemical & Biological	\$25,000	\$25,000	7/17/2008	Oct-08	Only One Source - Other

CONTRACTOR	PURPOSE	APPROPRIATION ACCOUNT	TOTAL OBLIGATION (DOLLAR VALUE)	TOTAL AMOUNT (FULL PERFORMANCE VALUE)	START DATE	END DATE	REASON NOT COMPETED
SUPERIOR COMMUNICATIONS, INC.	Funding to purchase hand held radios, batteries, and battery chargers for Department of Homeland Security (DHS) National Biodefense Analysis and Countermeasures Center (NBACC).	Laboratory Facilities	\$31,458	\$31,458	09/25/2008	09/30/2009	Only One Source - Other
TRANSITCENTER, INC.	Federal employee commuter mass transit subsidy benefits program. TransitChek vouchers for employees at the Environmental Measurements Laboratory (EML) located in New York, New York.	Lab Facilities	\$43,764	\$43,764	12/06/2007	11/30/2008	Only One Source - Other
NATIONAL DEFENSE INDUSTRIAL ASSOCIATION	Funding for DHS stakeholder conference in Los Angeles, C.A.	M&A Business Operations	\$46,500	\$46,500	01/07/2008	01/30/2008	Only One Source - Other
Gyphon Scientific-Default Location	Funding for the Commercial DNA Synthesis System Analysis	Chemical & Biological	\$49,561	\$49,561	7/17/2008	11/17/2008	Only One Source - Other
NATIONAL ACADEMY OF SCIENCES	Funding for the Disasters Roundtable (DR) effort.	Infrastructure Geophysical	\$65,000	\$65,000	09/03/2008	08/31/2009	Only One Source - Other
Safe Environment Engineering (SEE)-Default Location	Funding for Integrated Chemical, Biological, Radiological, Nuclear, Explosive Detection System Pilot Demonstrations.	Chemical & Biological	\$70,155	\$70,155	8/15/2008	8/15/2009	Only One Source - Other
XCONOMY INC	Xconomy services for Tech Share and other DHS S&T directorates	Transition	\$75,000	\$75,000	10/01/2007	09/30/2009	Unique Source
National Academy of Sciences-Default Location	Funding for the Forum on Microbial Threats.	Chemical & Biological	\$75,000	\$75,000	9/3/2008	9/3/2009	Only One Source - Other
GOLDBELT RAVEN LLC	IT hardware/software for Plum Island Animal Disease Center	Chemical & Biological	\$78,647	\$78,647	06/15/2008	08/14/2009	Only One Source - Other
ENSCO INC	Theoretical Chemistry Analysis of Ion Mobility Spectrometry	Chemical & Biological	\$169,784	\$169,784	08/13/2008	06/30/2009	Unique Source
HALCYON PRODUCTS, INC.	Fire Ground Compass for First Responders	Transition	\$175,120	\$175,120	02/20/2008	8/21/2008	Unique Source
TOPAZ TECHNOLOGIES LTD	IT hardware/software for Plum Island Animal Disease Center	Chemical & Biological	\$223,120	\$223,120	06/25/2008	06/24/2009	Only One Source - Other
TRANSBOUNDARY ANIMAL BIOLOGICS, INC.	Enhancing the availability of veterinary biologics for transboundary diseases	Chemical & Biological	\$259,700	\$259,700	08/15/2008	09/30/2009	Unique Source
MILLER ENVIRONMENTAL GROUP INC.	Funding to purchase fuel remediation services.	Laboratory Facilities	\$291,807	\$291,807	03/01/2008	02/28/2010	Only One Source - Other

CONTRACTOR	PURPOSE	APPROPRIATION ACCOUNT	TOTAL OBLIGATION (DOLLAR VALUE)	TOTAL AMOUNT (FULL PERFORMANCE VALUE)	START DATE	END DATE	REASON NOT COMPLETED
BT SAFETY LLC	Chemical, Biological, and Radiological Risk Assessment Support.	Chemical & Biological	\$480,000	\$480,000	08/15/2008	08/14/2009	Unique Source
US Army Corps of Engineers (USACE)-Default Location	Funding to purchase Two KeyWatcher Illuminated Systems with locking slots for the NBACC Security Office.	Laboratory Facilities	\$521,406	\$521,406	9/30/2008	9/29/2009	Only One Source - Other
ANSI-ASQ NATIONAL ACCREDITATION BOARD, LLC	Funding for the private sector preparedness voluntary accreditation and certification program.	T&E Standards	\$899,861	\$899,861	06/12/2008	06/11/2009	Only One Source - Other
NATIONAL ACADEMY OF PUBLIC ADMINISTRATION INC	Government-Wide Homeland Security Research Study	Transition	\$975,000	\$975,000	06/10/2008	06/09/2009	Authorized by Statute
MCCONNELL GROUP, INC. THE	Scientific/Technical Support for DHS Scientific Programs at the Plum Island Animal Disease Center (PIADC)	Chemical & Biological	\$1,007,510	\$1,007,510	05/14/2007	02/14/2010	Unique Source
Modern Technology Solutions, Inc.-Default Location	Additional support for Unmanned System Technology	Borders & Maritime	\$1,404,158	\$1,404,158	1/24/2008	2/28/2010	Only One Source - Other
International Association of Firefighters-Default Location	Development of New pressure vessel for emergency responder self contained breathing apparatus	Transition	\$2,000,077	\$2,000,077	7/1/2008	10/2/2009	Only One Source - Other
ELECTRIC POWER RESEARCH INSTITUTE, INC.	Recovery Transformer (Rec X)	Infrastructure Geophysical	\$2,800,000	\$2,800,000	09/30/2008	05/31/2009	Unique Source

Question: Please provide for the record a list of all contracts over \$1 million in total value executed by S&T in 2008. Organize by contractor, purpose, dollar award, full performance value, contract start date, contract end date, and contract type (e.g., firm fixed price, etc.).

ANSWER: Please see the following table.

CONTRACTOR	PURPOSE	TOTAL OBLIGATION (DOLLAR AWARD)	TOTAL AMOUNT (FULL PERFORMANCE VALUE)	START DATE	END DATE	CONTRACT AWARD TYPE
SCIENCE APPLICATIONS INTERNATIONAL CORPORATION	TIGER Assays Novel, Emerging and Engineered Threats	\$1,000,271	\$1,000,271	01/25/2008	01/24/2010	Cost-plus-fixed-fee
CACI-WGI, INC.	Information Sharing Capstone Integrated Product Team Engineering and Transition Support	\$1,008,518	\$1,008,518	05/27/2008	05/26/2009	Delivery / Task Order
MOTOROLA, INC.	Provide Motorola radios and accessories to VTA, EML, TSL, PIADC using the U.S. Secret Service Motorola Contract HSS01-06-D-0005. S&T's Motorola ID # is 1036476150.	\$1,329,611	\$1,329,611	09/19/2008	09/19/2009	Delivery / Task Order
LOCKHEED MARTIN CORPORATION	HITS: Tunnel Detection Technologies Project	\$1,530,251	\$1,530,251	02/01/2008	07/31/2009	Cost-plus-fixed-fee

CONTRACTOR	PURPOSE	TOTAL OBLIGATION (DOLLAR AWARD)	TOTAL AMOUNT (FULL PERFORMANCE VALUE)	START DATE	END DATE	CONTRACT AWARD TYPE
INTERNATIONAL ASSOCIATION OF FIREFIGHTERS	Development of New pressure vessel for emergency responder self contained breathing apparatus	\$2,000,028	\$2,000,028	07/01/2008	10/02/2009	Fixed-price
ELECTRIC POWER RESEARCH INSTITUTE, INC.	EPRI - Electric Power Research Institute; Recovery Transformer Program	\$2,800,000	\$2,800,000	09/30/2008	05/31/2009	Cost-sharing
BOEING COMPANY, THE	HIPS:SAFECON	\$2,810,052	\$2,810,052	04/15/2008	04/14/2010	Cost-plus-fixed-fee
THALES COMMUNICATIONS, INC.	Thales - Communication Devices - Delivery of LRIP radios for DHS Pilot Tests. Delivery of EDM verification test report.	\$6,275,000	\$6,275,000	02/22/2008	08/22/2009	Fixed-price
AMERICAN SUPERCONDUCTOR CORPORATION	REG Planning & Technology Demonstration. Physical Design Package-E75th Substation Complete, 50 meter HTS cable demonstration testing completed, Completion of Phase II Demonstration, Phase III Review, Award of Phase III, Program Review #9	\$6,492,194	\$6,492,194	01/23/2008	09/30/2010	Cost-sharing
NORTHROP GRUMMAN SYSTEMS CORPORATION	HIPS: Project CHLOE Concept & Prototype Development	\$6,645,971	\$8,126,461	11/12/2007	07/11/2009	Cost-plus-fixed-fee

Question: Please provide for the record a list of all S&T contracts, grants and other transactions where work is performed outside of the United States. Organize by contractor, purpose, dollar award, full performance value, contract start date, and contract end date.

ANSWER: Please see the following table.

Contractor	Purpose	Total Obligation (Dollar Award)	Total Amount (Full Performance Value)	Contract Start Date	Contract End Date
CEIA USA, LLC	The purpose of this purchase requisition is to provide funding for the Non-Metallic Cargo Screening Transportation Security Laboratory. Due to the urgency to develop this capability, S&T has specified rapid prototype development or modifications of COTS capable devices to meet or beat the 120 day delivery requirement allowing the integration of performance testing and evaluation of the selected units in Canada by Transport Canada.	\$598,950	\$598,950	12/18/2008	12/14/2009
REED EXHIBITIONS LIMITED	The purpose of this procurement action is to fund the fee for S&T to exhibit and participate in the International Security National Resilience (ISNR) Conference to be held in London during December 4-5, 2007.	\$73,601	\$73,601	06/28/2007	12/15/2007
The General Environmental Technos Co	Environmental Measurements Laboratory (EML) requested the General Environmental Technos Co to remove the EML sampling equipment located at the Meteorological Research Institute in Ryori, Japan.	\$1,719	\$1,719	09/14/2007	09/13/2008
THE CHAMELEON GROUP INCORPORATED	Seminar: Behind The Scene's Seminar of Israel's Counter-Terrorism and Security Operations.	\$9,750	\$9,750	2/9/2008	2/16/2008

QUESTIONS FOR THE RECORD SUBMITTED BY

THE HONORABLE HAROLD ROGERS

Acting Under Secretary Bradley Buswell
Developing and Transitioning Homeland Security
Research Products Into Use

Container Security Device

Question: In spite of multiple years of funding, S&T has yet to produce a viable Container Security Device (CSD). Please detail the progress made in developing both the CSD and the Advanced Container Security Device (ACSD) and indicate when S&T and CBP expect the CSD and ACSD to be fielded.

ANSWER: Container Security Device (CSD): In FY 2008, two vendors, Science Applications International Corporation (SAIC) and Georgia Tech Research Institute, delivered 20 Container Security Device (CSD) prototypes, which the S&T Directorate evaluated and tested. Both prototypes showed promising results during testing. However, some deficiencies were discovered in functional operations, as well as in environmental operations. The S&T Directorate is working with the two vendors to address the deficiencies and to couple the devices with a global communications system known as the Marine Asset Tag Tracking System), which is a separate development effort. In late FY 2009 and FY 2010, each vendor will submit an improved CSD for further testing. Upon completion of successful testing, the S&T Directorate will transition the CSD test and evaluation assessments and finalized specifications to DHS Customs and Border Protection and DHS Policy.

Advanced Container Security Device (ACSD): In FY 2008, the S&T Directorate received 40 ACSD prototypes for testing from two vendors, SAIC and L-3 communications. The S&T Directorate determined that the L-3 prototypes did not meet the minimum specifications and did not further pursue them. The SAIC prototypes showed promising results and were pursued. In FY 2009, the SAIC prototypes will require further algorithm development prior to full testing and evaluation. In FY 2010, the final prototypes are expected to be delivered and in FY 2011, final field testing and evaluation will be completed prior to transition of the ACSD standards.

Countering IEDs

Question: DHS has focused a good deal of attention on developing methods to prevent the use and limit the consequences of IEDs in the domestic setting through a research initiative within S&T and through first responder grants. Please indicate what S&T has accomplished thus far under this initiative.

ANSWER: Accomplishments under this initiative include:

- Established within the S&T Directorate a Program Executive Office for Countering Improvised Explosive Devices (C-IED) to coordinate C-IED activities across the S&T Directorate and with outside organizations. The Program Executive Officer serves as one of the co-chairs of the National Science and Technology Council Subcommittee on Domestic IEDs.
- Collaborated with representatives from Federal Government research and development organizations to publish Research Challenges in Combating the Terrorist Use of Explosives in the United States.

Continued collaboration will lead to a coordinated C-IED roadmap that will guide DHS S&T C-IED research.

Person-borne Improvised Explosive Devices (PBIED) Detection Project

- Developed a backscatter x-ray based system with the capability of providing whole body imaging capabilities with effective detection metrics with the highest possible throughput. Preliminary tests of the prototype system were largely successful. The system is currently undergoing more extensive operational tests and evaluations. Several S&T Directorate stakeholders expressed interest in deploying this system upon completion of the ongoing evaluations. This equipment offers the stakeholder a means of searching individuals without direct contact and in real-time.
- Developed a walkthrough detection portal to collect and identify trace explosives on people more efficiently than conventional trace detection portals. Detection is based upon Mass Spectrometry, which has long been acknowledged as superior to the Ion Mobility Spectrometer used in conventional portals. Additionally, the improved system uses a series of doors to aid in the collection of explosive particles and vapors. Several S&T Directorate stakeholders expressed interest in deploying this system as it offers them the capability of screening people for explosive traces without directly contacting them.

Vehicle-Borne Improvised Explosive Devices (VBIED) Detection Project

- Conducted two assessments of technology to screen for VBIEDs and conducted an assessment of the feasibility of vibrometry-based VBIED screening. The assessment established the feasibility of the vibrometry-based approach, but a field demonstration of the prototype system produced less than favorable results. The second technology assessed was a neutron-based technology for domestic VBIED screening. The S&T Directorate established this program to improve screening times and make screening targets safe from collateral radiation. Although the neutron-based screening technology needs further refinements, such a technology would allow S&T Directorate stakeholders to screen large trucks or box vans for explosive threats without the time consuming process of unloading their contents.

Standoff Technology Integration and Demonstration Program

- Field tested technology designed to accelerate the development of integrated standoff and remote countermeasure architectures in crowd situations such as large public events and mass transit facilities. The 2008 field test took place at the Toyota Center, a 6,000-seat, multipurpose arena in Kennewick, Washington. Though not as large as an urban arena, the venue represented the characteristics of a large public event: dynamic crowd flows with crowd density effects and multiple approaches. Testers used infrared cameras and a millimeter wave radar system to detect concealed objects. These two technologies integrated via a target dispatch system that allowed testers to track and scan a single person by orthogonal screening systems. An integrated console allowed for sensor control and monitoring by an operator team. Finally, testers deployed video analytics to detect anomalies. In future years, the S&T Directorate will further develop and improve the tested components, and eventually combine into an integrated system. The next demonstration is tentatively scheduled for September 2009.

Prevent/Deter Program

- Established program to support research on terrorism events; understand the relationship between community characteristics and violent extremism; conduct content analyses of extremist group rhetoric; and assess international de-radicalization programs.

Predictive Screening Project

- Conducted research to validate screening behaviors and pre-suicide bombing behaviors that indicate fear of detection. The S&T Directorate expects to transition the initial validation work to the operational screening community by FY 2011.
- Developed pattern extraction tools to identify terrorist-related behaviors. Initial product transitions include geo-behavioral pattern extraction technologies to identify IED targeting patterns from overseas attacks; and anomaly detection technologies that, when used in combination with the existing targeting system, increase screening accuracy in cargo bound for the U.S. This will extend cargo-based pattern extraction technologies to air- and land- border transit portals and applying geo-behavioral pattern extraction technologies to predict potential domestic IED attack locations.

Bomb Assessment and Render Safe

- Collaborated with the Office of Bombing Prevention and the National Bomb Squad Commanders Advisory Board (NBSCAB) to develop two Bomb Squad Strategic Plans, one in 2007 and one in 2008. These plans informed S&T Directorate program development and strategic investment.
- Conducted, with the Technical Support Working Group (TSWG), Critical Incident Response Technology Seminars that focused on refining bomb squad technology requirements and needs. Initiatives that resulted from these efforts include:
 - A research proof-of-concept was developed for a Non-Explosive IED Defeat Tool.
 - Development of a formulation to destroy TNT which utilized a dilute amine solution without burning.
 - Characterization of two vehicle-borne IED disruption tools (data is being validated by testing tools against mock vehicle bombs and will populate an operational database for bomb squads).
 - A Single-sided X-Ray Backscatter system has been delivered in first quarter 2009, and is currently being integrated with a robot and cart delivery system to be complete in 2009.
 - Ten electronic countermeasures systems were distributed to bomb squads across the country. Operational control of these systems has now been transitioned to FBI. Current work with FBI includes development of next generation system for state/local bomb squads.
 - A non-explosive water cannon to counter VBIEDs will be delivered in 2009.
 - A no-water explosive charge to defeat VBIEDs will be delivered in 2009.

Effective Risk Communications Against the IED Threat

- Developing preliminary recommendations for guidelines to government officials and civic leaders on issuing hazard and risk warnings for IED events. The S&T Directorate will deliver the recommendations in FY 2010. Ultimately, this multi-year effort will result in a modeling and simulation-based system for use by government officials, first responders and civic leaders in training and evaluation risk communications strategies for disasters and terrorist events.

Critical Infrastructure Protection Program

- Working with the U.S. Army Corps of Engineers, Engineering Research and Development Center (ERDC) to conduct basic research in the following areas:
 - Blast vulnerability and mitigation for cable stay bridges: conducting blast testing and computational analysis on bridge cables and towers to understand failure mechanisms and develop mitigation strategies.

- Blast vulnerability and mitigation for tunnels: conducting blast testing and computational analysis on mitigation schemes to protect underwater mass transit tunnels constructed with cast iron.
- VBIED and waterborne attacks embankment dams: conducting small- and large-scale blast testing and computational analysis to understand the failure mechanisms of embankment dams subjected to VBIED attacks at the crest of the dam as well as surface and submerged waterside attacks.
- Blast Resistant Materials: identifying and testing new materials to protect high value structures that are likely targets of IED attacks and reduce casualties from blast and shrapnel.
- Kinetic Energy Penetrators: conducting blast testing and computational analysis on mitigation schemes to protect critical infrastructure targets from kinetic energy penetrators, explosively formed projectiles and shaped charges.
- Working to transition solutions in the following areas:
 - Bay Area Rapid Transit (BART) mitigation strategy: in partnership with BART, conducting small-scale blast experiments and computational analysis to design a mitigation strategy to protect a key vulnerability identified in the BART system.
 - Brick Tunnel Analysis: in partnership with ERDC, conducting blast testing and computational analysis to characterize the behavior of brick constructed tunnels under explosive loads for a key mass transit stakeholder.
 - Bridge Design Tool: in partnership with ERDC, developing engineering guidance and design tools for bridge owners, operators and developers to retrofit existing bridges or construct new bridges to meet appropriate security requirements given the existing blast and projectile threat environment.
 - Blast Analysis Tools: in partnership with ERDC, and the Technical Support Working Group (TSWG), developing fast-running numerical models to enable infrastructure owners and operators to estimate the effects of explosive events on critical assets and assess the effectiveness of mitigation measures. Current work focuses on tunnels, bridges, dams and complex urban environments.

THURSDAY, APRIL 23, 2009.

TESTIMONY OF MEMBERS OF CONGRESS

MEMBER REQUESTS

WITNESSES

HON. KEITH ELLISON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MINNESOTA

HON. DEBBIE HALVORSON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

HON. HENRY CUELLAR, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

HON. RUSH D. HOLT, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

OPENING STATEMENT OF CHAIRMAN PRICE

Mr. PRICE. The subcommittee will come to order. Welcome. Today we will be taking testimony from Members of Congress who have asked for project consideration as part of the fiscal year 2010 budget requests for the Department of Homeland Security.

As I have previously stated, the subcommittee earmarks funding within three areas of DHS: for predisaster mitigation, for emergency operations centers, and for bridges that are deemed an obstruction to navigation and must be altered. On occasion the subcommittee earmarks projects outside of these categories, but it is uncommon.

Of course, Members may also make programmatic requests that do not require a specific earmark, we will welcome any suggestions along those lines today as well, and we look forward to the customary input from Members throughout the entire appropriations process.

We look forward to hearing from our Members today, beginning with Congressman Ellison. Keith please step up to the table. Your full written statement will be entered into the record, so I ask that you limit your oral remarks to a five minute presentation.

Before we begin, however, let me ask our Ranking Member, Mr. Rogers, for any comments he wants to make.

Mr. ROGERS. I have no comments.

Mr. PRICE. No comments, so we will proceed.

Keith Ellison, a Member from Minnesota, welcome. Please proceed.

THURSDAY, APRIL 23, 2009.

MEMBER REQUESTS**WITNESS****HON. KEITH ELLISON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MINNESOTA**

Mr. ELLISON. Mr. Chairman, thank you for allowing me to present today, and also let me thank Ranking Member Rogers. I certainly appreciate the opportunity and really appreciate being able to take part in this forum.

I am here today to provide additional details for an earmark request that I have submitted on behalf of the City of Minneapolis. This is a request for \$1 million to build a new emergency operations center in Minneapolis. This new center would provide the needed space and required technology to effectively manage future emergency incidents in Minneapolis, as well as the greater Twin Cities metro area.

In August 2007, we experienced a collapse of the Interstate 35W bridge in Minneapolis, and this dramatic event in which we lost 13 members of our community, and over a hundred people suffered severe injuries, also highlighted the importance of this project.

More importantly I think, this tragedy helped to show the nation that a well-organized emergency response saves lives. Many people thought that more than 13 people would have lost their lives in this tragic incident, but because of the quick emergency response, many people were in fact saved. Of course, every minute and every hour counts when such a tragedy strikes.

The bridge collapse also revealed the shortcomings of the undersized and poorly equipped Minneapolis Emergency Operations Center. I will refer to it as the EOC. The EOC was the command center coordinating the local, state and federal emergency response to the bridge collapse.

The Federal Emergency Management Agency, FEMA, and the United States Fire Administration, USFA, in an after action assessment stated that the current Minneapolis EOC was inadequate to meet the needs of a complex emergency incident. Let me quote from the report:

“The EOC is located in the basement of city hall and is used when a large-scale emergency or disturbance occurs that involves multiple city agencies. The EOC is essentially a single room, which did not have enough space for all of the representatives from the organizations having statutory authority to be present.

“There is not enough room for a policy coordinating group, usually staffed by political and administrative leaders, or for other planning, logistical or public information functions. The inadequate size and functionality of the current EOC was rated by most respondents as the biggest obstacle to management of the response.

“Particularly during the evening of the collapse, the EOC was simply not capable of handling the number of staff and elected officials who reported to the Center.”

I can testify since I was there myself and recognized that we just had a severe space and therefore logistical barrier. My appropriation request will be used to build a new EOC with additional space

and necessary technology to enable emergency personnel more effective management capability to address a broad range of possible emergency incidents throughout the Twin Cities.

The Twin Cities contains the nation's twelfth largest regional economy, and it includes a concentration of critical infrastructure and key resources and, most importantly, boasts a regional population of approximately three million people.

The new EOC is consistent with and supported in the Minnesota Homeland Security strategy, the Twin Cities Urban Area Security Initiative strategy and the Minnesota State Preparedness Report. The final design for the new EOC has been completed, and approximately \$5.6 million in local funds have been identified for the project.

The operating and maintenance budget has been developed and will be secured with city general fund dollars. The federal appropriations request of \$1 million would permit completion of construction by spring of 2010, about a year from now.

Mr. Chairman, in conclusion, I want to thank the entire committee, along with the Ranking Member, for the time and consideration of this important request. Thank you very much.

[The information follows:]

**CONGRESSMAN KEITH ELLISON
STATEMENT BEFORE THE SUBCOMMITTEE ON HOMELAND
SECURITY
APPROPRIATIONS COMMITTEE
ON MINNEAPOLIS EMERGENCY OPERATIONS CENTER
APRIL 23, 2009**

Let me start by thanking Chairman Price and Ranking Member Rogers for providing the forum to make a statement of support for such an important appropriations request.

I am here today to provide additional details for an earmark request that I have submitted on behalf of the City of Minneapolis. This is a request for \$1,000,000 to build a new Emergency Operation Center in Minneapolis. This new center would provide the needed space and required technology to effectively manage future emergency incidents in Minneapolis as well as the greater Twin Cities metro area.

The August 2007 collapse of the Interstate-35W Bridge in Minneapolis showed the nation that a well-organized emergency response saves lives. Thirteen people were killed and over 100 people were injured, but we know that the rapid response of the region's first responders in the minutes and hours that followed the tragedy saved countless lives. The bridge collapse also revealed the shortcomings of the undersized and poorly equipped Minneapolis Emergency Operations Center (EOC). The EOC was the command center coordinating the local, state and federal emergency response to the bridge collapse.

The Federal Emergency Management Agency (FEMA)/United States Fire Administration (USFA), in an after-action assessment, stated that the current Minneapolis EOC was inadequate to meet the needs of a complex emergency incident. Let me quote from the report:

“The EOC is located in the basement of city hall and is used when a large-scale emergency or disturbance occurs that involves multiple city agencies. The EOC is essentially a single room, which did not have enough space for all the representatives from the organizations having statutory authority to be present. There is not enough room for a policy coordinating group, usually staffed by political and administrative leaders, or for other planning, logistical, and public information functions. **The inadequate size and functionality of the current**

EOC was rated by most respondents as the biggest obstacle in the management of the response. Particularly during the evening of the collapse, the EOC was simply not capable of handling the number of staff and elected officials who reported to the center.” (my emphasis)

My appropriations request will be used to build a new EOC with additional space and the necessary technology to enable emergency personnel more effective management capabilities to address a broad range of possible emergency incidents throughout the Twin Cities metropolitan area.

The Twin Cities contains the nation’s twelfth largest regional economy. It includes a concentration of critical infrastructure and key resources and, most importantly, boasts a regional population of approximately three million people.

The new EOC is consistent with, and supported in, the Minnesota Homeland Security Strategy, the Twin Cities Urban Area Security Initiative Strategy, and the Minnesota State Preparedness Report. The final design for the new EOC has been completed, and approximately \$5.6 million in local funds have been identified for the project. The operating and maintenance budget has been developed and will be secured with city general fund dollars.

The federal appropriations request of \$1 million would permit completion of construction by the spring of 2010.

Mr. Chairman, in conclusion, I thank the committee for its time and consideration of this critical appropriations request.

Mr. PRICE. Thank you, Mr. Ellison. We appreciate that testimony.

I have no questions. Do you, Mr. Rogers?

Mr. ROGERS. No questions.

Mr. ELLISON. Thank you.

Mr. PRICE. Thank you very much.

Mr. ELLISON. Have a fine day.

Mr. PRICE. We will next call to our witness table Representative Deborah Halvorson from Illinois, one of our new Members. Ms. Halvorson, please proceed.

THURSDAY, APRIL 23, 2009.

MEMBER REQUESTS

WITNESS

HON. DEBBIE HALVORSON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Ms. HALVORSON. Thank you, Chairman Price, Ranking Member Rogers and Members of the committee. Thank you so much for allowing me to testify today on behalf of my constituents in the 11th Congressional District of Illinois.

I come before you today to ask you for consideration of a \$5 million appropriation for the Central Elementary School in Ottawa, Illinois, for predisaster mitigation. On September 15, 2008, the remainder of Hurricane Ike swept through Illinois, causing severe storms and some of the worst flooding my state had ever seen in decades.

First of all, my district was very much affected. Particularly in the historic city of Ottawa they saw severe damage. Because of the storm, Ottawa residents were evacuated from nursing homes, roads were deemed to be unsafe, falling trees caused further damage, and with destruction throughout the area Ottawa's Central Elementary School was hit particularly hard and experienced a great deal of damage. Central Elementary School houses over 400 fifth and sixth grade students.

The flooding caused two significant and devastating effects on the school, which has prevented students from being able to return to the classroom. First, water damage virtually destroyed the school, making it unsafe environmentally for the children. Second, asbestos was found inside the school building and the soil surrounding the building.

So for the time being, church basements and mobile classrooms throughout the Ottawa community are serving as classrooms for the 400 students, and, as you can imagine, the logistics involved in providing ongoing education has presented numerous challenges on multiple levels.

Local officials have been placed in difficult positions of having to find quick solutions for a very expensive problem. The school board has decided that the best option at this point is to take the entire school and put them in an abandoned WalMart for the next school year until they can find a permanent solution.

The simple fact is that the small community of Ottawa is unable to assume the full financial burden of making sure that the stu-

dents have a location to attend school. The specific amount of money that the school will receive from FEMA is unclear at this point, but it is unlikely that these funds will be adequate for the students to return to the school.

There is a lot of work that needs to take place before we can get our fifth and sixth graders back to a proper classroom to start learning again. We need to make sure that the school is structurally safe, free from toxic materials and that necessary precautions are taken to prevent substantial flood damage in the future. Rebuilding the school in the current location poses a risk to flooding again.

An appropriation of any amount will help provide the critical financial resources needed to either rebuild the school in a location outside the flood plain or rebuild on existing location just somehow to mitigate the risk of future flooding.

So I am grateful to the members of our community that have helped in every way to help the children of Central Elementary School continue their education in these challenging times. The church basements have been converted to classrooms. Parents have volunteered their time and energy and school employees have worked tirelessly, but I ask please that this committee consider funding for Central Elementary School.

Fifth and sixth graders need help, and this is not the time in their life that they should go from church basements to an abandoned WalMart for their schooling.

I really appreciate your time, Chairman Price and Ranking Member Rogers, to help us in this needy time.

[The information follows:]

TESTIMONY OF CONGRESSWOMAN DEBBIE HALVORSON BEFORE THE
COMMITTEE OF APPROPRIATIONS, SUBCOMMITTEE ON HOMELAND
SECURITY

CENTRAL ELEMENTARY SCHOOL FLOOD

APRIL 23, 2008

Chairman Price, Ranking Member Rogers, and Members of the Committee:

Thank you for allowing me to testify today on behalf of my constituents in the 11th Congressional District of Illinois. I come before you today to ask that you consider a \$5,000,000 appropriation for the Central Elementary School in Ottawa, Illinois for pre-disaster mitigation.

On September 15, 2008 the remnants of Hurricane Ike swept through Illinois causing severe storms and some of the worst flooding my state had seen in decades. My district was very much affected, and in particular, the historic city of Ottawa saw severe damage.

Because of the storms, Ottawa residents were evacuated from nursing homes, roads were deemed to unsafe to travel on, and fallen trees caused further damage. With destruction throughout the area, Ottawa's Central Elementary School was hit particularly hard and experienced a great deal of damage due to the flooding.

Central Elementary School houses over 400 5th and 6th grade students. Like many of the schools in Ottawa, Central Elementary is known to have one of the best educational programs in our state. The community advocates for high quality education and strongly supports the school system in Ottawa.

Despite the efforts of volunteers and school employees who worked hard to place sandbags outside the school, over two feet of water flooded Central's campus and buildings when the Illinois River overflowed its banks. Flood waters overwhelmed the building, including the auditorium and classrooms, as water spilled through the foundation and vents.

The flooding also caused two significant and devastating effects on the school which has prevented students from being able to return to the classroom. First, water damage virtually destroyed the school making it an unsafe environment for children, and second, asbestos was found inside the school building and the soil surrounding the building.

After accessing the levels of toxic materials in the building, tests showed contamination by the presence of polynuclear aromatic hydrocarbons (PNA) above Tier 1 standards. This type of soil contamination not only prevents students from resuming classes at

Central Elementary School, but it also makes virtually impossible to repair the existing structure due to mitigation costs.

For the time being, church basements and mobile classrooms throughout the Ottawa community are serving as classrooms for the 400 students of Central Elementary School. As you can imagine, the logistics involved in providing ongoing education has presented numerous challenges on multiple levels. Local officials have been placed in the difficult position of having to find a quick solution to a very expensive problem. The school board has decided that the best option at this point is to house the Central Elementary School students in an abandoned Wal-Mart building while a permanent solution is found.

The simple fact is that the small community of Ottawa is unable to assume the full financial burden of making sure the students of Central Elementary School have a location to attend class. The specific amount of money that the school will receive from FEMA is unclear at this point, but it's unlikely that these funds would be adequate for the students to return to school and all learn under the same roof in a permanent structure.

There is a lot of work that needs to take place before we can get our 5th and 6th graders back into a proper classroom and learning together again. We need to make sure the school is structurally safe, free from toxic materials, and that necessary precautions are taken to prevent substantial flood damage in the future.

An appropriation of any amount will help provide the critical financial resources needed to either rebuild the school in a location outside of the floodplain or rebuild on the existing location in a manner that will mitigate the risk of future floods.

I'm grateful to the members of our community that have reached out and helped the children of Central Elementary School continue their education in these challenging times. Church basements have been converted to classrooms, parents have volunteered their time and energy, and school employees have worked tirelessly to make sure this flood has as little impact as possible on the quality of education being offered to the students afflicted by the flood. I urge the members of the Committee to share in the passion that the community of Ottawa has for its children and quality education. Please appropriate funding for Central Elementary School so they can provide a learning environment our children most definitely deserve.

Mr. PRICE. Thank you very much. Let me just ask you briefly to comment on your current dealings with FEMA. You do have a declaration—

Ms. HALVORSON. Yes, sir.

Mr. PRICE [continuing]. And there is a possible eligibility there. What do you understand that situation to be?

Ms. HALVORSON. Well, unfortunately we are still working with them. They were told in the beginning that the money that they would get could help them relocate.

Now they have been told that the money will only be to fix the school they are in. However, it is minimal. It will not come near the cost to fix the school, and the school will have to be left in the place it is at. It is in a floodplain where it will flood over and over again.

So we need whatever help we can get to mitigate the fact that we do not want it to still be structurally unsound and so we need whatever help we can to mitigate the process to make it safe from this to happen again. The parents are scared to put their fifth graders and sixth graders back in a situation where this could happen again over and over again.

Mr. PRICE. Well, we will certainly give this consideration. We understand very readily the challenge you are facing here and the need to get this school back in business in a safer way, a way that will resist future damage. We will have to see—

Ms. HALVORSON. Right.

Mr. PRICE [continuing]. What the fit is between this and the kind of categories of funding that we have available.

Mr. ROGERS.

Mr. ROGERS. No questions.

Mr. PRICE. No questions. So thank you very much, Ms. Halvorson.

Ms. HALVORSON. And thank you both very much. We are just looking for every avenue possible to help these children.

Mr. PRICE. We understand. Thank you.

Ms. HALVORSON. Thank you.

Mr. PRICE. So we will next call Congressman Cuellar. Welcome.

Mr. CUELLER. Mr. Chairman, Mr. Rogers.

Mr. PRICE. Congressman, we are glad to have you. We ask you to summarize your remarks within five minutes, and we will put your full statement in the record.

THURSDAY, APRIL 23, 2009.

MEMBER REQUESTS

WITNESS

HON. HENRY CUELLAR, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. CUELLER. Thank you, Mr. Chairman. First of all, I appreciate the work that you all do in this committee. As you know, I chair one of the subcommittees in the Homeland Security, so I appreciate what the Appropriations folks do here.

I have a couple of requests here. I just want to talk about one. It has to do with an advance emergency response wireless network

for the city of Hidalgo. This is a FEMA predisaster mitigation account in the amount of \$500,000. Basically what we are asking here, Mr. Chairman, is to create a wireless broadband network to provide public alert and warning communications.

One of the things that we have seen down there on the border, Mr. Chairman, is the fact that we have the situation of what is happening across the river, number one, the situation with the drug cartels across the river. At the same time, being on the river in that particular area we have put in some money for levees to control the flooding. There was a huge flooding there back about 20, 30 years ago.

So what this will allow is to have a wireless broadband network for alert and warning communications, and this is something that I would ask you to consider. I have some other requests, but I know you all are very busy, and the rest of the testimony is there. I just wanted to bring this up at this time.

[The information follows:]

**Homeland Security Appropriations Subcommittee
Testimony- Congressman Henry Cuellar (TX-28)**

Chairman Price, Ranking Member Rogers and Members of the subcommittee: Thank you for the opportunity to address the Committee and to speak to the importance of Homeland Security projects in the 28th Congressional District of Texas.

The 28th District contains four counties along the US-Mexico border, the nation's largest inland trade port in terms of trade volume and three major population centers, one of which bears current Urban Area Security Initiative designation. The projects I have submitted for inclusion in the Homeland Security appropriations bill are in alignment with the three accounts identified by the Chairman and are of direct significance to the safety and security of the infrastructure and citizens in the 28th district of Texas.

Today's challenging economy is straining the budgets of communities across Texas, but the need for strong, effective emergency response networks remains as pressing as ever and areas along the southern border continue to face daunting challenges in coordinating their emergency response and security efforts.

Right now, with border violence on the rise, it is more important than ever that we work to protect border communities.

Homeland Security Appropriations Subcommittee
Testimony – Congressman Henry Cuellar (TX-28)

I strongly support my project submission of an **Advanced Emergency Response Wireless Mesh Network submission for the City of Hidalgo, Texas submitted to the FEMA Pre-Disaster Mitigation account in the amount of \$500,000.** This program will create a wireless broadband network to serve as an integrated internet-based public alert and warning communication system to educate and assist the public in responding to emergencies and natural disasters.

Located along the international border with Mexico, the City of Hidalgo faces the threat of increasing spillover violence associated with drug trafficking, gunrunning, kidnaping and illegal alien smuggling as well as varied everyday emergencies and threats from natural disasters. It is essential that to national security that the City is ready and prepared in the event of increased violence on US soil or natural disaster. The development of this network is one of many important steps to ensure the safety and security of our border communities. In addition, in the past, the City has endured substantial damage resulting from major storm systems arising in the Gulf of Mexico. Hurricanes Dolly and Ike brought heavy winds that generated large amounts of vegetative and C&D debris that was deposited throughout Hidalgo County, TX in unincorporated county areas and multiple cities. The network will help detect and respond to these natural disasters much quicker.

This important project will install strategically placed small antennas around the city creating a wireless mesh messaging network to serve as integrated public alert and warning system to a rural area that currently has minimal interconnectivity. This network

Homeland Security Appropriations Subcommittee
 Testimony – Congressman Henry Cuellar (TX-28)

would bring 145 computer systems and would to connect several City institutions, including the Fire, Police, City Hall, Municipal Court, Administration, Finance, Water, and Code Enforcement.

Breakdown of Use of Funds

Computer Equipment	\$ 163,300
Vehicles for Support Services	\$ 86,700
Training for City Employees & Support Services	\$ 56,666
Security / Storage	\$ 56,666
Software Applications & Operating System	\$ 56,666
Antenna Installation	\$ 80,000
TOTAL	\$ 500,000

The City plans to match 25% of project cost.

Homeland Security Appropriations Subcommittee
Testimony – Congressman Henry Cuellar (TX-28)

I would also like to strongly speak in support of the following four projects:

South Texas Regional Emergency Operations Center requested for the FEMA Emergency Operations Center account in the amount of \$500,000.

The Emergency Operations Center (EOC) will provide a location where multiple levels of government, agencies, and organizations can coordinate decisions, resources, and public information on a strategic level. The EOC is an important support element to the Incident Command structure. For all incidents, regardless of cause, response will focus on actions taken to save lives, sustain life, and protect infrastructure. It is essential to our homeland security that our public safety officials will be able to mitigate emergencies or disasters on both sides of the border and support interoperable communications in the region.

City of Hidalgo Old town Site Drainage submitted to the FEMA Pre-Disaster Mitigation account in the amount of \$300,000.

The City of Hidalgo, Texas is proposing a construction project for infrastructure improvements. The improvements will include a repair of an Old Town Site drainage system. The network of storm sewers that collect surface runoff was installed in the 30's and 40's and has become inadequate to drain the drainage basin. This project is a structural retrofitting to eliminate street flooding that takes place during 10-year storm events and severe tropical storms and hurricanes that take place in Southern Texas. The ability to eliminate or mitigate this flooding will go a long way in reducing storm related damage claims and associated re-construction cost.

Homeland Security Appropriations Subcommittee
Testimony – Congressman Henry Cuellar (TX-28)

Frio County Emergency Operations Center, requested for the FEMA Emergency Operations Center account in the amount of \$500,000.

The Frio County Emergency Operations Center (EOC) would enhance disaster preparedness by serving as a central location for emergency management personnel to coordinate responses to a potential disaster. The EOC is an critical support element to the Incident Command structure. For all incidents, regardless of cause, response will focus on actions taken to save lives, sustain life, and protect infrastructure. This facility will serve a essential homeland security role as a location to provide critical training to first responders and emergency coordinators in order to prepare for future emergencies.

Rio Grange Valley Border Security and Technology Training Center in the City of Hidalgo requested for the FEMA Emergency Operations Center account in the amount of \$1,000,000.

The City of Hidalgo, Texas, in partnership with South Texas College, proposes to establish a 20,000 square foot Hidalgo Border Security and Technology Training Center. This project will significantly enhance the regions ability to develop, utilize and provide for the implementation of and training in critical technologies and polices related to border security. The center's unique service strategy is to provide training for targeted industry clusters that support the needs and requirements of Border Security and Emergency Preparedness and Response and is critical to ensuring the safety of our border communities and national security.

Mr. PRICE. All right. Thank you very much.

Mr. ROGERS. do you have any questions?

Mr. ROGERS. No questions.

Mr. PRICE. All right. We appreciate your appearing.

Mr. CUELLER. Thank you, sir.

Mr. PRICE. And we will give due consideration to your request.

Mr. CUELLER. Thank you for your time.

Mr. PRICE. We had one additional witness scheduled, but I do not believe he is on the scene. All right.

VOICE. He is here, Mr. Chairman.

Mr. PRICE. All right. Good. Good. Our colleague, Rush Holt from New Jersey arriving, just in the nick of time.

Rush, we welcome you here. We ask that you give us a five minute oral summary of your statement. We will put whatever you want in the record.

THURSDAY, APRIL 23, 2009.

MEMBER REQUESTS

WITNESS

HON. RUSH D. HOLT, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

Mr. HOLT. I hope I can keep it to less than that. Thank you, Mr. Chairman, Mr. Rogers and the committee. Thanks for the opportunity to testify on the fiscal 2010 Homeland Security appropriations.

As I have already provided the subcommittee with information, I have requests for some specific projects in Old Bridge, Shrewsbury, West Windsor Township and Trenton, and I will not revisit those requests right now. I would like to talk about a couple of programmatic matters.

As you may know, I have a programmatic funding request regarding the Commercial Equipment Direct Assistance Program, the so-called CEDAP. CEDAP fills a critical role in helping local law enforcement and first responders by providing qualified applicants with the means to buy commercially available equipment that can be used to make our community safe.

Since its inception in 2005, CEDAP funding has been reduced from \$50 million to its current low in fiscal year 2009 of \$8 million. During 2008, more than 3,500 applications were approved for funding. However, based upon the availability of funds only 1,000 jurisdictions were ultimately served by the program. Twenty-five hundred approved applications were placed on the 2009 CEDAP list.

In September 2008, then Senator Biden introduced the Homeland Security Law Enforcement Improvements Act, which called for allocating not less than \$75 million for the CEDAP program for fiscal years 2009 and 2010, and I think this would be an appropriate funding level so I request that you take a look at the CEDAP funding and consider an increase to something on the order of \$75 million.

Second, I would like to bring to the committee's attention a situation at Amtrak that I believe represents a shortcoming in safety preparations and effective counterterrorism response.

Earlier this year I was made aware of the existence and activities of the Amtrak's Office of Security Strategy and Special Operations. This element, which does not answer to the leadership of the existing Amtrak Police Department, has created SWAT-like units and intelligence liaison relationships with our intelligence agencies and conducted hostage rescue training exercises, all without, as far as I can tell, integrating its activities within the existing Amtrak Police Department's chain of command.

Police union officials have visited me and talked about training exercises that have been conducted without notifying, for example, either the Washington Metropolitan Police Department or the FBI Joint Terrorism Task Force in Washington. This created something of a scene.

This OSSSO entity has, according to its own officials, received millions of dollars of rail security funding approved by Congress, and when they met with me earlier they pressed for still more. I am deeply concerned about this entity's activities and the clear disconnect within Amtrak over who is in charge of rail security in the northeast corridor and elsewhere in the Amtrak system.

So I ask the committee to conduct a probing look at this, at the organization and its relationship with the Amtrak Police Department, and give some thought to what measures Amtrak should take either on its own or with congressional direction to ensure that there is a coherent, unified organization looking at rail security.

I appreciate the committee's time and attention on these matters, and I would be happy to answer any questions.

[The information follows:]

Oral Testimony of Rep. Rush Holt
Before The Homeland Security Subcommittee
House Committee on Appropriations
On The Fiscal Year 2010
Department of Homeland Security Appropriations Act
April 23, 2009

Chairman Price, Ranking Member Rogers, members of the subcommittee—thank you for this opportunity to discuss my views and requests regarding the Fiscal Year 2010 Department of Homeland Security Appropriations bill. As I've already provided the subcommittee with the information it needs on my requests for the Township of Old Bridge, The Borough of Shrewsbury, West Windsor Township, and the City of Trenton, I will not revisit those requests today. Instead, I'd like to discuss a programmatic matter, as well as an oversight matter relating to rail security that I believe you may be interested in pursuing further. Let me first address the program of concern to me today.

As you may know, I have a programmatic funding request regarding the Commercial Equipment Direct Assistance Program (CEDAP). CEDAP fills a critical role in helping local law enforcement and first responders by providing qualified applicants with the means to buy commercially available equipment that is used to make our communities safer from criminals and potential terrorist attacks. Since its inception in 2005, CEDAP funding has been reduced from \$50 million to its current low in Fiscal Year 2009 of \$8 million. During the 2008 CEDAP process, 3,573 applications were approved for funding. However, based upon the availability of funds only 1,045 jurisdictions were ultimately served by the program. The remaining

2,528 approved applications were placed on the 2009 CEDAP list, but with \$8 million allocated only a fraction of the pending applications will be filled.

In September 2008, then-Senator Joseph Biden introduced S. 3524, the Homeland Security and Law Enforcement Improvements Act, which called for allocating not less than \$75 million for the CEDAP program for Fiscal Years 2009 and 2010. I believe that this is the appropriate funding level for this program in light of the continuing equipment and preparedness gaps our first responders face, as well as the ongoing threats from organizations like Al Qaeda. Accordingly, I ask that you fund CEDAP at not less than \$75 million for Fiscal Year 2010. I also ask unanimous consent to place into the record a number of support letters for the CEDAP program from homeland security-related businesses from around the country.

Second, I wanted to bring to the subcommittee's attention a situation at Amtrak that I believe represents a threat to public safety and effective counterterrorism response in the event of an attack on the system.

Earlier this year, I was made aware of the existence and activities of Amtrak's Office of Security Strategy and Special Operations. This element—which does not answer to the leadership of the existing Amtrak Police Department—has allegedly created, among other things, mobile SWAT-like units, intelligence liaison relationships with our intelligence agencies, and conducted hostage rescue training exercises—and all without integrating its activities within the existing Amtrak Police Department's chain of command. Police union officials who visited with me earlier this year allege at least one incident in which OSSSO elements conducted a

hostage rescue exercise without notifying either the Washington Metropolitan Police Department or the FBI Joint Terrorism Task Force in Washington.

This OSSSO entity has, according to its own officials, received millions of dollars of rail security funding approved by Congress, and when they met with me earlier this year they pressed for still more. I am deeply concerned about this entity's activities and the clear disconnect within Amtrak over who is in charge of rail security along the northeast corridor and elsewhere in the Amtrak system. Accordingly, I ask the subcommittee to conduct a probing, public examination of the OSSSO, its relationship to the Amtrak Police Department, and what measures Amtrak should take—either on its own or via Congressional direction—to ensure that there is only one entity in Amtrak charged with rail security.

I appreciate the subcommittee's time and attention to these matters, and I would be happy to answer any questions.

**ACISS Systems, Inc.***"The right information, when and where it's needed"*

Tel: (727) 786-5450
Fax: (727) 786-5545
33920 US Highway 19 N Ste 150
Palm Harbor, FL 32684
www.aciss.com

March 2, 2009

Honorable David E. Price
North Carolina-4th, Democrat
U.S. House of Representatives
2162 Rayburn Building
Washington, DC 20515

Dear Congressman Price,

Recently 16 companies delivered approximately \$17 million dollars worth of homeland security equipment to 1,045 first responders through the 2008 CEDAP program. It was quite a sight to see more than 700 responders from around the country assembled to receive training on the equipment they were awarded in Washington, DC during the week of February 8th. Besides the obvious pride in seeing our technology put onto the front lines of crime and terror, each one of the companies competitively chosen for the CEDAP program reside in small towns across the country (Warminster, PA, Londonderry, NH, Burtonsville, MD, Princeton, NJ to name a few), and make up Main Street America at its innovative best, where collectively more than 200 people are employed to manufacture and provide training for the CEDAP program.

In the last three years, the CEDAP program has seen its appropriated funding diminish from \$40 million in 2006, to a new low of \$8 million in 2009. In light of the recent stimulus package, where many dollars were sent to established "shovel ready" programs and projects, all of which were meant to keep businesses and families afloat, CEDAP was overlooked. A supplemental appropriation of \$25 million would allow for another 1,000 to 2,000 first responders to receive equipment with little effort since more than 2,700 approved applications are still in the queue from 2008.

Obviously, this well-established and vetted program can be instrumental in supporting the stimulus goals, increase high-tech jobs that keep us on the forefront of national preparedness, and provide the needed tools for our first responders. Your support is critical in garnering supplemental funding in 2009, as well as bolstering the annual appropriation in 2010 to a level commensurate with needs among the first responder community.

Sincerely,



Anthony Bastian, CDP, MCSE
President

"The right information, when and where it's needed!"



March 6, 2009

Honorable David E. Price
North Carolina-4th, Democrat
U.S. House of Representatives
2162 Rayburn Building
Washington, DC 20515

Dear Congressman Price:

Recently 16 companies delivered approximately \$17 million dollars worth of homeland security equipment to 1,045 first responders through the 2008 CEDAP program. It was quite a sight to see more than 700 responders from around the country assembled to receive training on the equipment they were awarded in Washington, DC during the week of February 8th. Besides the obvious pride in seeing our technology put onto the front lines of crime and terror, each one of the companies competitively chosen for the CEDAP program reside in small towns across the country (Warminster, PA, Londonderry, NH, Burtonsville, MD, Princeton, NJ to name a few), and make up Main Street America at its innovative best, where collectively more than 200 people are employed to manufacture and provide training for the CEDAP program.

In the last three years, the CEDAP program has seen its appropriated funding diminish from \$40 million in 2006, to a new low of \$8 million in 2009. In light of the recent stimulus package, where many dollars were sent to established "shovel ready" programs and projects, all of which were meant to keep businesses and families afloat, CEDAP was overlooked. A supplemental appropriation of \$25 million would allow for another 1,000 to 2,000 first responders to receive equipment with little effort since more than 2,700 approved applications are still in the queue from 2008.

Obviously, this well-established and vetted program can be instrumental in supporting the stimulus goals, increase high-tech jobs that keep us on the forefront of national preparedness, and provide the needed tools for our first responders. Your support is critical in garnering supplemental funding in 2009, as well as bolstering the annual appropriation in 2010 to a level commensurate with needs among the first responder community.

Sincerely,

Richard C. Miller
President and CEO

Americas:
E.D. Bullard Company
1898 Safety Way • Conitana, NY 41031-9303
Toll free: 877-BULLARD (285-5273)
Tel: 859-234-6616 • Fax: 859-234-6987
www.bullard.com

Europe:
Bullard GmbH
Lilienthalstrasse 12
53424 Remagen • Germany
Tel: +49-2642 999980 • Fax: +49-2642 999929
www.bullard.com

Asia-Pacific:
Bullard Asia Pacific Pte. Ltd.
LJK Building
701, Sims Drive, #04-03 • Singapore 387283
Tel: +65-6745-0556 • Fax: +65-6745-5
www.bullard.com



March 3, 2009

Honorable David E. Price
North Carolina-4th, Democrat
U.S. House of Representatives
2162 Rayburn Building
Washington, DC 20515

Dear Congressman Price,

Recently, 16 companies delivered approximately \$17 million dollars worth of homeland security equipment to 1,045 first responders through the 2008 CEDAP program. It was quite a sight to see more than 700 responders from around the country assembled to receive training on the equipment they were awarded in Washington, DC during the week of February 8th. Besides the obvious pride in seeing our technology put onto the front lines of crime and terror, each one of the companies competitively chosen for the CEDAP program reside in small towns across the country (Warminster, PA, Londonderry, NH, Burtonsville, MD, Princeton, NJ to name a few), and make up Main Street America at its innovative best, where collectively more than 200 people are employed to manufacture and provide training for the CEDAP program.

In the last three years, the CEDAP program has seen its appropriated funding diminish from \$40 million in 2006, to a new low of \$8 million in 2009. In light of the recent stimulus package, where many dollars were sent to established "shovel ready" programs and projects, all of which were meant to keep businesses and families afloat, CEDAP was overlooked. A supplemental appropriation of \$25 million would allow for another 1,000 to 2,000 first responders to receive equipment with little effort since more than 2,700 approved applications are still in the queue from 2008.

Obviously, this well-established and vetted program can be instrumental in supporting the stimulus goals, increase high-tech jobs that keep us on the forefront of national preparedness, and provide the needed tools for our first responders. Your support is critical in garnering supplemental funding in 2009, as well as bolstering the annual appropriation in 2010 to a level commensurate with needs among the first responder community.

Sincerely,

Jack Hornberger
President and CEO



MARCH 3, 2009

Honorable David H. Price
North Carolina-4th, Democrat
U.S. House of Representatives
2162 Rayburn Building
Washington, DC 20515

Dear Congressman Price,

Recently 16 companies delivered approximately \$17 million dollars worth of homeland security equipment to 1,045 first responders through the 2008 CEDAP program. It was quite a sight to see more than 700 responders from around the country assembled to receive training on the equipment they were awarded in Washington, DC during the week of February 8th. Besides the obvious pride in seeing our technology put onto the front lines of crime and terror, each one of the companies competitively chosen for the CEDAP program reside in small towns across the country (Warminster, PA, Londonderry, NH, Burtonsville, MD, Princeton, NJ to name a few), and make up Main Street America at its innovative best, where collectively more than 200 people are employed to manufacture and provide training for the CEDAP program.

In the last three years, the CEDAP program has seen its appropriated funding diminish from \$40 million in 2006, to a new low of \$8 million in 2009. In light of the recent stimulus package, where many dollars were sent to established "shovel ready" programs and projects, all of which were meant to keep businesses and families afloat, CEDAP was overlooked. A supplemental appropriation of \$25 million would allow for another 1,000 to 2,000 first responders to receive equipment with little effort since more than 2,700 approved applications are still in the queue from 2008.

Obviously, this well-established and vetted program can be instrumental in supporting the stimulus goals, increase high-tech jobs that keep us on the forefront of national preparedness, and provide the needed tools for our first responders. Your support is critical in garnering supplemental funding in 2009, as well as bolstering the annual appropriation in 2010 to a level commensurate with needs among the first responder community.

Sincerely,

Douglas Perkins
Vice President



March 2, 2009

Honorable David E. Price
North Carolina-4th, Democrat
U.S. House of Representatives
2162 Rayburn Building
Washington, DC 20515

Dear Congressman Price,

Recently 16 companies delivered approximately \$17 million dollars worth of homeland security equipment to 1,045 first responders through the 2008 CEDAP program. It was quite a sight to see more than 700 responders from around the country assembled to receive training on the equipment they were awarded in Washington, DC during the week of February 8th. Besides the obvious pride in seeing our technology put onto the front lines of crime and terror, each one of the companies competitively chosen for the CEDAP program reside in small towns across the country (Warminster, PA, Londonderry, NH, Burtonsville, MD, Princeton, NJ to name a few), and make up Main Street America at its innovative best, where collectively more than 200 people are employed to manufacture and provide training for the CEDAP program.

In the last three years, the CEDAP program has seen its appropriated funding diminish from \$40 million in 2006, to a new low of \$8 million in 2009. In light of the recent stimulus package, where many dollars were sent to established "shovel ready" programs and projects, all of which were meant to keep businesses and families afloat, CEDAP was overlooked. A supplemental appropriation of \$25 million would allow for another 1,000 to 2,000 first responders to receive equipment with little effort since more than 2,700 approved applications are still in the queue from 2008.

Obviously, this well-established and vetted program can be instrumental in supporting the stimulus goals, increase high-tech jobs that keep us on the forefront of national preparedness, and provide the needed tools for our first responders. Your support is critical in garnering supplemental funding in 2009, as well as bolstering the annual appropriation in 2010 to a level commensurate with needs among the first responder community.

Sincerely,

A handwritten signature in black ink, appearing to read "John Romanowich".

John F. Romanowich,
President and CEO

Mr. PRICE. Thank you. We do appreciate you coming forth and addressing these policy matters, particularly this latter concern, which I agree does warrant our attention as we prepare the bill, so thank you for flagging this matter this morning.

Mr. ROGERS, do you have any questions?

Mr. ROGERS. Only to comment briefly. I appreciate your bringing to our attention the CEDAP request. That is a popular thing in my part of Kentucky. Of course, we will give that due consideration, but I do appreciate your highlighting that aspect. Thank you.

Mr. HOLT. Thank you. If I may just say for the record so that it is clear to others, CEDAP gives a preapproved list that makes it easier for small organizations without large procurement departments to choose approved items and get on with it.

Mr. ROGERS. Commercial Equipment Direct Assistance Program, and that is a proper name.

Mr. HOLT. Thank you.

Mr. PRICE. Thank you very much.

Mr. HOLT. Thank you.

Mr. PRICE. With that, we thank all of our witnesses, and the Subcommittee is adjourned.

Statement of Rep. John M. McHugh

before the

**Subcommittee on Homeland Security
House Committee on Appropriations**

“Upstate New York Cyber Initiative”

April 22, 2009

Thank you, Mr. Chairman, for the opportunity to testify today on an issue of great national importance. Specifically, as you know the potential for the use of cyber-attacks as a weapon to jeopardize critical information and thus harm our economy and otherwise diminish the well-being and safety of all Americans. Additionally, U.S. commercial losses from cyber attacks have the potential to be in the range of billions of dollars.

It is clear that given the severity of the potential threat, our nation must take steps to enhance our ability to train and educate the cyber security experts needed to safeguard sensitive information, thereby protecting both the private and public sectors. In response to this critical need I have respectfully requested that federal funds be provided in Fiscal Year 2010 for the Upstate New York Cyber Initiative.

The Upstate New York Cyber Initiative would be administered by Clarkson University in Potsdam, New York, which I am privileged to represent. In addition, through this proposal, Clarkson would establish and maintain a collaborative cyber security training center and team designed to educate large numbers of highly qualified individuals in the fields of information assurance and cyber security. Of note, cooperation and collaboration by Initiative team members

would provide coverage of key domains including the financial sector, national critical infrastructures, business and industry, as well as state and federal governments.

The Upstate New York Cyber Initiative team would also include the State University of New York (SUNY) at Buffalo (home of the National Security Agency certified Center of Excellence in Information Systems Assurance), the Rochester Institute of Technology, and The Advanced Course in Engineering (ACE) cyber security training program, which was initiated by the National Science Foundation and is located in Rome, New York. The synergy of the institutions would address critical Cyber security areas including: requirements gathering, R&D, testing, cyber exercises, and placement of interns.

The Upstate New York Cyber Initiative team would constantly update security training modules to anticipate and respond to new threats, improve warning capabilities, accelerate comprehensive responses to real time attacks and, most importantly, educate the next generation of security experts. Moreover, the training center would allow each school to share critical information and integrate best practices for cyber security training and education.

Mr. Chairman, while I am aware that the Homeland Security Appropriations bill has historically limited the amount of member requests, I would respectfully request that the Subcommittee carefully consider providing funding to the Initiative I have just described. I thank you again for the opportunity to share my perspective on this issue and your efforts to improve our nation's security. I look forward to working with you as the appropriations process continues.

United States House of Representatives

Committee on Appropriations

Subcommittee on Homeland Security

Fiscal Year 2010

Outside Witness Testimony

TESTIMONY OF
WILLIAM W. MILLAR
PRESIDENT
AMERICAN PUBLIC TRANSPORTATION ASSOCIATION
SUBMITTED TO THE
HOUSE APPROPRIATIONS SUBCOMMITTEE ON HOMELAND SECURITY

April 16, 2009

SUBMITTED BY

American Public Transportation Association
1666 K Street, N.W.
Washington, DC 20006
Tel: (202) 496-4800
Fax: (202) 496-4324



APTA is a nonprofit international association of nearly 1,500 public and private member organizations including transit systems and commuter rail operators; planning, design, construction and finance firms; product and service providers; academic institutions; transit associations and state departments of transportation. APTA members serve the public interest by providing safe, efficient and economical transit services and products. Over ninety percent of persons using public transportation in the United States and Canada are served by APTA members.

Mr. Chairman, thank you for this opportunity to provide testimony to the Subcommittee on the security needs of the public transportation industry for Fiscal Year 2010. We appreciate the fact that you and this committee have made security a priority for the tens of millions of Americans who use public transportation an important priority of this Committee. We look forward to working with you on this issue and thank you for your leadership on transit security.

ABOUT APTA

The American Public Transportation Association (APTA) is a nonprofit international association of nearly 1,500 public and private member organizations, including transit systems and commuter rail operators; planning, design, construction, and finance firms; product and service providers; academic institutions; transit associations and state departments of transportation. APTA members serve the public interest by providing safe, efficient, and economical transit services and products. More than ninety percent of the people using public transportation in the United States and Canada are served by APTA member systems. In accordance with the National Infrastructure Protection Plan, APTA is recognized by the Department of Homeland Security (DHS) as serving the capacity of the Mass Transit Sector Coordinating Council (SCC).

PUBLIC TRANSIT SECURITY/ ALL HAZARDS RISK EXPOSURES & NEEDS

Public transportation is a critical component of our nation's infrastructure. Americans take more than 10.7 billion transit trips each year. People use public transportation vehicles more than 35 million times each weekday. This is eighteen times the number of daily boardings on the nation's domestic airlines.

Both the Administration and Congress have fully acknowledged that terrorist threats to transit agencies are real, and have not diminished. The Government Accountability Office (GAO) released a 2002 report which said "about one-third of terrorist attacks worldwide target transportation systems, and transit systems are the mode most commonly attacked." More recently, on February 29, 2008, the Office of Intelligence of the Transportation Security Administration (TSA) released a report concluding that public transportation in America remains vulnerable to terrorist attack. The report states: "The volume of previous attacks and recent plotting against mass transit systems overseas demonstrates continued strong terrorist interest in targeting this sector." The report further states that: "Previous rail attacks in Madrid, London, and Mumbai could inspire terrorists to conduct similar attacks in the United States." Transit agency and passenger risk exposure is very real, and threats upon systems and their operations have, in fact, occurred and continue.

Safety and security have always been the top priority of the public transportation industry. Since 9/11, transit systems have taken many steps to further improve security. Public transit agencies with state and local governments, have invested billions of dollars on security and emergency preparedness programs. While we are pleased that Congress recognizes the importance of investing in the safety of public transportation, federal investment in transit security has been minimal when compared to other transportation modes. For example, since 9/11 the federal government has spent nearly \$30 billion on aviation security and has allocated only \$1.4 billion for transit security.

In 2004, APTA surveyed U.S. transit agencies to determine what actions were needed to improve security for their customers, employees and facilities. In response to the survey, transit agencies around the country identified in excess of \$6 billion in transit security investment needs.

State and local governments and transit agencies are doing what they can, but it is important for the federal government to increase support for transit security.

In August, 2007, H.R.1, the 9/11 Commission Recommendations Act of 2007, was signed into law (Public Law 110-53). The legislation authorizes \$3.4 billion in transit security funding over a four year period. The legislation also set in place a number of the structural elements that APTA and the nation's transit systems had been seeking, including broad eligibility for capital and operational improvements, a rejection of a "one-size fits all" approach to transit security, a recognition of the open nature of transit facilities and services, interagency coordination between DHS and DOT, consultation and coordination at all levels of government and with industry stakeholders, information sharing and intelligence analysis, research and development, and fair enforcement and liability considerations.

PROGRAM NEEDS AND GRANTS

APTA asks the committee to provide appropriations for the FY 2010 Transit Security Grant Program (TSGP) in the amount of \$900 million, the level authorized under the 9/11 Commission Recommendation Act of 2007. We appreciate Congress' recognition of the importance of securing our nation's transit systems by providing substantial funding in the FY 2009 Department of Homeland Security Appropriations bill and the American Recovery and Reinvestment Act (ARRA). However, even those funding levels have not adequately addressed the overwhelming security needs identified by APTA members or met the authorized levels for those programs. We further ask that you again include language that directs DHS to award funds directly to transit agencies and prohibits DHS from imposing a local match requirement, consistent with Congressional intent expressed in the conference report of the 9/11 Commission Act.

The grant application and award process needs to be streamlined dramatically. We are hopeful that the oversight efforts of Congress, which have led to recent proposed reforms in the TSGP grant process, will achieve the desired results and expedite the delivery of funds to transit agencies with security improvement needs.

It is important to recognize that, for several years now, APTA and its member transit agencies have sought procedural simplification, urging that grants be provided directly to transit agencies and without local match requirements. We greatly appreciate that Congress included in the ARRA prior-year provisions that direct DHS to award funds directly to public transportation agencies, and prohibit DHS from imposing a local match requirement. The delays in grant distribution and obligations in recent years and the continual reorganization of the relevant agencies within DHS should not prejudice funding for transit security in FY2010. The security needs remain and have not diminished, and APTA's member agencies remain committed to the expeditious obligation and expenditure of funds to their important security projects.

In addition to the transit security grant funding, we urge Congress to provide \$600,000 to enable APTA to maintain and operate the Public Transit Information Sharing Analysis Center (ISAC). Funding for this program was authorized under the 9/11 Commission bill under Section 1410 (d), which provides for the sharing of security information between transit agencies and DHS. The ability to share vital information is crucial in preventing and mitigating potential terrorist attacks.

Although we have been advised by DHS that a one-year grant will be provided to sustain this important resource, its continuity remains uncertain.

We also urge Congress to provide \$500,000 to DHS for the APTA security standards program. APTA is recognized as a Standards Development Organization (SDO) for the public transportation industry. H.R. 1 requires that DHS work with the transit industry. We are applying our growing expertise in standards development to transit industry safety and security, best practices, guidelines and standards. Over the last several years, APTA has worked closely with the Department of Transportation (DOT), DHS and industry leaders to develop standards that help transit agencies use available resources as effectively as possible. And while this program has proven its success, its continuity also remains uncertain as short term grants through the U.S. DOT have now been exhausted.

The ISAC and security standards are two important national programs that, although modest in funding needs, can significantly enhance transit security at the local level.

We must also point out that the recent Budget submission of this Administration cites a proposal to add "Funding of \$50 million [which] will provide 15 new Visual Intermodal Protection Response Teams at the Transportation Security Administration to increase additional random force protection capability by deploying to transit hubs unannounced." This proposal was not discussed with the transit industry, and it is expressly prohibited under the provisions of the 9-11 Commission Act (Sec. 1303). We have urged the Administration to reconsider the "unannounced" provision of this proposal that conveys a message that is in conflict with established procedures and legislation, and to make a greater effort to coordinate with the transit industry in advance of such future proposals.

Finally, with regard to technology research and development, it is the general view of the industry that there is no current formal structure that brings the federal government and transit industry together to discuss transit security technology priorities, needs and areas of potential interest for technology advancement and research. The public transportation industry has, over the recent years, cooperated with DHS to provide test-beds for evaluating various technologies but the types of technologies to be tested were unilaterally determined by DHS. To date, there have not been any collaborative meetings with transit operators to identify needs relative to security technology or research. Any format for strategic planning of security technology research and development that does not fully engage the actual industry is inherently flawed. It is imperative therefore that DHS instruct the Transportation R & D Working Group to enlist representation from Mass Transit and other transportation sectors and to include such representation as full participants including preliminary stages of needs identification and strategy development.

SECURITY INVESTMENT NEEDS

Since the events of 9/11, the transit industry has invested billions of its own funds for enhanced security measures, building on the industry's already considerable efforts. At the same time, our industry conducted comprehensive reviews to determine how we further improve on existing security practices. This effort has included a range of activities, which include research, best practices, education, information sharing in the industry, and surveys. As a result we have a better understanding of how to create a more secure environment for our riders and of the most critical security investment needs.

Our survey of public transportation security identified enhancements of at least \$5.2 billion in additional capital funding to maintain, modernize, and expand transit system security functions to meet increased security demands. Over \$800 million in increased costs for security personnel, training, technical support, and research and development have been identified, bringing total additional transit security funding needs to more than \$6 billion.

Responding transit agencies were asked to prioritize the uses for which they required additional federal investment for security improvements. Priority examples of operational improvements include, but are not limited to:

- Funding current and additional transit agency and local law enforcement personnel
- Funding for over-time costs and extra contract security personnel during heightened alert levels
- Training for security personnel
- Joint transit/law enforcement training
- Security planning activities
- Security training for other transit personnel

Priority examples of security capital investment improvements include:

- Radio communications, including interoperable systems
- Security cameras on-board transit vehicles and in transit stations
- Controlling access to transit facilities and secure areas
- Automated vehicle locator systems
- Security fencing around facilities
- Intrusion detection systems
- Asset and facilities hardening
- Infrastructure that supports law enforcement resources

The 9-11 Commission Act recognized a broad range of security improvements and activities as eligible uses of transit security grant funds. DHS and TSA have promulgated grant program guidance that aim to restrict the eligible uses of funds in a manner inconsistent with the goals of the authorizing legislation. We urge Congress and the Administration to work to maintain the broad eligibility as intended under the authorizing legislation.

ORGANIZING FOR IMPROVED HOMELAND SECURITY AND COUNTERTERRORISM

APTA recently provided recommendations to the presidentially appointed Study Team currently conducting its interagency review of organizational reform of homeland security and counter-terrorism structures and initiatives. Efforts to improve the current organization of Homeland Security programs as they relate to public transportation security can be undertaken within the basic framework that currently exists. Certain approaches to policy and program administration may need to be altered, but largely the base structure is already in place. Our comments relative to options for improved Homeland Security policy and organizational management in several specific topical areas follow.

Interagency Coordination

The impressions of the mass transit sector since the creation of the Department of Homeland Security are that while we, as an industry infrastructure have made some gains in establishing working relationships with the various DHS Directorates, we continue to see examples of competition, strained relationships and silos within the Department. This condition ultimately results in delays, deferrals and duplication of effort.

A similar condition is seen to exist between the DHS and the DOT, in spite of the Public Transportation Annex to the Memorandum of Understanding (MOU) that was intended to provide a path for partnership and collaboration.

Similarly, it is the impression of the mass transit sector that while we have seen some strengthening of the outreach and partnering between DHS and this sector through activities such as the "Coordinating Councils", we continue to see DHS proceed on critical activities such as security technology research and development unilaterally and without seeking industry input. We recommend that DHS continue to expand its outreach to the Mass Transit SCC and other industry-wide organizations through the DHS Directorate of Science and Technology and the TSA Chief of Technology Office with respect to security technology research and development.

The statutory provisions of the 9-11 Commission Act stressed significant consultation and coordination between the DHS and DOT components. The responsibility for successful interagency coordination must ultimately rest with department and agency leadership, but oversight by OMB and senior White House officials could assist in this regard. Further, utilizing existing mechanisms and structures, such as the Mass Transit SCC and federally recognized Standards Development Organizations (SDOs) such as APTA can assist in bringing multiple federal agency partners to the table to work through complex and difficult issues.

Seamless Integration between International and Domestic Efforts

The proliferation of international terrorism upon mass transit facilities and services exemplifies the need to ensure that international agreements are achieved and nurtured to enable information and resource sharing as well as communication of lessons learned. Such agreements must, however, transcend beyond government and should be expanded to include the involvement of those infrastructures such as mass transit.

The goal of integrating domestic and international efforts can also be fulfilled through existing structural and programmatic means within the transit security arena. Even before the attacks

of September 11th, APTA had been working with international industry members to evaluate security planning efforts and best practices, analyzing the responses to overseas terrorist attacks on and around transit assets. Our collaboration with our international members and partners has been of particular assistance in the immediate aftermath of several of the most recent international transit security incidents. APTA members include London Underground Limited, Metro de Madrid, S.A., and the Moscow Metro, and APTA was able to coordinate and communicate with each of these systems literally within hours of the terrorism incidents each experienced. APTA International membership includes many others across Europe, South America, the Middle East and Asia. APTA Members and staff also serve on the Security Commission of the International Union of Public Transport based in Brussels. These efforts are the model for international cooperation in the security arena.

Capability to Coordinate Planning for Federal Response to Domestic Incidents

Many of the programs authorized under the 9-11 Commission Act provide a framework for organization with regard to coordinated security planning and incident response. Interagency coordination, and coordination with industry stakeholders through the existing frameworks of the Mass Transit SCC, SDO, and ISAC, all provide opportunities for improvement in this area.

A number of our member agencies have strong emergency response exercise programs and this same DHS-supported effort should be expanded to other transit agencies. The most effective method for determining the effectiveness of plans is to put them to an actual test. While DHS has undertaken very large scale exercises through programs such as "TOPOFF", it would be advisable to expand the nationally sponsored drills and exercises to test on smaller scales as well and to alternate the focus of the drills so that each of the critical infrastructures can be effectively included.

Capacity to Coordinate Stakeholder Efforts to Respond to Domestic Incidents

One of the weaknesses we see under current law particularly applies to federal coordination with transit industry partners and the application of the DHS/FEMA "All Hazards" approach to policy. As elements of state, regional and local government, transit systems throughout the country have historically and regularly assisted in the response to natural disasters. As a result, transit systems capacities and needs should be considered during any and all planning for preparedness, response and recovery.

APTA member systems have assisted directly with the response to numerous natural disasters over the last decade, including Katrina/Rita, flooding in the Midwest states, the Northridge earthquake, and forest fires in the Western states. This is certainly in addition to our response to the terrorism-induced disaster of September 11th. It was our response to 9-11 that led many of us in the industry to truly view our transit employees as "First Responders". There are many areas where federal assistance and improved collaboration could enable the transit industry to provide greater support and assistance to communities affected by natural disasters.

APTA strongly supports the concept of planning for incidents from an "All Hazards" perspective. It has been our experience that often the same technologies, plans and resources that are brought to bear in addressing a security incident are similar to those that are required in other forms of incidents and emergencies. Consequently, economies and efficiencies can be realized where grants that are currently narrowly restricted only for counterterrorism application can be utilized to also address other hazards. We would therefore encourage that the use of DHS grants be expanded to enable such broader and more complete application, with, of course, the appropriate justifications being provided.

CONCLUSION

In light of the nation's heightened security needs since 9/11, we believe that increased federal investment in public transportation security is critical. The public transportation industry has made great strides in transit security improvements since 9/11 but much more needs to be done. We need the federal government to increase its support for transit security grants that help transit systems address the \$6 billion in identified transit security investment needs. We urge Congress and the Administration to fully fund and implement the provisions set out in the 9/11 Commission Recommendations Act. It should also be understood and appreciated that investment in public transit security programs, resources and infrastructures provides a direct benefit in preparation and response to natural disasters as well.

We thank you for the opportunity to submit testimony on the security needs of our nation's transit agencies and their riders. We thank you for everything Congress has done to date leading to improvements and efficiencies that will, in turn strengthen the safety and security for the millions of people who use transit every day.

Corporate Headquarters
 616 Innovation Drive
 Chesapeake, VA 23320
 Office: 757.312.0790
 Fax: 757.312.0795
 www.ursanav.com



DC Metro Operations
 11654 Plaza American Drive
 #555
 Reston, VA 20190
 Office: 703.957.6401
 Fax: 757.312.0795

May 8, 2009

The Honorable David E. Price
 Chairman
 Subcommittee on Homeland Security
 House Committee on Appropriations
 B-307 Rayburn House Office Building
 Washington, DC 20515

The Honorable Harold Rogers
 Ranking Member
 Subcommittee on Homeland Security
 House Committee on Appropriations
 1016 Longworth House Office Building
 Washington, DC 20515

Subject: **eLoran should be maintained** as Critical Standalone Backup to GPS

Dear Chairman Price and Ranking Member Rogers:

UrsaNav is a *Veteran-Owned* and *Service-Disabled Veteran-Owned Small Business* that provides advanced engineering and IT products and solutions for the homeland security, critical infrastructure protection, and national defense markets. Our focus is on developing and deploying solutions for interference-enabled crime fighting, counterinsurgency operations, irregular warfare, and legacy transformation. Enhanced Loran (eLoran) is a key component of our solutions package for these critical areas.

On February 7, 2008, the Department of Homeland Security announced their commitment to eLoran as the backup system to GPS to ensure continuation of critical national infrastructure during GPS outages. The 2008 U.S. Federal Radionavigation Plan, just released by the Obama administration in February of this year, ties DHS's decision to the findings of the recently released Institute for Defense Analysis' Independent Assessment Team (IAT) report, and the endorsement of the U.S. National Space-based Position, Navigation, and Time (PNT) Executive Committee in March, 2008. In part, the IAT found:

- Assurance of national GPS-based Position, Navigation, and Time (PNT) availability to meet critical national and economic security is prudent and responsible policy,
- eLoran is the only cost-effective, seamless PNT backup for national needs that is completely interoperable with and independent of GPS, and
- U.S. Government policy decisions are necessary to motivate users to equip and to demonstrate continued leadership internationally.

Finally, in their conclusions, the IAT unanimously recommended that the U.S. Government complete the eLoran upgrade and commit to eLoran as the national backup to GPS for the next 20 years.

The U.S. and international community applauded the February 2008 U.S. decision. It was well timed to take advantage of European developments that had demonstrated the exceptional value-for-money and high performance of minimally-manned eLoran stations. For instance, the United

Kingdom recently established a new automated eLoran station that will operate with stations in Norway and France. The U.S. DHS announcement stimulated government eLoran investment decisions and development activities worldwide.

Based upon Congressional and international commitment to eLoran, private companies such as ours invested in eLoran product and service offerings. We subsequently established and solidified the United States' position as the global leader for the eLoran industry in engineering, product development, and manufacturing, and created hundreds of American high-tech jobs. We need your help in ensuring the U.S. does not lose its eLoran leadership position.

On behalf of our employees, we strongly encourage your continued support for funding to: (1) continue operation of the U.S. Loran-C system until it is upgraded to Enhanced Loran (eLoran) standards, (2) speedily transition to the eLoran position, navigation, timing, and data (PNT&D) system in the U.S., (3) fulfill existing international agreements to operate Loran and, in the future, eLoran across our land and sea borders with Canada and Russia, and (4) implement the latest technologies to make the eLoran system more efficient and capable of outsourcing to significantly reduce total cost of ownership.

GPS is ingrained in our lives like time, electricity, and water. Without it, there could be chaos in many sectors simultaneously. Filling gaps in GPS service to the public and private sectors using eLoran is a necessary component of our ability to always be prepared. Please refer to the Appendix for additional details.

In closing, I want to thank you and the committee for the opportunity to present our statement and for your leadership in this critical area of national security. I would be delighted to meet with your staff at any time to discuss how we might work together to achieve this goal. I can be reached at 703.623.5212 or Email: cschue@ursanav.com. Our website can be viewed at www.ursanav.com.

Very Best Regards,



Charles Schue
President & CEO

Appendix: (1) White Paper on (e)Loran

APPENDIX: WHITE PAPER ON eLORAN

SUBMITTED BY:
CHARLES SCHUE, PRESIDENT & CEO

URSA NAV, INC.
 616 INNOVATION DRIVE
 CHESAPEAKE, VA 23320

PHONE: 757.312.0790 X205
 EMAIL: CSCHUE@URSANAV.COM

On Friday, April 24, 2009, a seemingly innocuous navigation problem created some tense moments in Washington, D.C. The White House and Capitol Hill were evacuated after a small airplane strayed into restricted airspace because the pilot's *GPS system stopped working*. Publicly the Departments of Defense, Transportation, and Homeland Security all suggest that "if GPS fails, there are other systems that back it up besides Loran." Where exactly were those backup systems when two fighter jets and two United States Coast Guard helicopters were dispatched to intercept the aircraft? Loran was available, but the aircraft owner did not have a backup navigation receiver on board. This is most probably because the government's inconsistent policies on Loran and eLoran have deterred the pilot from investing in technology that uses the nation's only independent, complementary, multi-modal GPS backup.

A simple web search will reveal many other unclassified incidents or anomalies, most of which are significantly more troublesome. Equipment failure, interference, jamming, spoofing, weather (terrestrial and solar), and terrain are issues with any Position, Timing, or Navigation (PNT) system. That is why any prudent operator has a backup system, preferably one that has dissimilar failure modes than the primary system. As a nation, we are moving towards a sole-means PNT solution that has no multi-modal backup: the Global Positioning System (GPS).

The reality is that GPS is ingrained in our society like time, electricity, and water. It touches our lives every day in ways we might not even realize. High profile examples of our dependence upon this technology include:

- Telecommunications
- Military Combat Systems
- Electric Power Delivery Systems
- Criminal Tracking Systems
- Maritime Domain Intelligence
- Personal/Vehicle Navigation
- Aircraft/Maritime Navigation
- Hazardous Material Tracking
- Financial Transactions
- Automotive Telematics
- Highway Toll Systems
- First Responders

An interruption to GPS service could have a significant negative impact on the U.S. economy and, possibly, the safety of U.S. citizens. Chaos could occur in many sectors at the same time. We are not aware of any plan by the Administration for dealing with a localized or widespread GPS anomaly. Without a backup system, we are creating a vulnerability that could embarrass this Administration, endanger our citizens, and cripple our economy. Enhanced Loran, or eLoran, is the only multi-modal backup to GPS, is completely independent and complementary to GPS, fills gaps in GPS service, and yet it is in danger of being terminated!



GPS is vulnerable. This simple statement of fact, known worldwide, is documented in many scientific, industry, and government reports and papers. These concerns are driving the investment of billions of dollars worldwide to mitigate the vulnerabilities. China, Russia, Japan, France, the UK, and India have all stepped out and are making significant investments in technology infrastructure to protect themselves from GPS outages. They are developing, or upgrading, their own Global Navigation Satellite Systems (GNSS): Beidou, Galileo, GLONASS, QZSS, and GAGAN, respectively. Further, many nations, including the U.S., are investing in GNSS/GPS augmentation systems to overcome system deficiencies. These augmentations include the Wide Area Augmentation Systems (WAAS), Local Area Augmentation System (LAAS), Differential Global Positioning System (DGPS), European Geostationary Navigation Overlay Service (EGNOS), and the Multi-Functional Satellite Augmentation System (MSAS).

However, for as much as these augmentations will help alleviate some system deficiencies, a failure of the primary GNSS service results in the unusability of the associated augmentation systems. Therefore, these same foreign nations, along with at least ten others, continue to operate and invest in Loran-C and Enhanced Loran (eLoran) as the best independent, complementary backup to GNSS/GPS. While the rest of the world is moving forward with protecting their national infrastructure, the U.S. continues to waffle. Our lack of commitment to a comprehensive PNT solution results in negative impacts inside the government, to the U.S. economy, and to the U.S. world leadership in the PNT community.

At the Congressional level, discontinuing Loran is a two pronged issue: the "decision", and continued system funding. While the official decision and announcement of the continuation of the eLoran system as the long term backup to GPS is the most crucial, the modernization funding is also critical.

Most government sponsored studies agree that eLoran should be designated as the standalone backup to GPS until, and unless, another backup alternative is developed. The Loran modernization effort should continue until the system is: (1) fully converted to eLoran using the most current technology available, (2) current in its infrastructure maintenance (buildings, runways, antennas, etc.), and (3) capable of unmanned or minimally manned operation.

Why should the American Citizen care? We are very aware of the tremendous economic benefits of GPS: carefree position, navigation, and timing. Less well known is what happens when GPS is not available. In a world of intentional and unintentional interference, jamming, and spoofing, which component of our nation's critical infrastructure are we willing to live without: communications or navigation?

Additionally, although only a small fraction when compared to the GPS economic engine, 90 percent of the world's Loran industrial base is located within the U.S. Contrary to popular belief, today's Loran is not antiquated. The modernized eLoran system consists of leading edge technology such as atomic-clock based precision timing systems, state-of-the-art high-powered transmitters, and sophisticated command and control infrastructure. The personnel operating and maintaining these systems are electronics, IT, civil, and mechanical engineering specialists. Especially in these tough economic times, it seems ludicrous to strangle the high-technology small businesses that provide eLoran products and services.

What are the estimated non-recurring and recurring costs? Loran's current annual operating cost is between \$36M and \$54M. Current technology, when applied to the eLoran system

modernization, is capable of providing significant operational efficiencies and improvements, while concurrently reducing its annual total cost of ownership by at least fifty percent.

Who are the players? The U.S. portion of the North American Loran system is operated by the Coast Guard. U.S. radionavigation policy and planning for Loran is provided in the Federal Radionavigation Plan (FRP). The FRP is jointly prepared by the Departments of Defense, Homeland Security, and Transportation. The U.S. has international agreements in place with Canada and Russia for interconnecting and operating Loran across these important borders. Thus, the U.S. Department of State also has an interest in Loran policy and decisions.

Who should the money go to? Current operating funds for Loran are part of the Coast Guard's annual budget. Recapitalization and modernization funds have historically been provided to the Federal Aviation Administration (FAA). An interagency agreement between the FAA and the Coast Guard determines the modernization project slate each year, based upon funding (if any) that Congress provides. Any subsequent funding should be provided directly to the Coast Guard, as long as (1) it is identified as specifically applicable to Loran recapitalization and modernization to eLoran, (2) the multiple modes (aviation, maritime, land mobile, location based, precision time and frequency) served by the system are represented, and (3) the system is completely converted to eLoran and fully operational as soon as practical.

What efforts are required moving forward? A U.S. decision as to the future of Loran is required.

Immediate: Funding for an eLoran Program should be inserted into the FY10 Budget. Some momentum has been lost with the lack of consistent modernization funding. However, it is possible to leverage new technology and knowledge to rapidly complete the transition of our nation's Loran system to eLoran, and to increase system efficiency through unmanning the Loran system, thereby freeing up these assets for other critical Coast Guard programs.

Establishing an eLoran Program allows for consistent implementation of Congressional goals, coordination and cooperation between affected stakeholders, measurement towards completion of those goals, and conservation of funds. Specific program goals should include, in no particular order:

- Providing government leadership and representation at international eLoran organizational conferences and meetings.
 - Providing government leadership and representation for international standards development for the eLoran system, user equipment, and testing.
 - Providing high-speed data transmission capability using the eLoran signal, but without affecting PNT users.
 - Supporting submission of requisite eLoran standards to international bodies, such as the IMO, IEC, ITU, NMEA, RTCM, and RTCA.
 - Speedily completing the transition to eLoran.
 - Relocating the Port Clarence, AK station to a site in Nome, AK.
 - Relocating the Attu, AK station to a site on nearby Shemya Island, AK.
 - Installing Differential eLoran monitor sites at critical harbors, airports, and other high-risk transportation nodes.
 - Upgrading, replacing, or removing existing monitor sites, as necessary.
-

- Gathering and validating information to develop accurate ASF correction databases.
- Upgrading site infrastructure and providing associated site hardening, to allow for unmanned or minimally manned operation.
- Providing assistance to legacy Loran users in converting to eLoran.
- Augmenting existing sites, or adding sites, as necessary to provide complete coverage of the U.S., including Hawaii, Puerto Rico, and other areas where U.S. critical infrastructure requires the protection of alternative PNT services.
- Outsourcing operations and maintenance of the system while retaining oversight and quality control.

Long Term: An incontrovertible decision and announcement on eLoran's continued role in the Federal Radio Navigation Plan and assurance of adequate annual operating and maintenance funding is necessary.

Active support is required to ensure the eLoran system continues to be a part of the U.S. critical national infrastructure. The following bullets are specific actions that are required.

- Support continued Operations and Maintenance (O&M) funding, beginning with the FY10 budget.
 - Support additional funding in the FY10, and subsequent, budget for a speedy transition to eLoran.
 - Continue to rebuff any attempt to terminate the system.
 - Push for a long term commitment to eLoran and a final U.S. policy decision supporting the operation of eLoran until and unless a more capable backup solution to GPS is developed.
-



**Statement for the Record
For the
Subcommittee on Homeland Security
Committee on Appropriations
U.S. House of Representatives**

**On the FY 2010 Appropriations
For the Federal Emergency Management Agency
Department of Homeland Security**

**By
Russell Decker CEM
President
United States Council of the International Association of Emergency
Managers**

April 30, 2009

Chairman Price, Ranking Member Rogers, and distinguished members of the Subcommittee, thank you for allowing me the opportunity to provide a statement on critical budget and policy issues for the Federal Emergency Management Agency/ Department of Homeland Security. After the President's budget request is submitted next week, we would appreciate the opportunity to provide additional comments if we have concerns.

I am Russ Decker, the Director of Emergency Management and Homeland Security for Allen County, Ohio. Allen County is a mid-size rural county in northwest Ohio with a population of just over 100,000. I serve as the President of the United States Council of the International Association of Emergency Managers (IAEM-USA). I have 19 years of emergency management experience, with the last ten as a local director. I have also served as President of the Emergency Management Association of Ohio.

IAEM-USA is our nation's largest association of Emergency Management professionals, with more than 4,000 members including emergency managers at the state and local government levels, tribal nations, the military, colleges and universities, private business and the nonprofit sector. Most of our members are city and county emergency managers who perform the crucial function of coordinating and integrating the efforts at the local level to prepare for, mitigate the effects of, respond to, and recover from all types of

disasters including terrorist attacks. Our membership includes emergency managers from large urban areas as well as rural areas.

We deeply appreciate the support this subcommittee has provided to the emergency management community over the past few years, particularly your support for the Emergency Management Performance Grant Program as well as strengthening FEMA. We have also appreciated your continued direction to DHS and FEMA to consult with their primary local and state stakeholders.

Emergency Management Performance Grants (EMPG)

We urge that EMPG funding be increased to a minimum of \$487 million, that the program be retained as a separate account, and that Congress continue to include language making it clear that the funding is for all hazards and can be used for personnel.

EMPG which has been called “the backbone of the nation’s emergency management system” in an Appropriations Conference Report constitutes the only source of direct federal funding for state and local governments to provide basic emergency coordination and planning capabilities for all hazards including those related to homeland security. The program supports state and local initiatives for planning, training, exercise, mitigation, public education, as well as response and recovery coordination during actual events. All disasters start and end at the local level, which emphasizes the importance of building this capacity at the local level. Funding from EMPG frequently makes a difference as to whether or not a qualified person is present to perform these duties in a local jurisdiction.

We appreciate that the Subcommittee has recognized that EMPG is different from all the other post September 11, 2001 homeland security grants. Specifically, EMPG has existed since the 1950s. It was created to be a 50-50 cost share program to ensure participation by state and local governments to build strong emergency management programs. The program has been under funded for decades and remains so today.

The program is authorized at \$680 million in PL 110-53. The legislation creating EMPG is purposefully broad to allow jurisdictions to focus their attention on customizing capabilities for each local jurisdiction. Therefore, FEMA’s guidance should not try to make one size fit all, but should be written so as to allow maximum flexibility in meeting the specific capability requirements within each local jurisdiction.

Funding from EMPG has always been important to local government emergency management offices, but it is becoming even more so during the current economic downturn. Many of our IAEM-USA members have told us that their programs are facing budget reductions which will result in reduced staffing, reduced or eliminated training, and reduced public outreach. Perhaps most importantly, our members have told us that many emergency management programs are at the point where local elected officials are considering reducing their commitment from a full time emergency manager

to a part time emergency manager, or moving the emergency management functions as added duties to other departments. This will have the effect of actually reducing emergency management services in many areas of the country – all this at a time when disasters and emergencies threaten more people and property than ever before.

Many local emergency management programs have historically provided significantly more than the 50% match that is required for their EMPG allocations. Simply receiving all of the 50% Federal match of their contributions would make a big difference in maintaining their programs.

Emergency Management Institute (EMI)

We urge the Subcommittee to provide needed additional funding to update the key emergency management courses of the EMI curriculum and develop new ones, to provide additional personnel required to handle the workload associated with updating and developing new courses, to support technology upgrades, and to support the Emergency Management Higher Education Program. We would also suggest that funding be provided to review and modernize the Integrated Emergency Management Course (IEMC) which trains the leadership of communities to respond. We would respectfully suggest that the Subcommittee request that FEMA provide information on the funding necessary to accomplish these tasks.

We appreciated the additional \$1.253 million in EMI funding provided by Congress in FY 2009 and your direction that detailed budget information on EMI be included in the Congressional budget justification for FY 2009.

The Emergency Management Institute (EMI) provides vitally needed training to State and local government emergency managers through on-site classes and distance learning. This “crown jewel” of emergency management training and doctrine has suffered from lack of funding and loss of focus on the primary objectives of the Integrated Emergency Management System (IEMS).

A renewed focus on continuing education for professional emergency managers is vital. EMI core curriculum, including the Master Trainer Program, E-Courses and G-Courses are essential to the professional development of career emergency managers and to support state level training programs.

We also continue to support the highly successful Emergency Management Higher Education Program at EMI. This program, though underfunded, has produced significant improvements in the preparation of emergency managers at the over 160 colleges and universities now offering emergency management academic programs. In addition they interact with over 400 colleges and universities. The program has also established and maintained the essential collaboration between emergency management practitioners and the academic and research disciplines so essential to a comprehensive approach to emergency management. To continue to achieve these results and accomplishments and

further advance the Higher Education Program, it is necessary to augment the existing two person staff.

PreDisaster Mitigation (PDM)

We urge the Subcommittee to support this program at an appropriate level. Many more applications are received than there is funding to support.

The program will sunset on September 30, 2009. A reauthorization bill has passed the House and we will be working with the Senate to support the continuation of the program.

Principal Federal Official (PFO)

We urge the Subcommittee to again include bill language prohibiting the funding of any position designated as a Principal Federal Official (PFO) or Senior Federal Official for any Stafford Disaster Relief declared disaster or emergency.

IAEM has consistently opposed the appointment of PFOs. It leads to confusion. Instead, our members want the Federal Coordinating Officer (FCO) to have unambiguous authority to direct and manage the federal response in the field. It is absolutely critical for state and local officials to have one person empowered to make decisions and coordinate the federal response in support of the state.

Professional Emergency Managers

IAEM-USA applauds the President's selection of Craig Fugate to be the next Administrator of FEMA and Tim Manning as Deputy Administrator for National Preparedness. Both of these individuals represent actual emergency management practitioners from the local and State government arena. They bring a wealth of professional credentials, experience, and a seasoned understanding of the importance of the partnerships required between local, State and the Federal Government for effective emergency management. We look forward to working with Craig and Tim and other members of the new leadership team at FEMA and anticipate an expanded level of dialogue between FEMA leadership and the stakeholders at the local and tribal levels.

Review of Programs

The arrival of these new, experienced and professional emergency managers to positions of leadership within FEMA offers an ideal opportunity for FEMA to do a comprehensive and critical reexamination of several functions and programs established and partially implemented toward the end of the last Administration. Some of the programs appear to be increasing the burden of "unfunded mandates" on state and local agencies without providing value or meeting the needs of FEMA's customers. Over the last two years, IAEM has been asked to review and comment on a number of such initiatives. While we took a positive attitude and tried to suggest ways to make them more effective and "reality-based", the underlying concepts driving some of these initiatives appeared to us

to be fundamentally flawed. Two of the initiatives that require immediate review are the GAP analysis and the Integrated Planning System (IPS). For example, IPS should be reviewed to determine if it fully meets the needs of local, state and federal disaster planners. The current version, based heavily on the DOD Joint Operations Planning and Execution (JOPES) model may be a great model—if you are the military and funded and equipped with the resources of the military. State and local governments do not have that luxury. We urge Congress to work with the new leadership of FEMA and to support a much needed “reality check,” in the form of a comprehensive program review, to ensure that FEMA is making the most of its resources.

Implementing Legislation to Strengthen FEMA

IAEM-USA strongly supports the full implementation of Post-Katrina Emergency Management Reform Act (PKEMRA), PL 109-205, and we urge the Subcommittee to support the efforts of Craig Fugate, Tim Manning, and the other new leaders of FEMA by insisting on its implementation. There must be a return to established emergency management doctrine within FEMA – all hazards, integrated, all phases (preparedness, mitigation, response, and recovery).

The FEMA Administrator should have the maximum amount of access to the White House and the FEMA Administrator should be clearly responsible for the coordination of the Federal response to disasters as the legislation clearly requires. Homeland Security Presidential Directive-5 and Homeland Security Presidential Directive-8 should be revised to conform to the requirements of PKEMRA.

All elements of preparedness must be returned to FEMA to comply with PKEMRA. Functions that are duplicative or possibly competing with those of FEMA should not be established and funded in other DHS offices. For example, the Office of Operations Coordination was created shortly after the enactment of PKEMRA and it was assigned several responsibilities that PKEMRA assigned to FEMA notwithstanding PKEMRA’s prohibition on transferring functions, responsibilities, etc. outside of FEMA. These include, but are not limited to coordinating activities related to incident management, the national planning scenarios, the Integrated Planning System, and duplicating the role of the Office of Disaster Operations in FEMA. It is unclear what the roles are of the National Operations Center and the National Response Coordination Center in managing the coordination of the Federal Response in preparation for responding to an event.

An example of the problems caused by duplication of FEMA services within DHS is the discussion regarding the perceived differences between Incident Management and Emergency Management. Emergency Management is the broader, overarching and systematic approach to the issue of dealing with the consequences of all disasters and emergencies, whether natural, technological, or homeland security. Incident management, while important, is a much more narrowly focused sub-element of response, one of the four phases of emergency management (mitigation, preparedness, response and recovery). Functions clearly and unambiguously assigned to FEMA by law

should not be moved out or duplicated on the basis that the Administrator of FEMA is the lead “only” in Emergency Management, not incident management.

Congress rejected the DHS Stage 2 Reorganization and clearly and unambiguously moved all Preparedness functions and personnel to FEMA. IAEM-USA believes that Section 506 (c) (1) and (2) of the Homeland Security Act as amended by the Post Katrina Reform Act clearly prohibits the transfer of any asset, function or mission from FEMA without a specific Act of Congress. A major function of FEMA is to rebuild relationships with State and local officials. Therefore, the Intergovernmental Affairs function assumes a much higher level of importance. Despite the clear prohibition on moving this function from FEMA, we understand there are still 11 positions performing this vital role still under the National Protection and Programs Directorate (outside of FEMA) on a non-reimbursable detail. These positions and funding should be immediately transferred to FEMA for the intergovernmental affairs office at FEMA.

Conclusion

In conclusion, we urge the Subcommittee to continue to build emergency management capacity by increasing EMPG to \$487 million. We urge increased funding for the Emergency Management Institute. Congress passed the PKEMRA to give FEMA the clear authority and tools to do its job and put a fence around it to give protection for its mission and resources. We urge the Subcommittee to insist on the appropriate implementation of the Act.

Contact information:

International Association of Emergency Managers, 201 Park Washington Court, Falls Church, VA. 22046. Telephone: 703 538 1795

Government Affairs Chair: Randy Duncan (rduncan@sedgwick.gov)

Policy Advisor: Martha Braddock (braddock@iaem.com)



Statement of the Fleet Reserve Association
On the

Fiscal Year 2010 U.S. Coast Guard Budget

Submitted to

Subcommittee on Homeland Security
Appropriations Committee
United States House of Representatives

April 22, 2009

THE FRA

The Fleet Reserve Association (FRA) is the oldest and largest enlisted organization serving active duty, Reserves, retired and veterans of the Navy, Marine Corps, and Coast Guard. It is Congressionally Chartered, recognized by the Department of Veterans Affairs (VA) as an accrediting Veteran Service Organization (VSO) for claim representation and entrusted to serve all veterans who seek its help. In 2007, FRA was selected for full membership on the National Veterans' Day Committee.

FRA was established in 1924 and its name is derived from the Navy's program for personnel transferring to the Fleet Reserve or Fleet Marine Corps Reserve after 20 or more years of active duty, but less than 30 years for retirement purposes. During the required period of service in the Fleet Reserve, assigned personnel earn retainer pay and are subject to recall by the Secretary of the Navy.

FRA's mission is to act as the premier "watch dog" organization in maintaining and improving the quality of life for Sea Service personnel, their families and survivors. In addition to serving as a leading advocate on enlisted personnel and quality of life programs on Capitol Hill the Association also sponsors a National Americanism Essay program, awards over \$100,000 in scholarships annually and provides disaster and/or relief to shipmates and others in distress.

The Association is also a founding member of The Military Coalition (TMC), a 35-member consortium of military and veteran's organizations. FRA hosts most TMC meetings and members of its staff serve in a number of TMC leadership roles.

FRA celebrated 84 years of service in November 2008. For over eight decades, dedication to its members has resulted in legislation enhancing quality of life programs for Sea Services personnel, other members of the Uniformed Services plus their families and survivors, while protecting their rights and privileges. CHAMPUS, now TRICARE, was an initiative of FRA, as was the Uniformed Services Survivor Benefit Plan (USSBP). More recently, FRA led the way in reforming the REDUX Retirement Plan, obtaining targeted pay increases for mid-level enlisted personnel, sea pay for junior enlisted sailors and hazardous duty incentive pay for U.S. Coast Guard boarding teams. FRA also played a leading role in successfully advocating for predatory lending protections for service members and their dependents.

FRA's motto is: "Loyalty, Protection, and Service."

**CERTIFICATION OF NON-RECEIPT
OF FEDERAL FUNDS**

Pursuant to the requirements of House Rule XI, the Fleet Reserve Association has not received any federal grant or contract during the current fiscal year or either of the two previous fiscal years.

INTRODUCTION

Mr. Chairman and distinguished members of the Subcommittee, the Fleet Reserve Association (FRA) appreciates the opportunity to present its recommendations on the United States Coast Guard's FY 2010 Budget.

Prior to addressing these issues, FRA wishes to thank Congress for the generous pay, health care and benefit enhancements enacted in recent years. Improved wounded warrior transition and support services are very important as are other benefit improvements which are essential to maintaining the all-volunteer force and military readiness.

Funding parity with DoD for US Coast Guard personnel programs remains a high priority for FRA, and the Association notes continuing challenges within the Coast Guard to adequately fund previously authorized active and Reserve people programs. The Coast Guard is a small service but has a huge impact on the daily lives of our citizens.

COAST GUARD BUDGET

Although details regarding the Administration's FY 2010 Budget are unknown at this point, the Association appreciates the \$9.36 billion FY 2009 appropriation for the Coast Guard, which is \$290 million above the Administration's request, and \$729 million above FY 2008. The spending bill included \$97.6 million for new Coast Guard Headquarters in Washington, DC.

US COAST GUARD AUTHORIZATION

FRA supported the US Coast Guard Authorization (H.R. 2830 and S. 1892) from the 110th Session and is concerned that the proposals are stalled over several different issues. The Association believes that authorization legislation is fundamental to Congressional budgeting and effective oversight of federal agencies, and is encouraged to hear that the new Administration will offer new Coast Guard Authorization legislation this year.

The legislation from the last Congress addressed several important personnel related issues. These include emergency leave retention authority whereby service members would be allowed to retain leave they would otherwise forfeit due to support of major disasters or other emergencies declared by the President; legal assistance authority for Coast Guard Reservists that establishes parity among all similarly situated Reservists who have served on active duty for more than 30 days under mobilization authority and makes them eligible for legal assistance upon release from active duty; and authority for reimbursement for certain medical-related travel expenses when a service member is stationed on an INCONUS island and his/her family member is referred to a specialty care provider off-island that is less than 100 miles from the primary care provider.

In addition, both bills authorized end strength of 45,500, and made Coast Guard retirees eligible for the Armed Forces Retirement Home (AFRH). The Senate bill included a policy change authorizing recreational facilities to be included in the public/private

venture (PPV) program similar to service housing projects. The Senate bill also changed the vice commandant position from a 3-star position to a 4-star position, which will better align the Coast Guard with the other armed forces.

END STRENGTH

According to the 2009 U.S. Coast Guard Posture Statement, the Coast Guard end strength is currently at 41,873 active duty, 8,100 Reservists, 7,000 civilian employees, and 34,000 volunteer Auxiliarists and has been at that level for several years even though the Coast Guard has been tasked with additional responsibilities in recent years. The Coast Guard took over the National Capitol Region Air Defense (NCRAD) mission in September of 2006, and there have been increased demands with the passage of “The Coast Guard and Maritime Transportation Act of 2006.” Even a modest increase to active duty end strength in FY 2010 would immediately translate to a higher level of mission effectiveness. FRA supports adequate manpower to meet growing operational requirements and notes there are annual limits to increasing Coast Guard end strength because of recruiting and training limitations. According to Admiral Thad Allen, Commandant of the Coast Guard, in his 2008 State of the Coast Guard Address, “There has been no material change in the Coast Guard’s end strength in the past 50 years despite more demands and the current era of persistent challenges.”

PAY

Congress has for the past few years improved compensation that, in turn, enhanced the recruitment and retention of quality personnel in an all-volunteer environment. Adequate and targeted pay increases for middle grade and senior petty and noncommissioned officers have contributed to improved retention, morale and readiness. More than 50 percent of the uniformed service community is married and satisfactory compensation helps relieve much of the tension brought on by demanding operational tempos.

For FY 2010, the Administration recommended a 2.9 percent across-the-board basic military pay increase which is equal to the Employment Cost Index (ECI). FRA strongly supports pay increases that are at least 0.5 percent above the ECI (3.4 percent in FY 2010) to close the gap between civilian and uniform services pay. Previous annual 0.5 percent higher-than-ECI raises reduced the pay gap with the private sector from 13.5 percent in FY 1999 to 2.9 percent today.

Assuming authorization by the Armed Service Committee, FRA urges the Subcommittee to authorize funding of annual active duty pay increases that are at least 0.5 percent above the ECI, to help close the pay gap between active duty and private sector pay and ensure adequate appropriations to fund these increases in the Coast Guard’s budget.

HEALTH CARE

The FRA strongly supports adequate funding for the Coast Guard Health Care Fund (HCF) in order to meet readiness needs, fully fund TRICARE, and improve access for all beneficiaries regardless of age, status or location. The Association is concerned that the new Administration's FY 2010 budget may include significant TRICARE fee increases paid by retired uniformed services beneficiaries. The FRA believes strongly that these proposed increases are disproportional, inequitable, inappropriate and unwise.

Eroding benefits for career service can only undermine long-term retention and readiness. The men and women serving in the Coast Guard today are very conscious of actions by Congress affecting those who preceded them in service. One reason Congress enacted TRICARE-for-Life (TFL) in 2001 is that the Joint Chiefs of Staff at that time said that inadequate retiree health care was affecting attitudes among active duty troops. The FRA believes strongly that the Defense Department has not sufficiently investigated and implemented other options to make TRICARE more cost-efficient without shifting costs to beneficiaries, and strongly supports bipartisan legislation sponsored by Representatives Chet Edwards' and Walter Jones' ("The Military Retirees Health Care Protection Act" H.R. 816).

Due in large part to the unique range of geographic locations to which they are assigned, Coast Guard personnel and their families often struggle to find medical providers who accept TRICARE beneficiaries. While implementation of TRICARE Prime Remote alleviated many of these problems, costs associated with the standard benefit and low reimbursement rates can make finding a health care provider a daunting task in many areas. And, Coast Guard personnel who choose to receive care at DoD Military Treatment Facilities (MTFs) may have to travel long distances for care. FRA is concerned that low reimbursement rates will continue to make health care access a significant challenge for Coast Guard personnel stationed in remote locations.

The FRA urges the Subcommittee to authorize full funding for health care benefits to ensure access for all beneficiaries, and support "The Military Retirees Health Care Protection Act" (H.R. 816).

Reserve issues

Reserve Health Care – FRA is grateful to Congress for allowing Reservists to purchase TRICARE Reserve Select (TRS) coverage per the FY 2007 National Defense Authorization Act, (NDAA). We also appreciate the provision in the FY 2009 NDAA that mandates recalculation of TRICARE Reserve Select (TRS) premium to reflect actual costs. The Association believes it should be a priority to restrain health cost increases for TRICARE Select Reserve members who are increasingly being asked to serve their country.

FRA notes that TRICARE Reserve Select for gray area retirees is something on the minds of CG Reservists and this may become a recruiting and retention issue in the future as members realize that by buying into TRICARE during their service time could

potentially leave them without coverage in the future. FRA supports authorization and funding that allows Reserve personnel and their families participate in TRICARE.

Reserve Early Retirement- Unfortunately the effective date of a key provision in the FY 2008 NDAA, which reduces the Reserve retirement age by three months for each cumulative 90-days ordered to active duty is effective upon the enactment of the legislation and NOT retroactive to 7 October 2001. This issue is addressed in the “The National Guardsmen and Reservists Parity for Patriots Act” (H.R. 208), sponsored Rep. Joe Wilson (S.C.), and companion legislation in the Senate (S. 644) is sponsored by Senator Saxby Chambliss (Ga.). If enacted commensurate funding for this should be included in the U.S. Coast Guard budget.

The 2008 NDAA authorized a stipend of \$300 for targeted billets to receive reimbursement for Inactive Duty for Training (IDT) travel and funding was not provided. The Coast Guard needs the ability to have the right people in the right places. The authority to pay for IDT travel needs to be expanded, but more importantly the Congress must provide the funding to support this important readiness tool.

The Association notes that the USCGR is authorized an end strength of 10,000, but funded for only 8100. FRA believes we cannot sustain current services in support of military requirements without the funding necessary to increase end strength over the next few years.

HOUSING

The Coast Guard currently owns 4,000 family homes, at an average age of 40+ years, with an extensive maintenance and recapitalization project backlog. The costs are compounding and funds are not available to keep pace for adequate maintenance and replacement. If authorized, FRA supports Coast Guard initiatives to improve family housing. DoD has privatized approximately 85 percent of their homes using public-private venture (PPV) authorities; however, the Coast Guard has not been able to leverage the same equity and needs adequate resources to do so.

FRA urges reform of housing standards that inequitably depress Base Allowance for Housing (BAH) rates for mid-to-senior enlisted members. The vast majority of Coast Guard personnel and their families use private housing and collect BAH and FRA believes that there is an urgent need to update the standards used to establish housing allowance rates. Only married E-9s now qualify for BAH based on local single family home costs. At a minimum, the BAH standard for a single-family detached house should be extended over several years to qualifying service members beginning in grade E-8 and subsequently to grade E-7 and below as resources allow. If authorized by the Armed Services Committee, FRA strongly urges commensurate authorization and funding in the Coast Guard budget.

PERMANENT CHANGE OF STATION (PCS) ALLOWANCES

The Association urges this Subcommittee to be aware of the need to upgrade permanent change-of-station (PCS) allowances to better reflect the expenses Coast Guard members are forced to incur while complying with government-directed relocation orders. And if enhancements are authorized by the Armed Services Committees, FRA urges funding in the Coast Guard's budget to fund these enhancements.

Shipment of POVs –FRA supports increasing the number of privately owned vehicles (POV) a military family can ship during a PCS from one vehicle to two for duty assignments in Alaska, Hawaii and US Territories. This is an issue of particular concern to Coast Guard personnel stationed in these locations since many married personnel have spouses who need transportation to work, and meet family obligations

Weight Allowances – FRA also recommends modifying PCS household goods weight allowance tables for personnel in pay grades E-7, E-8 and E-9 to coincide with allowances for officers in grades O-4, O-5, and O-6, respectively. These allowances would more accurately reflect the normal accumulation of household goods over the course of a career.

Dislocation Allowance – Moving household goods on government orders can be costly. Active duty personnel endure a number of permanent changes of station (PCS) during a career in uniform. Each move requires additional expenses for relocating and establishing a new home.

Retiring personnel are *not* currently entitled to a dislocation allowance despite the fact that his or her orders can be construed as a permanent change of station that reflect a management decision to order the member's retirement or transfer. Providing the member is moving to a new location, the retiring Coast Guardsman will face the same expenses as if transferring to a new duty station.

If authorized, FRA believes a dislocation allowance should be funded for personnel retiring from active duty. After serving 20 or more arduous years of service, retiring personnel moving household locations in excess of 50 miles from their final duty station, should be entitled to a dislocation allowance equal to at least one month of basic pay.

CHILD CARE

The availability and accessibility of affordable child care is a very important quality of life issue for Coast Guard personnel and their families. Coast Guard child care centers operate under the same standards for care as similar DoD facilities. The Coast Guard's child care program includes operating nine (9) child development centers (CDC), a child care subsidy program allowing members affordable access to private sector child care centers, and whenever possible access to DoD CDCs.

High-cost child care can often be attributed to the fact that most of the unit locations preclude access to DoD and Coast Guard child development centers. The Coast Guard continues to explore ways to assist with child care costs to members in remote, high cost areas, and FRA stresses the importance of adequately funding this important program.

Education Benefits

The Association is grateful for the enactment of the Post 9/11/2001 GI Bill last year that provides a new benefit package for service members that served after 9/11/2001. Unfortunately benefits for those Reservists served before 9/11/2001 are authorized under the separate Reserve Montgomery GI Bill program and are only 25 percent of the benefits provided for active duty participants despite the intended 47 percent to 50 percent level. FRA urges attention to this inequity by providing adequate funding for the Reserve MGIB.

FAMILY READINESS

FRA strongly supports adequate funding to support Coast Guard family readiness programs. The Coast Guard Work-Life programs provide a range of support programs designed to assist members and their families with the rigors and challenges of military life. Service delivery is difficult due to the geographic location of Coast Guard families.

Resources are needed to support new initiatives to keep pace with DoD sponsored programs such as family member elder-care, sexual assault prevention and response program, personal financial management advisors, and dedicated field specialists supporting increasing demands that can not be implemented without additional funding and staff.

It is often said that the military recruits the service member, but retains the family. As our Nation asks more from its all-volunteer force, at least 50 percent of whom are married, family support has never more important.

As stated by Master Chief Petty Officer of the Coast Guard Skip Bowen in a *FRA Today* article, "Family readiness in the Coast Guard is unique to the other services. For the other branches of the military, family readiness is more geared toward a deployment. While the Coast Guard does have units that deploy in the same manner that DoD services deploy, the main difference is that the Coast Guard is deployed 100 percent of the time."

He also referenced the Coast Guard Ombudsman program which is directly related to families. Volunteers provide much needed support and our military spouses can benefit from their services if they are at their home duty station and their loved one is at sea. While some may think of the Coast Guard as a "home-based operation," many Coast

Guardsmen deploy from where they live and spend significant time away from home – anywhere from 185 to 230 days out of the year. The Ombudsmen are there to provide information for the spouses, and the spouses need to understand how the program works.

EXCHANGE/MWR PROGRAMS

The Coast Guard relies heavily on vital non-pay benefit programs to provide for the health and well-being of its personnel and their dependents, and to ensure good morale as well as mission readiness.

The Coast Guard's Morale, Welfare, and Recreation (MWR) program and the Coast Guard Exchange System (CGES) provide important services to members and their families. Proceeds from CGES sales generate funds for MWR programs including retail stores, fitness centers, gymnasiums, libraries and child development centers. All indirectly support the Coast Guard's mission while helping ease the challenges and rigors of often demanding duty assignments.

The Coast Guard operates fitness centers, bowling centers, picnic areas, movie theaters, community centers, and youth programs that without adequate funding will be degraded. New initiatives to keep pace with DoD programs such as Boy's and Girl's Clubs cannot be implemented without additional funding. In addition, second destination shipping funding is needed to provide goods and services without burdening the service member with increased costs. Continuing budget pressures threaten to degrade this important and needed benefit for Coast Guard personnel.

FRA asks that this Subcommittee, the full Committee and its Senate counterparts to provide appropriate funding support for CGES and MWR programs to ensure the well-being and morale of all Coast Guard personnel and their families.

CONCLUSION

Mr. Chairman, the FRA appreciates the opportunity to submit its views for the record on funding pay, health care and other programs important to Coast Guard personnel. The Association salutes you and members of your distinguished Subcommittee for effective funding of our Nation's all-important fifth Armed Force, and for your untiring commitment to the men and women serving so proudly in our United States Coast Guard.

NATIONAL CONGRESS OF AMERICAN INDIANS



NCAI TESTIMONY TO HOUSE APPROPRIATIONS COMMITTEE
 SUBCOMMITTEE ON HOMELAND SECURITY
 ON FY 2010 APPROPRIATIONS

APRIL 2009

EXECUTIVE COMMITTEE

PRESIDENT

Joe A. Garcia
 Ohkay Owingeh
 (Pueblo of San Juan)

FIRST VICE-PRESIDENT

Jefferson Keel
 Chickasaw Nation

RECORDING SECRETARY

W. Ron Allen
 Jamestown S'Kallam Tribe

TREASURER

gaishááho
 Lac Courne Ojibwe

REGIONAL VICE PRESIDENTS

ALASKA

Mike Williams
 Alaska Native Community

EASTERN OKLAHOMA

Joe Grayson, Jr.
 Cherokee Nation

GREAT PLAINS

Ron His Home Is Thunder
 Standing Rock Sioux Tribe

MIDWEST

Robert Chicks
 Sockbridge-Munsee

NORTHEAST

Randy Noka
 Narragansett

NORTHWEST

Brian Cladoshy
 Swinomish Tribe

PACIFIC

Joana Majel
 Paumotu

ROCKY MOUNTAIN

Scott Russell
 Crow Tribe

SOUTHEAST

Archie Lynch
 Hainai-Saponi Tribe

SOUTHERN PLAINS

Darrell Flying Man
 Cheyenne-Arapaho Tribe

SOUTHWEST

Derek Valdo
 Pueblo of Acoma

WESTERN

Avin Mayle
 Fallon Paiute Shoshone Tribe

EXECUTIVE DIRECTOR

Jacqueline Johnson Pata
 Tlingit

NCAI HEADQUARTERS

1301 Connecticut Avenue, NW
 Suite 200
 Washington, DC 20036
 202.466.7767
 202.466.7797 fax

There are over 560 tribal governments in the United States. As independent sovereign governments, tribes are not subdivisions of the states but completely separate nations. Tribal governments, have broad emergency and first responder responsibilities, as well as extensive border security responsibilities including immigration, anti-terrorism and smuggling.

In general, state governments do not have jurisdiction on Indian reservations. As such, tribes have all the same responsibilities for the public safety and security of their community as any other government, including "homeland security."

Nearly forty tribes are located directly on or near the U.S. international borders with Mexico and Canada. Hundreds of other tribal governments are the only major governmental presence in rural and isolated locations, serving as the first and often only law enforcement authority and emergency responders for their Native and non-Native communities. In addition, dozens of tribes have major national critical infrastructure on their lands, including national oil pipelines, nuclear facilities, missile sites, and dams.

NCAI REQUEST:

- (1) State Homeland Security Grant Program: 1% for Tribal Grants
- (2) Tribal Government Document Compliance: \$25 Million
 - A. Tribal ID Compliance Grants: \$20 Million
 - B. Tribal Document Guide Book: \$5 Million
- (3) Reimbursement to Indian Health Service for DHS Expenditures: \$5 million
- (4) Report Language: Clarifying States Must Include Tribes

(1) STATE HOMELAND SECURITY GRANT PROGRAM: 1% TRIBAL GRANTS

In the *Implementing the 9/11 Commission Recommendations Act of 2007 (P.L. 110-53)* Congress acknowledged the importance of tribes' relationship directly with the federal government, the Department of Homeland Security, and authorized homeland security funds to be available directly to tribes to strengthen a streamlined homeland security infrastructure.

The bill authorized Congress/DHS to expend a "minimum of 0.1%" (*of the total of the State Homeland Security Grant Program (SHSGP) + Urban Area Security Initiative (UASI) program*) for "Directly Eligible" Tribal governments. For the FY08 appropriations that minimum equaled about \$1.6 million.

There are over 560 tribes, who combined had to share this \$1.6 million. Many of those tribes are the size of states like of West Virginia and Connecticut. One tribe alone, the Tohono O'odham tribe on the Arizona border, has a \$3 million annual need. During this same time, each U.S. Territory received 0.8%, or nearly \$12 million each.

The authorization already exists for the appropriators to set the amount at their choosing (as long as it is a "minimum" of 0.1%). The tribes, therefore, respectfully request that the Homeland Security Subcommittee allocate at least 1% (*of the SHSGP + UASI*) towards tribal applicants. While 1% (approximately \$10-15 million) will still be woefully insufficient in comparison to the need, it will be a dramatic improvement.

(2) TRIBAL GOVERNMENT DOCUMENT COMPLIANCE: \$25 MILLION

Congress has taken a number of steps since 9-11 to increase the security of government issued ID cards. DHS has correctly recognized that Tribal governments are not a subdivision of state governments, but are separate sovereigns with separate citizenships, and therefore their governmental IDs must be addressed separately. Tribal governments are pleased to be a part of the homeland security effort to increase the security of their governmental ID cards. However, tribal governments have few resources available to them to help meet these new mandates.

A. TRIBAL ID COMPLIANCE GRANTS: \$20 MILLION (WESTERN HEMISPHERE TRAVEL INITIATIVE/REAL ID)

In past budget briefings, then DHS Secretary Chertoff estimated that it would cost states approximately \$8 per card to increase the security and infrastructure to meet the Congressional and DHS's guidelines. Since many tribal governments will probably need to take additional steps than states to meet these new requirements, we currently estimate it will be closer to \$10-15 per card for tribal governments. Together, tribal governments have approximately 2 million enrolled tribal citizens. A conservative estimate of the cost to increase the security of Tribal government ID cards to meet these federal requirements, therefore, ranges from \$20-30 million.

B. TRIBAL DOCUMENT GUIDE BOOK: \$5 MILLION

There are increasing document and ID requirements throughout DHS, including, but not limited to TSA for domestic flights, WHTI for international border crossing, and REAL ID for state drivers' licenses. While nearly all tribes have some form of documentation, many of these federal agencies are unfamiliar with tribal documents and, therefore, reluctant to

recognize tribal sovereignty and tribal documents. Funds should be made available to DHS for the purpose of contracting, in consultation with the Department of Interior, with an Indian tribe, consortium of Indian tribes, tribal organization, or Tribal or Native owned business for the creation of a tribal document guide.

(3) REIMBURSEMENT TO INDIAN HEALTH SERVICE FOR DHS-ICE EXPENDITURES : \$5 MILLION

The Indian Health Service (IHS) is the federal agency responsible for providing health services to Native Americans in fulfillment of the federal government's treaty and trust responsibilities. These resources are already severely stressed, and Indians receive IHS appropriations at only 50% of the actual need. Unlike other health expenditures, Indian Health Services are actually a federal governmental treaty and trust obligation.

Unfortunately the IHS hospitals near the border have been forced to spend a disproportionate percentage of their funds to care for illegal immigrants which have been funneled onto the reservations by DHS strategy of moving crossing patterns away from urban areas into more rural areas. Furthermore, while DHS has an agreement with HIS for when illegal immigrants are in their "custody," they have been playing fast-and-loose with that definition and dropping off aliens in order to avoid reimbursement issues. The IHS facility on the Tohono O'odham reservation in Arizona, for example, estimates that they spend \$2.5-3 million a year on illegal immigrant health care. ICE already has statutory authority to "reimburse other federal agencies for certain costs."

(4) REPORT LANGUAGE: CLARIFYING STATES MUST INCLUDE TRIBES

With tribes having direct eligibility for only one major DHS grant thus far (the SHSGP) tribes are still dependent upon the good graces of state governments for ensuring that they are included in planning and grant eligibility. Unfortunately, many states, like California, continue to actively deny tribal access to most DHS resources. It would be helpful to reinforce current law in the report language along the lines of the following language.

- *"In order to receive DHS funds, states with federally recognized tribes within their borders must include those tribal governments within their planning processes, ensure that those tribes have access to all grants to which they are eligible, and not impose unreasonable or unduly burdensome requirements on those tribal governments as a condition of providing grant funds or resources."*
-



**STATEMENT OF COLLEEN M. KELLEY
NATIONAL PRESIDENT
NATIONAL TREASURY EMPLOYEES UNION**

ON

**CUSTOMS AND BORDER PROTECTION ISSUES
AT THE PORTS OF ENTRY**

BEFORE

**THE HOUSE SUBCOMMITTEE ON HOMELAND SECURITY
APPROPRIATIONS OF THE U.S. HOUSE OF
REPRESENTATIVES
APPROPRIATIONS COMMITTEE**

April 17, 2009

Chairman Price, Ranking Member Rogers, distinguished members of the Subcommittee; I would like to thank the Subcommittee for the opportunity to provide this testimony. As President of the National Treasury Employees Union (NTEU), I have the honor of leading a union that represents over 22,000 Customs and Border Protection (CBP) Officers and trade enforcement specialists who are stationed at 327 land, sea and air ports of entry (POEs) across the United States. CBP employees make up our nation's first line of defense in the wars on terrorism and drugs.

In addition, CBP trade compliance personnel enforce over 400 U.S. trade and tariff laws and regulations in order to ensure a fair and competitive trade environment pursuant to existing international agreements and treaties, as well as stemming the flow of illegal contraband such as child pornography, illegal arms, weapons of mass destruction and laundered money. CBP is also a revenue collection agency, expecting to collect an estimated \$29 billion in federal revenue according to FY 2009 revenue estimates.

First, NTEU would like to thank the Committee on Appropriations for rejecting the previous Administration's FY 2009 budget request to repeal the law and rescind the FY 2008 appropriated funding to implement a new enhanced retirement benefit for all eligible GS-1895 CBP Officers. The Committee also included \$200 million in its FY 2009 funding bill to cover the conversion costs associated with this enhanced retirement benefit.

NTEU members are extremely grateful that, despite then-President Bush's request, the Committee remained firmly committed to this new enhanced retirement program. NTEU commends the Committee on its forethought and perseverance in enacting and funding this vital legislation. Nothing that the Committee has done since the creation of the Department of Homeland Security (DHS) has had a more positive effect on the morale of the CBP Officer.

FUNDING FOR DHS HUMAN RESOURCES MANAGEMENT SYSTEM

NTEU also commends the Committee for adding a provision, Section 533, in the Consolidated Security Disaster and Continuing Appropriations Act for FY 2009 that prohibits the expenditure of funds to apply a new DHS human resources management system to employees eligible for inclusion in a bargaining unit. Because of this funding prohibition, DHS announced that the agency would rescind application of this new human resources system as of October 2, 2008.

NTEU requests that identical language to Section 533 prohibiting the use of appropriated funds to implement any part of the regulations promulgated pursuant to Title 5, Chapter 97 is again included in the FY 2010 DHS funding bill.

Prior to the funding prohibition, the Committee had been extremely thoughtful and deliberative in allocating funds for implementation of the DHS personnel system. The FY 2006, 2007 and 2008 appropriations were well below the President's budget request. Also, in the last Congress, DHS authorizers acted to end this discredited program. At NTEU's request, the House Homeland Security Committee approved an amendment to the FY 2008 DHS Authorization bill to repeal the new DHS Human Resources Management System. The full

House passed the FY 2008 DHS Authorization bill, but the Senate unfortunately failed to act on this legislation. NTEU will continue to seek the repeal of Title 5, Chapter 97.

NTEU has continuing concerns regarding Title 5, Sec. 9701(h). This section states that, after passage of five years following the completion of the "transition period," DHS will have no authority to issue regulations pertaining to the new human resource management system authorized by Sec. 9701, including regulations that would modify, supersede, or terminate any regulations that were already issued. In other words, the regulations in place at the end of the 5-year period would stay in place and no new regulations could be issued. The 5-year period ended in February 2009. And even though DHS has rescinded the application of the human resource system and DHS has no authority to issue any new regulations, regulations remain in place for adverse actions, appeals, performance management, and pay and classification and can be reactivated if the funding prohibition is lifted.

FUNDING FOR CBP SALARIES AND EXPENSES AT THE PORTS OF ENTRY

Staffing Southbound Inspections at U.S.-Mexico Land Ports:

In the last year, an epidemic of violence has erupted right across the U.S. southern border in Mexico due to an increase in Mexican drug cartel activity there. Drug violence in northern Mexico has skyrocketed with more than 6,000 homicides since January 2008. This violence is fueled by arms smuggling and bulk cash drug proceeds transiting south from the U.S.

The last Administration fell down on the job of inspecting outbound traffic through U.S. land ports and not all U.S.-Mexico passenger vehicle, rail and truck port crossings are staffed or equipped to conduct southbound inspections. Rightfully, the new Administration is focused on putting more resources into southbound inspections to help curb arms and bulk cash trafficking into Mexico.

NTEU is providing information to Congress and the Administration to help formulate this new policy and to assess security equipment and other needs to address the increased threat to CBP personnel at the southern border. Safety of CBP Officers at the ports of entry is a major concern. Appropriate facilities, staffing and equipment are necessary at the southern land ports to ensure CBP Officers' safety.

NTEU supported an amendment offered by the Chairman and Ranking Member of the Senate Homeland Security and Government Affairs Committee Senators Joe Lieberman (I-CT) and Susan Collins (R-ME), to the FY 2010 budget resolution, to provide an additional \$550 million to fight drug violence along the border. This budget amendment, approved by the Senate, includes \$260 million for Customs and Border Protection to hire, equip, train and deploy 1,600 additional personnel and 400 canine teams to the border to increase the number of inspections of vehicles heading south into Mexico.

This increase in CBP staffing at the ports of entry called for in the budget resolution, however, must be in addition to the increase in staffing called for in CBP's own staffing

allocation models. **NTEU asks the Committee to increase funding for salaries and expenses at the ports of entry to address these documented staffing needs.**

CBP Officer Staffing:

NTEU was very grateful that the Committee, in its FY 2007 DHS appropriations conference report, directed CBP to submit a resource allocation model for current and future year staffing requirements. For years, NTEU has said that CBP needs several thousand additional CBP Officers and CBP Agriculture Specialists at its ports of entry; that insufficient staffing and scheduling abuses are contributing to morale problems, fatigue, and safety issues for CBP Officers and CBP Agriculture Specialists, and that CBP is losing personnel faster than it can hire replacements.

CBP's staffing model concluded "that the agency needs 1,600 to 4,000 more officers and agricultural specialists at the nation's air, land and sea ports, or a boost of 7 to 25 percent, the GAO reported." (Washington Post, November 6, 2007)

NTEU is grateful that the Committee, in its FY 2009 DHS Appropriations bill, provided funds for 1,373 U.S. Customs and Border Protection Officers and CBP Agriculture Specialists at the ports of entry — an increase of 834 beyond those requested by the Bush Administration. Also, CBP announced in January 2009 that it is hiring 11,000 new CBP employees, however, the majority of these hires are to keep up with attrition, not to address optimal staffing levels as determined by CBP's own Resource Allocation Model. According to CBP, there are currently 19,726 CBP Officers of which nearly 3,400 are non-frontline supervisors—a **ratio of one supervisor for every 5 CBP Officers.**

NTEU is disappointed that the new Administration's FY 2010 budget outline includes increasing new hires for CBP Border Patrol Agents from 17,499 to 20,000—an increase of 1,500, but no explicit increase in frontline CBP Officer or CBP Agriculture Specialist new hires.

NTEU agrees with the observation of Senate Homeland Security and Governmental Affairs Committee Chairman Lieberman in his March 13, 2009 letter to the Senate Budget Committee. Chairman Lieberman states that "[t]he Border Patrol has almost doubled in the last three fiscal years, while the number of CBP officers at ports of entry has remained basically stable despite long wait times at the border. If this trend continues, it could lead to a misalignment of resources and the under-funding of critical border security priorities, in particular this nation's efforts to enhance the security of our ports of entry through the deployment of programs such as the Western Hemisphere Travel Initiative (WHTI), the Electronic System for Travel Authorization (ESTA), and US-VISIT."

Again NTEU calls on the Committee to fund staffing levels for CBP Officers and CBP Agriculture Specialists at the ports of entry as specified in CBP's own workforce staffing model, in addition to funding an increase in CBP Officer staffing needed to expand outbound inspection and address the increasing violence at the U.S.-Mexico border.

One Face at the Border and Training:

In 2006, Congress requested that the Government Accountability Office (GAO) evaluate the One Face at the Border initiative and its impact on legacy customs, immigration and agricultural inspection and workload. GAO conducted its audit from August 2006 through September 2007 and issued its public report, *Border Security: Despite Progress, Weaknesses in Traveler Inspections Exist at Our Nation's Ports of Entry* (GAO-08-219), on November 5, 2007. The conclusions of this report echo what NTEU has been saying for years:

- CBP needs several thousand additional CBP Officers and Agriculture Specialists at its ports of entry.
- Not having sufficient staff contributes to morale problems, fatigue, and safety issues for CBP Officers.
- Staffing challenges force ports to choose between port operations and providing training. In these instances...training is often sacrificed.
- CBP's onboard staffing level is below budgeted levels, partly due to high attrition, with ports of entry losing officers faster than they can hire replacements.

The Homeland Security Appropriations Committee added report language to the FY 2007 DHS Appropriations bill that, with regard to CBP's One Face at the Border initiative, directs "CBP to ensure that all personnel assigned to primary and secondary inspection duties at ports of entry have received adequate training in all relevant inspection functions." NTEU asks the Committee to again seek this information in report language to its FY 2010 DHS Appropriations bill.

NTEU's CBP members have told us that CBP Officer cross-training and on-the-job training continues to be woefully inadequate. In addition, staffing shortages force managers to choose between performing port operations and providing training. In these instances, it is training that is sacrificed.

It is apparent that CBP sees its One Face at the Border initiative as a means to "increase management flexibility" without increasing staffing levels. **NTEU again calls for Congress to end the failed One Face at the Border experiment and ensure that expertise is retained with respect to customs, immigration, and agriculture inspection functions at CBP.**

Agriculture Specialists Staffing:

NTEU was certified as the labor union representative of CBP Agriculture Specialists in May 2007 as the result of an election to represent all CBP employees that had been consolidated into one bargaining unit by merging the port of entry inspection functions of Customs, INS and the Animal, Plant and Health Inspection Service as part of DHS' One Face at the Border initiative.

According to GAO (GAO-08-219, page 31), CBP's staffing model "showed that CBP would need up to several thousand additional CBP Officers and agriculture specialists at its ports

of entry." And GAO testimony issued on October 3, 2007 stated that, "as of mid-August 2007, CBP had 2,116 agriculture specialists on staff, compared with 3,154 specialists needed, according to staffing model." (See GAO-08-96T page 1.) According to CBP, the current number of CBP Agriculture Specialists staff is 2,277, of which 312 are non-frontline supervisors. This is unacceptable. CBP needs to dramatically increase frontline Agriculture Specialist staffing levels.

NTEU also recommends that Congress, through oversight and statutory language, make clear that the agricultural inspection mission is a priority. NTEU would support asking DHS to report on how it is following U.S. Department of Agriculture procedures on agriculture inspections. The report should include wait times for clearing agricultural products and what measures could be implemented to shorten those wait times.

Trade Operations Staffing:

When CBP was created, it was given a dual mission of not only safeguarding our nation's borders and ports from terrorist attacks, but also the mission of regulating and facilitating international trade; collecting import duties; and enforcing U.S. trade laws. In 2005, CBP processed 29 million trade entries and collected \$31.4 billion in revenue. In 2009, the estimated revenue collected is projected to be \$29 billion—a drop of over \$2 billion in revenue collected.

Section 412(b) of the Homeland Security Act of 2002 (P.L. 107-296) mandates that "the Secretary [of Homeland Security] may not consolidate, discontinue, or diminish those functions...performed by the United States Customs Service...on or after the effective date of this Act, reduce the staffing level, or reduce the resources attributable to such functions, and the Secretary shall ensure that an appropriate management structure is implemented to carry out such functions."

Congress subsequently found that CBP was not in compliance with the Section 412(b) mandate. Therefore, Congress included Section 402 in the SAFE Port Act of 2006. This provision required CBP to prepare a Resource Allocation Model (RAM) every two years to determine optimal staffing levels needed to carry out the commercial operations of CBP, including commercial inspection and release of cargo. The first RAM was delivered to Congress in June of 2007 and states that currently, CBP has over 8,200 employees that are involved in commercial trade operations, but suggests that to carry out these commercial operations and to adequately staff the needs for priority trade functions, the optimal staff level in FY 2008 would be over 10,000. These numbers include CBP Officers and CBP Agriculture Specialists involved in the commercial inspection and release of cargo.

The Model proposes increases from the current floor of 2,263 customs revenue function employees, which includes Fine, Penalty and Forfeiture Specialists, Import Specialists, International Trade Specialists, Customs Attorneys, Customs Auditors, Chemists and CBP Technician positions, but notes that the Model is not tied to any specific budget request and does not reflect the Department's, CBP's, or the President's funding priorities. **The next RAM, as mandated by the SAFE Port Act, is due on June 30, 2009 and NTEU expects to see similar numbers in terms of CBP trade operations staffing needs.**

Customs revenues are the second largest source of federal revenues that are collected by the U.S. Government. The Committee depends on this revenue source to fund federal priority programs. The Committee should be concerned as to how much CBP trade enforcement staffing shortages cost in terms of revenue loss to the U.S. Treasury. According to a GAO report on Customs Revenue Functions (GAO-07-529), CBP collected nearly \$30 billion customs duties in FY 2006, but did not collect approximately \$150 million in antidumping duties alone in 2006. CBP has been unable to collect more than \$500 million in antidumping duties over the past 5 years. (See GAO-07-529, page 23 and pages 29-30.) GAO also concluded that CBP's shift in mission contributed to reduced focus and resources devoted to customs revenue functions.

NTEU urges the Committee to ensure that trade compliance personnel is increased to the staffing levels that CBP itself states in the 2007 RAM are sufficient to ensure effective performance of customs revenue functions.

Conclusion:

Each year, with trade and travel increasing at astounding rates, CBP personnel have been asked to do more work with fewer personnel, training and resources. The more than 22,000 CBP employees represented by the NTEU are capable and committed to the varied missions of DHS from border control to the facilitation of legitimate trade and travel. They are proud of their part in keeping our country free from terrorism, our neighborhoods safe from drugs and our economy safe from illegal trade. These men and women are deserving of more resources and technology to perform their jobs better and more efficiently.

Thank you for the opportunity to submit this testimony to the Committee on their behalf.

NANCY DRAGANI
PRESIDENT, NATIONAL EMERGENCY MANAGEMENT ASSOCIATION
AND EXECUTIVE DIRECTOR, OHIO STATE EMERGENCY MANAGEMENT AGENCY

STATEMENT FOR THE RECORD

APPROPRIATIONS FOR THE DEPARTMENT OF HOMELAND SECURITY FOR FISCAL YEAR
2010

THE UNITED STATES HOUSE OF REPRESENTATIVES
APPROPRIATIONS SUBCOMMITTEE ON HOMELAND SECURITY
MAY 1, 2009

INTRODUCTION

Thank you Chairman Price, Ranking Member Rogers, and distinguished members of the Committee for allowing me the opportunity to provide you with a statement for the record on the Department of Homeland Security's (DHS) fiscal year 2010 budget. I am Nancy Dragani, President of the National Emergency Management and Executive Director of the Ohio State Emergency Management Agency. In my statement, I am representing the National Emergency Management Association (NEMA), whose members are the state emergency management directors in the states, the U.S. territories, and the District of Columbia. NEMA's members are responsible to their Governors for emergency preparedness, homeland security, mitigation, response, and recovery activities for natural, man-made, and terrorist caused disasters.

In 2008, FEMA declared 75 major disasters; 17 emergency declarations; and 51 fire management assistance declarations. Overall, 40 states and two territories were impacted. The multi-hazards emergency management system continues to be the means to practice and exercise for devastating acts of terrorism, while at the same time preparing the nation for hurricanes, tornadoes, earthquakes, hazardous materials spills, and floods. We respectfully ask for your Committee to consider the role of emergency management as you address the FY 2010 appropriations and ask for your serious consideration of additional federal support for the only all-hazards program to build state and local emergency management capacity. Emergency Management Performance Grant (EMPG) is the only state and local matching grant program supporting preparedness efforts.

The Department of Homeland Security budget provides critical support to state and local emergency management programs. NEMA would like to address four critical issues regarding the proposed federal budget for the Department of Homeland Security:

1. **Addressing the needs for the Emergency Management Performance Grant (EMPG) level and maintaining flexibility in state's use of the program;**
2. **Federal support for the Emergency Management Assistance Compact (EMAC);**
3. **Significant deficits for improving state and local Emergency Operations Centers (EOCs);**
and
4. **Additional investment is needed for the nation's mitigation programs including the Predisaster Mitigation Grant Program.**

EMERGENCY MANAGEMENT INFRASTRUCTURE FUNDING

EMPG is the only program for All-Hazards Preparedness

Natural disasters are certain and often anticipated. Every state must be able to plan for disasters as well as build and sustain the capability to respond. EMPG is the only source of funding to assist state

and local governments with planning and preparedness/readiness activities associated with natural disasters. At a time when our country is continuing to recover from one of the largest natural disasters in history and making strides to improve the nation's emergency preparedness/readiness, we cannot afford to have this vital program be cut or just maintained. EMPG is the backbone of the nation's all-hazards emergency management system and the only source of direct federal funding to state and local governments for emergency management capacity building. EMPG is used for personnel, planning, training, and exercises at both the state and local levels. EMPG is primarily used to support state and local emergency management personnel who are responsible for writing plans; conducting training, exercises and corrective action; educating the public on disaster readiness; and maintaining the nation's emergency response system. EMPG is being used to help states create and update plans for receiving and distribution of emergency supplies such as water, ice, and food after a disaster; debris removal plans; and plans for receiving or evacuating people – all of these critical issues identified in the aftermath of Hurricane Katrina and the following investigations and reports. EMPG is the program being used to support state and local efforts for federal preparedness initiatives like the Target Capabilities List, Cost to Capability, Comprehensive Planning Guide 101, and Gap Analysis.

The state and local government partnership with the federal government to ensure preparedness dates back to the civil defense era of the 1950s, yet increased responsibilities over the last decade have fallen on state and local governments. NEMA's 2008 Biennial Report shows that the shortfall in EMPG funding has reached \$172 million. The total need for the program is \$487 million annually. The 9/11 Implementation Act authorized EMPG at \$680 million for FY 2010.

We appreciate all of the efforts of members of Congress and the Administration to allow for increases to the EMPG program; however, adjusted over the last fifteen years, the increases have not kept pace with inflation at a time when capacity is supposed to be increasing. Continued funding increases are necessary to make up for over a decade of degradation of funding and increased state and local commitments.

EMPG is the only all-hazards preparedness program within the Department of Homeland Security that requires a match at the state and local level. The 50/50 match is evidence of the commitment by state and local governments to make public safety and security a top priority. According to the Council of State Governments, 49 of 50 states are currently in a recession, and 41 states are looking at shortfalls in 2009 or 2010. States are faced with an estimated \$140 billion overall shortfall. The fiscal conditions warrant maintaining the intent of EMPG as all-hazards and as a flexible program. States should not be forced to set aside arbitrary amounts of EMPG for specific tasks – each state's hazards and risks are unique as is the approach to addressing these hazards. One size does not fit all in terms of the overall emergency management needs. Additionally, many of the EMPG funds help pay for the personnel to run key programs and reducing flexibility means that critical functions could be lost.

Attached is a recent document that outlines how states are using EMPG funds. Some of the key examples include:

- ARIZONA

The Emergency Management Performance Grant (EMPG) has enabled the state of Arizona to achieve a level of collaboration between the state, counties, cities, tribes, volunteer and faith-based organizations and the private sector that never existed before. EMPG recently funded the largest full-scale exercise ever conducted in Arizona, the "Coyote Crisis Campaign," a mass-casualty incident that over-burdened the surge capacity of area hospitals and challenged the ability of officials to manage a

multi-jurisdiction response. Arizona's first responders, health care providers and other emergency management partners responded to the terrorist scenario.

EMPG funds have provided the means to develop the capability to respond to bi-national incidents along the Arizona-Sonora border. The grant has been used to pay for state and local bi-national emergency preparedness activities (planning, training, and exercising) and the implementation of bi-national emergency alert and notification systems, interoperable communications, and IT systems that support the sharing of information and maintaining a common operating picture for emergency incidents.

- CALIFORNIA

The establishment of the Office for Access and Functional Needs (OAFN), in January 2008 is the result of EMPG funding. As part of the California Emergency Management Agency (CalEMA), the office identifies the needs of people with disabilities before, during and after a disaster; and integrates disability elements and resources into all aspects of emergency management systems. OAFN is currently funded by EMPG and provides two employees. In July 2008, OAFN published *Guidance on Planning and Responding to the Needs of People with Disabilities and Older Adults*, and released it specifically to California emergency managers, planners, and disability and older adult service systems, for planning and responding during disasters and recovery.

- CONNECTICUT

During the past three years, the Connecticut Department of Emergency Management and Homeland Security (DEMHS) has used EMPG to improve participation in the state's High Band Radio System. This is a communications network of last resort during a major disaster. Because of EMPG, 96 percent of Connecticut communities are connected to the system, as compared to only 24 percent in 2006. In a serious event, it would help impacted areas convey their most urgent life-sustaining needs, such as food, water and temporary shelters. The High Band System also links regional emergency management offices to local towns and to the State EOC.

- HAWAII

Emergency shelters can mean the difference between life and death in a vulnerable state like Hawaii, which is confronted by the possibility of many different types of hazards— earthquakes, hurricanes, tsunamis and volcano eruptions. In 2009, the state is dedicating part of its EMPG funds to conduct assessments and surveys of public and private facilities that could serve as emergency shelters; and support state and county participation in the development of a catastrophic hurricane disaster plan. EMPG money is also contributing to state readiness exercises involving terrorism, earthquake, tsunami, and hurricane emergency response scenarios.

- KENTUCKY

In 2008, the Commonwealth of Kentucky used EMPG dollars to develop and exercise a plan in the event of a New Madrid earthquake occurring in the western portion of the state. When the state was hit with a massive ice storm earlier this year, resulting in its worst disaster ever, state emergency management used the earthquake plan to support western counties decimated by the storm. Though designed for an earthquake, the plan was adapted for this disaster and was key in delivering aid to 103 counties with hundreds of thousands of citizens who had no power, no heat and no food. Also, because the plan had been thoroughly exercised - again due to EMPG funds - the state had already made adjustments and knew that it would work. Advance planning and exercise supported through EMPG saved lives in Kentucky.

- MISSISSIPPI

Thanks to the current EMPG funding level, all 82 counties in Mississippi, as well as the Mississippi Band of Choctaw Indians, have emergency management programs and emergency management directors. This was not always the case. Back in 2000, when EMPG funding was significantly lower, there were only 43 county emergency management programs. At the state level, nine area coordinators – all funded by EMPG – cover between six and 11 counties. Each coordinator works closely with their respective local emergency managers, responding to their requests for support and resources, and conducting training for the staff and educational presentations for residents. The importance of this integration came into play in September 2008 when Hurricane Gustav hit. The Mississippi Emergency Management Agency (MEMA) helped coordinate the unprecedented evacuation of more than three million people from South Louisiana and the city of New Orleans. The large number of evacuees was able to move easily through Mississippi and find shelter thanks to the coordination of all the county emergency managers and MEMA.

- OHIO

In 2008, the State of Ohio allocated approximately 74% of its EMPG funds directly to local governments to focus on sustaining and enhancing emergency management capability. Ohio recognizes the critical importance of building and sustaining local capabilities throughout the planning, response, recovery and mitigation phases of a disaster. As such, EMPG grant funds support 170 full time emergency management personnel in 88 counties who update and enhance county Emergency Operations Plans and applicable annexes that serve as the foundation of local capabilities. The State supports the counties in all aspects of emergency management, including grants management, planning activity identification, training and exercise and special projects. These efforts, coupled with the detailed guidance established for EMPG funds, further enhance the local capabilities and allow for increased identification of risks and hazards that threaten the 11 plus million residents of Ohio's 88 counties.

One such threat occurred in September 2008 when Ohio was faced with hurricane force wind gusts from the remnants of Hurricane Ike. As the winds moved through a large portion of the state, more than five million Ohioans were impacted and many lost power for more than a week. The ability of county emergency management agencies to coordinate response and resource support for the needs of the residents was a credit to their planning and preparedness efforts, supported by Ohio's allocations of EMPG funding.

- WISCONSIN

EMPG is a major reason for the successful response by both the state and local jurisdictions to the severe storms and flooding that occurred in Wisconsin in June 2008. Wisconsin requires the state, counties and municipalities to develop consistent, emergency management programs. To accomplish this, Wisconsin Emergency Management provides two-thirds of its EMPG grant to county emergency managers. They in turn assist municipalities in developing their annual plans of work. These documents include areas of planning, training, exercising, public education/information, grant administration, and other initiatives that focus on specific local needs.

BUILDING OUR NATION'S MUTUAL AID SYSTEM THROUGH EMAC

The Emergency Management Assistance Compact (EMAC) remains a the vehicle to utilize mutual aid assistance during disasters. Congress enacted EMAC in 1996 (P.L. 104-321). Currently 50 states, the U.S. Virgin Islands, Puerto Rico, Guam, and the District of Columbia are members of EMAC. EMAC requires member states to have an implementation plan and to follow procedures outlined in the EMAC Operations Manual. EMAC addresses issues such as reimbursement, liability protections, and workers' compensation issues.

In the last year, EMAC has provided critical aid to impacted states. In support of the 2009 Flooding in North Dakota and Minnesota, states deployed equipment, sandbags, and 1029 personnel to North Dakota and 6 personnel to Minnesota. Two individuals were deployed to the National Response Coordination Center (NRCC) at FEMA Headquarters to coordinate the state response under EMAC with the federal response. In all, 727 National Guard personnel and 302 civilians were sent to assist via the compact.

In February 2009, generators, cots with blankets, and 702 personnel were deployed to Kentucky to assist in the response and recovery following an ice storm that impacted the majority of the state. 528 personnel with civilian and 174 personnel were National Guard assets.

In response to the 2008 Hurricanes Gustav and Ike states deployed 12,274 personnel under EMAC to support the impacted states of Texas, Louisiana, and Florida. The response lasted 63 continuous days with a total of 265 completed missions.

In October 2006, Congress, under The Post-Katrina FEMA Reform Act authorized FEMA to appropriate up to \$4 million annually in grants in fiscal year 2008 to support EMAC operations and coordination activities, but no funds have been appropriated.

Prior to 2004, deployments under EMAC were primarily state emergency management and National Guard personnel. The value of EMAC was reaffirmed following Hurricanes Katrina and Rita by demonstrating that EMAC can be used to deploy "any resources one state would want to share with another". Combined with the requirements in the Post-Katrina Emergency Management Reform Act of 2006, EMAC has resulted in an unprecedented growth and involvement in EMAC across the nation. EMAC has also demonstrated the need for a unified mutual aid system (intrastate to interstate) that coordinates with the federal response.

EMAC has a five year strategic plan to put lessons learned into practice. The After-Action process from Hurricane Katrina allowed EMAC to examine how to improve the system after unprecedented disasters and an unparalleled growth in the use of the system.

Examples of improvements to be made with current and future funding as a result of lessons learned are outlined below:

- NEMA has been working with first responder disciplines to provide EMAC educational and training materials. This includes training on EMAC, integration with State Emergency Operations Centers, Incident Command Systems, resource typing, and credentialing;
- NEMA has established an EMAC Advisory Group that is working to better integrate mutual aid partners into the EMAC system before future disasters occur. The group includes

representatives from state and local government associations, the National Guard Bureau, emergency responder associations, public utility associations, the private sector, DHS/FEMA, and the Centers for Disease Controls. The discussions and interactions of this group serve to assist in adding local government assets to the scope of resources and other disciplines that can be readily plugged into the system;

- EMAC is evolving the tracking of resources through NEMA administrative management. EMAC is working towards an integrated system to allow for swifter approvals from the requesting and responding states, which will ultimately allow for improved tracking and faster response to requests for assistance;
- States are engaged in developing their own resource typed mission ready packages and EMAC is involved in assisting with responsibilities set in both the Post-Katrina Emergency Management Reform Act and the Implementing the 9/11 Commission Recommendations Act for resource typing and credentialing; and
- Building capabilities for A-Team operations to assist during disasters outside of State Emergency Operations Centers with resource management, integration of EMAC into exercises with the development of table-top exercises and inclusion in national level exercises such as TOPOFF, as well as address reimbursement ahead of mission deployments for both state and local resource providers.

While Emergency Management Performance Grants and homeland security grants are helping to build capabilities, the National Homeland Security Strategy counts on the fact that mutual aid is going to be put to use in a disaster. The support of EMAC is critical to helping offset the costs of disasters and building costly infrastructure at the federal level that could sit unused until a disaster. In order to meet the ever-growing need for and reliance on interstate mutual aid, NEMA is seeking reauthorization at \$4 million annually for 2010 and beyond and an annual \$4 million line item in the FEMA budget for building EMAC capabilities and our nation's mutual aid system.

IMPROVING STATE AND LOCAL EMERGENCY OPERATION CENTERS

During emergencies and disasters, emergency operations centers (EOCs) serve as the nerve center for state and local coordination. Federal agencies as well use these facilities to act as a central point for communication during response and recovery phases. States continue to require more monies to enhance state primary and alternate EOCs. According to data in the 2008 NEMA Biennial Report, it is estimated that almost \$497 million would be needed to build, retrofit and upgrade the facilities. The amount is a 26 percent increase over the 2006 estimate. For local EOCs, that number increases to \$1.1 billion, for a total of almost \$1.6 billion. This includes the costs to upgrade equipment and software, train personnel, and conduct operations during emergency and non-emergency situations. We appreciate Congress' recognition of the need for EOC improvements in the FY 2008 and FY 2009 appropriations as these investments are a down payment towards addressing this critical shortfall.

A separate line item for EOC improvements should be continued in the budget. Maintaining the flexibility of EMPG and having the separate program continue are priorities for emergency management.

INVESTMENT IN PREDISASTER MITIGATION

As the nation continues to recover from the 2004 and 2005 hurricane season and the numerous other disasters, mitigation opportunities are the only way to take advantage of lessons learned during disasters. The Disaster Mitigation Act of 2000 (DMA2K and P.L. 106-390) authorized a national

disaster hazard mitigation program “to reduce the loss of life and property, human suffering, economic disruption, and disaster assistance costs resulting from natural disasters and to provide a source of predisaster hazard mitigation funding that will assist States and local governments in implementing effective hazard mitigation measures that are designed to ensure the continued functionality of critical services and facilities after a natural disaster.” The title of the bill that authorizes the Predisaster Mitigation program is scheduled to sunset on September 30, 2009, after a one-year extension of the program.

Predisaster Mitigation grants accounts contained significant earmarks in FY 2008 and FY 2009, thus reducing the amount available for state and local governments to openly apply to be considered for the grants. The program funding is solely under the total national need, especially with the original intent of the law to provide each state with a portion of funding so lessons learned from disasters could be taken advantage of by all states. Each year, FEMA typically receives requests for grants averaging over \$450 million annually. When the program was proposed for the first time in FY 2003, the President proposed \$300 million annually. The FY 2003 figure was derived by taking a decade of mitigation opportunities annual averages, but took out the large disaster spikes like Hurricane Andrew and the North Ridge and Loma Prieta earthquakes.

While federal costs towards disasters remain a concern, significant commitments must be made towards both predisaster and post-disaster mitigation in order to lower overall disaster costs in the long run. With such low levels of funding, the predisaster mitigation program has never been fully able to address the intent of DMA2K. In 2005, the Multi-Hazard Mitigation Council published a study that found that every \$1 FEMA invested into mitigation projects saves society approximately \$4. The key to the value of the programs is that predisaster mitigation is coordinated through the Governors and the state hazard mitigation plan as required by DMA2K. The program addresses the unique areas of greatest need to prepare for and reduce the overall costs of a disaster event.

While NEMA is supportive of the Predisaster Mitigation Program, we remain supportive of both pre- and post-disaster mitigation. The Hazard Mitigation Grant Program (HMGP) must not be changed in order to ensure a balanced holistic national mitigation program that includes both pre- and post-disaster mitigation. As the Congress considers the Predisaster Mitigation program’s reauthorization, adequate funding levels are needed to give the program the opportunity to demonstrate real value for the investments. NEMA supports the program’s reauthorization and looks forward to working with Congress to improve the program.

CONCLUSION

Congress has affirmed their support for ensuring preparedness for our nation’s continuous vulnerability against all-hazards with additional investments to EMPG and emergency operations centers improvements. We must continue to build national preparedness efforts with a multi-hazard approach. In this year’s appropriations process Congress will make critical decisions that shape the future of emergency management in this country. As you begin your consideration, we ask you to recognize the importance of adequately funding the EMPG program and maintain the program’s flexibility for building capacity through people at the state and local level for all disasters. I thank you for the opportunity to testify on behalf of NEMA and appreciate your partnership.



**EMERGENCY MANAGEMENT PERFORMANCE GRANT
(EMPG) –
A Proven Investment in Protecting This Country
From All-Hazards**

April 2009

Since the early 1990s, the Emergency Management Performance Grant (EMPG) has served this country as one of the most successful and cost-effective grants ever created. As the only source of federal funding directed to state and local governments for planning, training, exercises and personnel for all hazards, EMPG enables local jurisdictions to develop and support their emergency management capabilities. This includes planning, training, exercises, public education and information, and many other day-to-day activities designed to prevent disaster loss.

A pass-through program for states to distribute funds to local governments, EMPG provides states with the flexibility to make funding decisions based on identified needs and priorities. States are not required to pass through a set amount, but most allocate at least half of their funding to local jurisdictions. This means that states and local/county/tribal jurisdictions collaborate in a coordinated approach to develop the best emergency management strategy for their citizens and the hazards they face.

The following are examples of how EMPG is impacting citizens across this country. From protecting those with special needs to developing life-saving communications systems, the success stories show how the small investment in EMPG ripples through this nation, teaching Americans how to better prepare for all threats, and helping them recover once a disaster strikes.

ARIZONA

The Emergency Management Performance Grant (EMPG) has enabled the state of Arizona to achieve a level of collaboration between the state, counties, cities, tribes, volunteer and faith-based organizations and the private sector that never existed before. EMPG recently funded the largest full-scale exercise ever conducted in Arizona, the "Coyote Crisis Campaign," a mass-casualty incident that over-burdened the surge capacity of area hospitals and challenged the ability of officials to manage a multi-jurisdiction response. Arizona's first responders, health care providers and other emergency management partners responded to the terrorist scenario. The partnerships developed during the preparation and conduct of the exercise will endure for a long time. The lessons learned have better prepared Arizona for an actual event.

EMPG funds have provided the means to develop the capability to respond to bi-national incidents along the Arizona-Sonora border. The grant has been used to pay for state and local bi-national emergency preparedness activities (planning, training, and exercising) and the implementation of bi-national emergency alert and notification systems, interoperable communications, and IT systems that support the sharing of information and maintaining a common operating picture for emergency incidents.

ARKANSAS

Preparedness and public outreach in Arkansas reached a new level in Fall 2008 when the Arkansas Department of Emergency Management (ADEM) took its Mobile Command Post to the University of Arkansas-Louisiana-Monroe college football game at War Memorial Stadium in Little Rock. It marked the first time in the history of the NCAA for such an undertaking. Thanks to EMPG funds, ADEM reached thousands of Arkansans and distributed pamphlets and brochures on the importance of being prepared, with a specific emphasis on having a family emergency supply kit. With five federally-declared disasters occurring in the state in 2008, football fans were very receptive to the preparedness materials.

Finally, EMPG helps maintain ADEM's role as a 24-communication point for the entire state. This allows all local jurisdictions to contact the agency at any time, report incidents, and gather additional data, research and support, without any additional cost to the local entity.

CALIFORNIA

The establishment of the Office for Access and Functional Needs (OAFN), in January 2008 is the result of EMPG funding. As part of the California Emergency Management Agency (CalEMA), the office identifies the needs of people with disabilities before, during and after a disaster; and integrates disability elements and resources into all aspects of emergency management systems. OAFN is currently funded by EMPG and provides two employees. It's anticipated this will expand to four employees on July 1, 2009. In July 2008, OAFN published *Guidance on Planning and Responding to the Needs of People with Disabilities and Older Adults*, and released it specifically to California emergency managers, planners, and disability and older adult service systems, for planning and responding during disasters and recovery. The guidance was mailed to emergency managers statewide and is available on the CalEMA agency website.

In addition, thanks to EMPG dollars, CalEMA's Law Enforcement Branch initiated a training program to introduce and prepare first responders and emergency management support personnel for the grim reality and task of fatality management in the event of a catastrophic disaster involving significant loss of lives. The devastating effects of Hurricane Katrina and the Indian Ocean tsunami was a wake-up call for emergency managers across the nation to address mass fatality planning and response, and to institute sound preparedness measures and programs. EMPG funding has been utilized to develop an eight-hour course, "Introduction to Coroners' Mutual Aid and Mass Fatality Planning." Specifically, the course is designed for law enforcement, fire service, hospital emergency planners, public health, emergency management, and private sector death care industry professionals. It introduces the State's Coroners' Mutual Aid System; provides an overview of the role and responsibilities of the Coroner; describes the fatality management process; discusses critical issues surrounding mass fatality incidents; and has relevant and current case studies to complement lecture material. The first course was offered in February 2009 and a second course is scheduled for June 2009. EMPG dollars have been instrumental in helping to establish and present this critical and unique training throughout the state.

COLORADO

In FY 2008, Colorado distributed approximately \$3 million directly to 58 counties, 10 municipalities and two tribes. These funds helped local governments to sustain their all-hazards emergency management programs, including staff, emergency operations centers, disaster plans, public education campaigns, and training and exercise activities. Additionally, DEM used these funds to support a number of critically unfunded preparedness initiatives across the state which included projects such as a communications systems in the Northwest Region to support public warning due to the increased wildfire threat from forest beetle infestation; planning to support Volunteer and Donations Management, Mass Care, Special Needs Populations and Animal Response Teams; and equipment purchases to improve and upgrade local emergency operations centers with computer hardware/software, radios, telecommunications equipment, displays and back-up generators.

CONNECTICUT

During the past three years, the Connecticut Department of Emergency Management and Homeland Security (DEMHS) has used EMPG to improve participation in the state's High Band Radio System. This is a communications network of last resort during a major disaster. Because of EMPG, 96 percent of Connecticut communities are connected to the system, as compared to only 24 percent in 2006. In a

serious event, it would help impacted areas convey their most urgent life-sustaining needs, such as food, water and temporary shelters. The High Band System also links regional emergency management offices to local towns and to the State EOC.

DEMHS has also used the grant to increase local participation in the EMPG program. In 2006, 85 towns – each with a functioning EOC and Emergency Management Director (EMD) – participated in the program. That number has now jumped to 140 participating towns. This represents 94 percent of Connecticut’s population of 3.6 million persons. DEMHS also increased the per capita share of funding to local towns from \$0.31 cents in 2006 to \$0.46 cents in 2009 and created several incentives such as stipends for computers and additional EOC Equipment to encourage other towns to join the program and to further professionalize the existing corps of EMDs in Connecticut.

DISTRICT OF COLUMBIA

EMPG is a cornerstone program in the nation’s capital, supporting a myriad of projects and initiatives that serve many population groups. These include unique regional planning efforts within the National Capital Region for National Security Special Events such as the G-20 Economic Summit, Presidential Inauguration and other high profile events such as the International Monetary Fund annual meeting.

Most recently, the District of Columbia Homeland Security and Emergency Management Agency (HSEMA) also used grant funding to distribute 1,000 free emergency preparedness kits to residents with special needs. It is also partnering with a local hospital to give the kits to homebound elderly.

In the area of emergency public information and warning, EMPG helps support Roam Secure Alert Network, which allows the city to send alerts through wireless text devices and emails in the event of a disaster. A traffic messaging system allows quick and accurate communication to the traveling public about driving pattern changes as a result of a major emergency. Reverse 911 uses the telephone system to alert residents and deliver notifications. The tool can make thousands of call each hour and can target precise geographic locations.

Finally, comprehensive and coordinated planning is an important component of disaster management. With EMPG money, HSEMA is updating the broad set of plans and protocols for each Emergency Support Function, detailing how lead and support agencies will perform their mission as identified within DC’s response plan. The district also has developed plans and protocols for the non-profit sector to address service coordination, financial and donation management, volunteer management and in-kind goods and services.

FLORIDA

EMPG funds support state and local governments in their efforts to sustain all-hazards emergency management capabilities throughout Florida. The grant provides full or partial funding at the state and local level for a variety of programs and projects including 45 state positions that are focused on the leadership for, response to, preparedness for, recovery from and mitigation of man-made and natural disasters; local programs for all 67 county programs with the state of Florida; a weeklong statewide hurricane exercise; a weeklong 2010 COOP exercise for 200 state and local partners during which the State EOC will be moved to the Florida National Guard training facility at Camp Blanding; funding for support for, maintenance of and renovation of space used for the SERT during activations in the State EOC; daily and redundant communication throughout the state and all counties; state incident management teams, logistical staging area caches and Joint Field Office (JFO) caches of equipment for state staff; bi-annual updating of the state Comprehensive Emergency Management Plan (CEMP) and its associated annexes; needed accessible supplies/equipment for people with disabilities in emergency

shelters; outreach emergency preparedness for people with disabilities, and training for emergency management personnel, shelter workers and advocates regarding people with disabilities during a disaster.

Additionally, EMPG funds indirectly impact and assist Florida's recovery efforts. Grant dollars are dedicated to operations and activities regarding catastrophic planning, all-hazards public education and exercises, implementation of the National Incident Management System, implementation of Americans with Disabilities Act into all phases of emergency management, and state and local emergency manager professional development. Each enhanced planning and preparation effort as well as pro-active training to share lessons learned and best practices better helps Florida with its capability to recover from any natural or man-made event.

GEORGIA

With more EMPG funding, Georgia has begun increasing its pass-through amounts to local EMAs by offering performance-based, measurable initiatives. One such project provides funding to local communities for severe weather warning systems. These systems are designed to help keep the citizens of Georgia out of harm's way and to aid in the timely provision of emergency services to those impacted by natural disasters or acts of terrorism. Applicants can apply for a variety of severe weather warning tools, such as outdoor sirens, reverse 911 calling equipment, NOAA weather warning radios or combination of systems. The choice is up to the local jurisdiction.

Another project made possible by EMPG is a contract between the Georgia Emergency Management Agency and the Georgia Association of Fire Chiefs (GAFC) for administrative oversight, management and operational expertise in the delivery of fire services coordination and planning efforts on behalf of or in conjunction with GEMA. The fire service is an important partner in many disasters and is frequently called upon in larger events that require mutual aid assistance from other jurisdictions. Sometimes, however, the various needs associated with mutual aid requests can place administrative burdens on the responding fire department(s). With this agreement, EMPG lends critical financial support so that the GAFC can provide on-duty or on-call coordination 24/7 of mutual aid requests for fire and fire rescue resources upon request of GEMA on behalf of a stricken unit.

HAWAII

Emergency shelters can mean the difference between life and death in a vulnerable state like Hawaii, which is confronted by the possibility of many different types of hazards— earthquakes, hurricanes, tsunamis and volcano eruptions. In 2009, the state is dedicating part of its EMPG funds to conduct assessments and surveys of public and private facilities that could serve as emergency shelters; and support state and county participation in the development of a catastrophic hurricane disaster plan. EMPG money is also contributing to state readiness exercises involving terrorism, earthquake, tsunami, and hurricane emergency response scenarios. In addition, the state is making resource management and logistics a priority with some of its grant funding. A disaster supply cache has been established in a former National Guard warehouse and building on this capability by adding equipment to support special health needs emergency shelters. Available items include meals-ready-to-eat, tarps, generators, blankets, beds and oxygen bottles.

IDAHO

EMPG impacts much of the Idaho Bureau of Homeland Security's scope of work. This includes updating and/or creating evacuation plans for several Idaho towns, which included collaboration with fire, police,

city officials, health district, school district and emergency responders. Some of the towns with completed plans are Boise, Star, Garden City, Kuna, Meridian and Eagle.

The state also completed several table-top exercises with combined grant funds. Some examples are the Area Command supporting the 2009 Special Olympics, focusing on public safety and associated policy issues in reference to local support of the Games; and the Boise Airport Security Tabletop involving coordination with Transportation Security Administration, the FBI and Boise Police subject matter experts who incorporated their inputs into the exercise scenario. The latter was attended by 47 airport operations staff, law enforcement, fire, emergency medical services, airline executives, and military response/management supervisors who collected issues, observations, and lessons learned to be analyzed and used for revising the Boise Airport Emergency Operations Plan. Numerous functional dam exercises also took place, including an Idaho Power exercise, which focused on a major dam failure along the Snake River. EMPG funds were also utilized to respond to local disasters including spring flooding in Kootenai and Shoshone Counties, mudslides in Valley County, and a severe winter storm and extraordinary snowfall emergency in: Bonner, Kootenai, Latah, Boundary, Shoshone, Power, Clearwater, Benewah, Freemont, Boise, Bonneville, Lewis, and Bear Lake Counties.

In addition, EMPG allowed Idaho to assist interested Tribal Nations with mutual aid agreements, and policies and procedures for coordinating response and recovery activities. The state was also able to install communications infrastructure and equipment, providing 24/7 communications access to first responder user groups located in mountain top locations where communications can be interrupted.

IOWA

Iowa works very hard to integrate its homeland security and emergency management functions into a comprehensive strategy that allows them to manage all facets of any disaster, regardless of cause. The integration extends to their grant dollars as well.

With homeland security grant money dedicated to the development, equipping and training of special teams that are available for statewide deployment in times of emergency or disaster, Iowa uses EMPG to develop plans, integrate training, and perform exercises that involve these special teams. The proof of the effectiveness of those efforts was most recently portrayed in the response to the 2008 floods. As a result of the work that has been done using EMPG and other grant funds in a combined effort, Iowa was able to deploy and use elements of its Urban Search and Rescue Team, Incident Management Team, Veterinary Rapid Response Team and Disaster Medical Assistance Team as major players in support of disaster operations in a number of localities across the state. This provided for a more efficient and effective response to what is to date the state's worst disaster.

KANSAS

The Kansas Division of Emergency Management (KDEM) created the Kansas Incident Management Team (IMT) Program with EMPG funding in the spring of 2007. Since then, it has proven to be an invaluable asset during emergency responses across the state, including the June 2008 Chapman Tornado and several flooding events.

An IMT is a group of individuals trained in the Incident Command System and in Emergency Operation Center (EOC) operations that can provide rapid emergency response to a jurisdiction or department during an incident or event. In what can be a chaotic situation, the team offers command and control capability, bringing expertise in logistics, planning and operations.

There are different types of IMTs depending on the size, scope and location of the event. For example, a local IMT is made up of representatives from fire, EMS, Department of Public Works, public health, emergency management, hospitals, law enforcement, county and city government, private industry, education and volunteers. Teams are requested through KDEM. Thanks to EMPG, IMTs are providing reliable knowledge and experience to disaster victims during times of their greatest need.

In addition to IMTs, Kansas uses EMPG to help local jurisdictions develop and update crucial Emergency Operations Plans. Grant funding has resulted in an online planning tool to make local Emergency Operations Plans easily accessible to all local users and the state. This tool allows local emergency planners to make updates and modifications easily and distribute changes to users without cumbersome administrative and tracking procedures. The system is also designed to lead local communities through the planning process using state developed standards, following NIMS guidance and allowing State planning staff to provide immediate guidance and feedback to local jurisdictions.

Since June 2006, when the tool was completed, more than 100 local emergency management agencies have been trained on the new system. KDEM has also approved 80 out of 105 County Emergency Operations Plans, which are compliant with the Kansas Planning Standards, NIMS and ICS. The remaining counties will have approved plans by the end of 2009. The tool has also proven to be one of the most cost effective. To implement the new technology statewide, it cost \$150,000 or less than \$1,500 per county.

KENTUCKY

In 2008, the commonwealth of Kentucky used EMPG dollars to develop and exercise a plan in the event of a New Madrid earthquake occurring in the western portion of the state. When the state was hit with a massive ice storm earlier this year, resulting in its worst disaster ever, state emergency management used the earthquake plan to support western counties decimated by the storm. Though designed for an earthquake, the plan was adapted for this disaster and was key in delivering aid to 103 counties with hundreds of thousands of citizens who had no power, no heat and no food. Also, because the plan had been thoroughly exercised - again due to EMPG funds - the state had already made adjustments and knew that it would work. Advance planning and exercise supported through EMPG saved lives in Kentucky.

MAINE

Despite hiring freezes and budget restrictions, the state of Maine has seen success in its emergency management efforts, thanks in part to EMPG funding. First, EMPG has allowed the state to retain capacity. Core planning, training, exercise, and communications positions functions remain in place during tough economic times because EMPG funds are available to match scarce state resources. Second, it has improved county emergency management agency capacity. EMPG has allowed several county EMAs to add staff and resources. The county agencies are the critical link between the state and local communities. Lastly, EMPG has allowed Maine to innovate at state, county and local levels. Because the EMPG program allows the use of "in-kind" resources as the non-federal match, communities, non-profit organizations and other state agencies can leverage volunteer time, donated resources, or existing non-federal funds to match EMPG for eligible projects.

At the local level, the fielding of Local Capacity EMPG Grants has revived commitment for emergency management in even the smallest communities. Some communities will receive reimbursements as little as \$250. However, even these amounts are seen as a commitment from the state and federal governments to support local EMA programs. This energizes local efforts far more than the funding level would indicate. At the state level, EMPG funds are supporting partnerships with non-profit

organizations and other state agencies to create a variety of positive outcomes. These include public education and outreach, volunteer and donations management and detailed risk analysis for developing hazards.

MARYLAND

A priority for Maryland is to use its EMPG money to promote solid emergency management principles, while strengthening local emergency management agencies. Accordingly, EMPG projects include critical damage assessment training to each area in the state; preparedness plans and exercises for hurricanes, tropical storms and other severe weather incidents in Maryland; and after-action reviews that identify corrective opportunities as well as best practices. One specific project supported by EMPG dollars in Maryland is the coordination of the DelMarVa Emergency Task Force. This is a tri-state preparedness initiative – unique in the Nation – that focuses on hurricanes, tropical storms and other natural disasters as well as man-made incidents. It includes all of Delaware, Maryland's nine Eastern Shore counties and two Virginia counties on the Delmarva Peninsula. Representatives work together toward a coordinated regional response to an event, including evacuation and sheltering planning; communications strategies; and recovery efforts.

MICHIGAN

With limited funds for travel and less manpower, traditional training methods were not meeting the training needs in Michigan. So, two years ago, the Michigan State Police Emergency Management and Homeland Security Division (EMHSD) set out to find an effective solution. With the help of EMPG funds, EMHSD has implemented a Learning Management System that features a web-based, self-paced system. It includes courses such as the "Damage Assessment Teams", which allows local and state teams to come up to speed quickly by reviewing the federal damage classification levels, evaluating the types of hazards they may encounter in a disaster's aftermath, and giving them an opportunity to practice rating damaged homes. The course only runs about 20 minutes and can be taken individually or reviewed in a group setting immediately before the teams go out into the field. Implementation of online training has reduced training costs incurred by local jurisdictions while improving performance in the field.

Michigan is also using EMPG to help address soaring debris related costs. In several recent federal disasters that have involved multi-jurisdictions in the state, debris operations have taken months to complete and several years to close out. The wealth of experiences and "lessons learned" in these large disasters were incorporated into the Michigan Disaster Debris Management Plan and the companion Local Disaster Debris Management Planning Handbook which were funded by the EMPG. Both documents were developed to conform to the requirements set forth in FEMA's Public Assistance Pilot Program. This coordinated planning effort is critically important to the ultimate success of future disaster debris management operations in Michigan. The goal of EMHSD in the coming months is to assist local jurisdictions in developing plans using the EMPG funding while taking advantage of incentives offered by FEMA's Public Assistance Pilot Program to these same local jurisdictions.

MINNESOTA

EMPG funds have allowed the state of Minnesota to address multiple emergency management issues that have a significant impact on disaster response and recovery. First, during the winter of 2009 EMPG monies were used to fund 10 disaster response and recovery workshops for local officials throughout the state. The workshops proved invaluable to the many local officials in the Red River Basin, providing training on the disaster declaration process and disaster assistance programs for individuals, communities and government entities such as schools. As it turned out, the timing of the workshops couldn't have been better. In March and April, Northwestern Minnesota was hit by extensive flooding in this same area that impacted 25 counties as well as one tribal community, and resulted in a major

disaster declaration. EMPG monies also permitted HSEM to fund a disaster recovery programs coordinator position. Among other responsibilities, that staff member plays a pivotal role in leading the activities of the Minnesota Recovers Task Force, which helps bring various resources to local governments attempting to fully recover from a major disaster, like the recent flooding. Finally, Minnesota passed along EMPG dollars to a city for a special regional sheltering project. This “mega shelter” will improve the capacity to effectively manage evacuees from the region including a neighboring state. The project not only includes planning activities with partners from local and state government agencies, but also those with community organizations. The facility owner is also ensuring that the remodeling and construction accommodates the requirements of a shelter with multiple functions.

MISSISSIPPI

Thanks to the current EMPG funding level, all 82 counties in Mississippi, as well as the Mississippi Band of Choctaw Indians, have emergency management programs and emergency management directors. This was not always the case. Back in 2000, when EMPG funding was significantly lower, there were only 43 county emergency management programs.

At the state level, nine area coordinators – all funded by EMPG – cover between six and 11 counties. Each coordinator works closely with their respective local emergency managers, responding to their requests for support and resources, and conducting training for the staff and educational presentations for residents. The importance of this integration came into play in September 2008 when Hurricane Gustav hit. The Mississippi Emergency Management Agency (MEMA) helped coordinate the unprecedented evacuation of more than three million people from South Louisiana and the city of New Orleans. Contra flow of traffic north along Interstates 59 and 55 required communication between multiple southern Mississippi counties with each other and the State Emergency Operations Center. The evacuation was executed perfectly to the plans in place. The large number of evacuees was able to move easily through Mississippi and find shelter thanks to the coordination of all the county emergency managers and MEMA.

NEBRASKA

Within Nebraska, 73 of 93 counties either have a full-time director or are part of a region with a full-time director and part-time deputy directors. This staffing is due to EMPG. Also, every county has a Local Emergency Operations Plan in place that is written to the state planning standards and updated yearly. Every five years, it has a full-scale review and rewrite. This system is in place and supported because of the EMPG funds passed to the local level to support the program. Ultimately, it maintains the existing baseline county programs in the most cost-effective way.

NEVADA

In Nevada, EMPG funding is essential for sustaining emergency management programs throughout the state, particularly as it relates to maintaining state and local emergency management personnel. Most of the full-time state emergency management positions are partially funded through the EMPG program. On the local level, EMPG supports approximately 31 full or part-time positions throughout the state. The total number of positions funded through EMPG funding, for both the state and local governments, is 61 full and part-time positions. All of these individuals are critical in preparing for, mitigating, responding to and recovering from the multiple natural and manmade hazards that Nevada faces. These risks include earthquakes, floods, winter storms, and large scale wildland fires. In fact, Nevada is ranked 4th in the nation for earthquake risks, behind Alaska, California, and Hawaii. EMPG allows the state to secure adequate staffing in order to develop its all-hazard approach.

NEW JERSEY

EMPG funds are used to support a variety of programmatic areas in the New Jersey Office of Emergency Management (NJOEM). For example, the NJOEM has a dedicated Field Training Unit (FTU) that provides more than 30 different courses and trained approximately 3000 state, county, local and other first responders, during 2008. EMPG dollars made several planning initiatives possible, including contra-flow plans for coastal communities, special needs planning initiatives, updating state floodplain management maps and a hazard U.S. (HAZUS) geological survey.

EMPG funding is also used to purchase equipment to address gap and need assessments, as well as supporting emergency management strategic goals. Enhancement of interoperable communications between 21 counties and 566 municipalities is one example of the strategic equipment development. Interoperable radio caches, antennas, wireless communications, repeaters and infrastructure equipment are being secured with a multi fiscal year procurement methodology to maximize performance and fiscal responsibility. Finally, EMPG funding lends direct salary support to 28 positions within the NJOEM offices. All 21 counties and 79 of New Jersey's municipalities received EMPG money to help fund emergency management coordinators salaries. The sub-grant program support extends beyond those localities being funded. For example, all 21 counties must ensure that at least 25% of their non-EMPG funded municipalities take part in an exercise program and submit for exercise credit.

OHIO

In 2008, the State of Ohio allocated approximately 74% of its EMPG funds directly to local governments to focus on sustaining and enhancing emergency management capability. Ohio recognizes the critical importance of building and sustaining local capabilities throughout the planning, response, recovery and mitigation phases of a disaster. As such, EMPG grant funds support 170 full time emergency management personnel in 88 counties who update and enhance county Emergency Operations Plans and applicable annexes that serve as the foundation of local capabilities. The State supports the counties in all aspects of emergency management, including grants management, planning activity identification, training and exercise and special projects. These efforts, coupled with the detailed guidance established for EMPG funds, further enhance the local capabilities and allow for increased identification of risks and hazards that threaten the 11 plus million residents of Ohio's 88 counties.

One such threat occurred in September 2008 when Ohio was faced with hurricane force wind gusts from the remnants of Hurricane Ike. As the winds moved through a large portion of the state, more than five million Ohioans were impacted and many lost power for more than a week. The ability of county emergency management agencies to coordinate response and resource support for the needs of the residents was a credit to their planning and preparedness efforts, supported by Ohio's allocations of EMPG funding.

EMPG has made other efforts possible. Continuity of Government Plan has been developed, involving all three branches of Ohio government; Executive, Judicial and Legislative. Ohio EMA recognizes that a comprehensive Continuity of Government (COG) plan includes not just the Executive branch COG, but also the Judicial and Legislative branches. The agency is aggressively reaching out to the Judicial Branch and Legislative branches to ensure that they have viable COG plans and also assisting the three branches in Continuity of Operations (COOP) planning, to include alternate work locations. The Ohio Supreme Court is now working with judges and court administrative staff and orienting them to the principles and key issues relevant to court emergency preparedness planning to ensure the continuity of court operations and the rule of law. Ohio EMA is offering an abridged COOP planning course for both the Ohio Senate and Ohio House of Representatives staffs and is providing ongoing plan review support. For

the Executive Branch, Ohio EMA developed a web based survey to evaluate technological and equipment needs to assist planning efforts for the move to the alternate location.

OREGON

The EMPG funds a portion of the Oregon Partnership for Disaster Resilience, a coalition between the state and the University of Oregon aimed at developing strategies that provide Oregon with a more holistic and cost-effective approach to addressing natural hazard risk. The project includes a diverse group of stakeholders and resources that work together in coordination and collaboration. This effort has helped counties and local communities in their overall planning, including mitigation, as well as initial steps in catastrophic long term disaster recovery planning.

EMPG funds also supplement very small city and county budgets with much needed training that wouldn't be possible otherwise. The grant helps state and local jurisdictions develop measurable objectives in fully developing comprehensive all-hazard emergency management plans. In addition, EMPG partially funds state-wide projects such as county wide communications plans, continuity of government plans, and developing regional exercise and training plans.

PENNSYLVANIA

EMPG has helped create better educated and better prepared emergency management coordinators throughout the state of Pennsylvania. The Pennsylvania Emergency Management Agency (PEMA) sets training and certification standards for the county coordinators and provides graduated reimbursement to the counties. Until the coordinator is certified, the counties are reimbursed 25-percent of the salary. As an incentive to completing the certification training, the counties are reimbursed 50-percent of the salaries when the coordinator is certified.

PEMA also encourages counties to meet Emergency Management Accreditation Program (EMAP) goals through EMPG. Counties receiving EMPG funding for salaries and benefits are required to submit an Annual Statement which includes the accomplishment of requirements. These requirements are based on EMAP standards and includes areas such as administration and finance; hazard identifications, risk assessment and consequence analysis; and resource management and logistics.

RHODE ISLAND

In the past three years, the state of Rhode Island has seen a trend of competitive local applications for EMPG pass-through dollars grow to more than four times the available funding. Currently, EMPG is supporting the training of more than 86 members of the Rhode Island State cabinet, support staff and essential personnel in the Incident Command System. This has significantly enhanced the understanding of NIMS and incident response, particularly during an all-hazards event and for COOP and COG planning. In addition, ICS training has also been provided with EMPG dollars to more than 1,800 members of various first response agencies along with business partners.

EMPG is also the primary funding mechanism for equipment and training for Urban Search and Rescue (USAR) Teams. A central warehouse for the Rhode Island Emergency Management logistics equipment and special tools and equipment for the USAR teams would not be possible without EMPG. Money has been allocated as well for school safety programs and to purchase emergency generators for shelters and pet sheltering.

SOUTH CAROLINA

Because hurricanes are a common threat to South Carolina, 10 years ago, the South Carolina Emergency Management Division began compiling, publishing and distributing the official South Carolina Hurricane

Guide annually. The publication emphasizes life-safety information and includes input from 12 state agencies, volunteer organizations and the private sector. It has become increasingly popular and now, utilizing EMPG, it's distributed in paper form to more than 675,000 households and businesses. It is also available year-round on the internet. In addition to standard advice about what people should do before, during and after hurricanes, it provides state-specific information, including shelter locations, evacuation routes, information hotline telephone numbers, key web addresses, important radio station emergency information frequencies, insurance information, pet information, and information for people with special needs.

UTAH

When the Utah Crandall Canyon Mine Collapse Disaster occurred in August 2007, emergency managers learned firsthand the importance of EMPG. Prior to the accident, Emery County officials had used the grant to conduct extensive training in the National Incident Management System (NIMS). They also dedicated funds to planning and personnel. These preparedness efforts enabled the local emergency management office to coordinate and work cooperatively with an extensive team of responders and officials that included law enforcement, emergency medical services, natural resources and U.S. Bureau of Land management representatives. As a result, the local EM office managed the incident for more than 30 days with little assistance from outside the region of Carbon and Emery Counties. Without the EMPG funds and the training and planning it made possible, this small community would have been overwhelmed by this tragic disaster that made national headlines.

VERMONT

Vermont uses EMPG dollars in many ways to strengthen local governments and families. Vermont Emergency Management (VEM) publishes 150,000 copies of a popular 12-page Family Preparedness Workbook for less than \$.10 a copy (second printing) and utilizes a distribution network to get them to the public. Partners in that distribution network include state agencies, the food bank (69,000 customers), senior centers, schools, health offices, hospitals, Vermont National Guard members (3,000), town offices, and the Boy Scouts. The workbook lists types of risks that can affect Vermonters, including pandemic flu; what to do in emergency situations; how to prepare a family plan; and where to find more information on these and other preparedness topics. This effort has been very successful; VEM receives on-line, bulk orders everyday at www.vemvt.com. Through a strong individual and family campaign, preparedness and awareness levels have increased substantially, especially for special needs individuals.

VIRGINIA

In March 2006, Virginia opened a new 17,100-square foot Emergency Operations Center (EOC) built with an EOC grant from FEMA to meet increasing emergency/disaster coordination and communications needs. Over the last three years, Virginia has used EMPG funds to support and fill in general funding gaps from the state to nearly double the operations staff and support technological, programmatic, and equipment enhancements that have turned the building into a state-of-the-art communications facility and one of the best EOCs in the nation.

The Virginia Emergency Operations Center provides workspace with full Information Technology and communications support for more than 250 state, federal, private sector and volunteer workers in a secure environment. Its 260-plus computers and numerous display formats, coupled with the ability to interact face-to-face, enables a level of communication and coordination that was impossible in the previous facility. The flexibility of the EMPG program helped make this facility possible while bringing a new level of disaster management capability to the state.

WASHINGTON STATE

Using EMPG funding, a Private Sector Integration Program has been established in Washington State, providing a sustainable link between private sector and public sector stakeholders during disasters so that information and resources needed before, during and after the event can be shared.

In a review of the state's response to a December 2006 windstorm that impacted multiple locations, it became clear that the state needed to improve its two way communications and coordination with private industry before, during, and after a disaster. There had been many examples around the country since 2007 that demonstrated the benefits of private/public partnerships. Private industry had assisted communities impacted by disasters providing resources, volunteers, and expertise. Particularly after Hurricane Katrina, many emergency management organizations recognized the power of pooling private/public resources to overcome the huge challenges posed by catastrophic events.

While many government entities recognize the value of tapping into private expertise and resources, most do not fully understand the need to develop easy access for the private sector to existing preparedness, response and recovery programs. This program "cracks the code" around how plug and play programs for business community access can be developed, and EMPG helped make it possible.

WISCONSIN

EMPG is a major reason for the successful response by both the state and local jurisdictions to the severe storms and flooding that occurred in Wisconsin in June 2008. Wisconsin requires the state, counties and municipalities to develop consistent, emergency management programs. To accomplish this, Wisconsin Emergency Management provides two-thirds of its EMPG grant to county emergency managers. They in turn assist municipalities in developing their annual plans of work. These documents include areas of planning, training, exercising, public education/information, grant administration, and other initiatives that focus on specific local needs.

In addition, county emergency management directors are required to attend monthly meetings with the state emergency management regional directors. These meetings feature guest speakers from other state agencies, voluntary agencies and federal agencies. Planning is done for training and exercises. Through this regular interaction, regional directors get to know county and municipal officials, risks and capabilities.

Ultimately, EMPG allows a comprehensive planning process among Wisconsin state officials, as well as county and local emergency managers. The relationships built through this regular coordination and contact proved to be invaluable during the 2008 flooding. Everyone was on the same page and working from a common playbook to get help where it was needed and restore communities as quickly as possible.

Written Statement
Submitted to the Subcommittee on Homeland Security
House Committee on Appropriations
April 23, 2009

Gerald R. Iwan Ph.D., Executive Director
National Environmental Services Center
West Virginia University, Morgantown, WV

Chairman Price, Ranking Member Rogers, and Members of the Subcommittee:

We request an appropriation of \$1.5 million in FY 2010 directed to the Community Water Infrastructure Center (CWIC). The mission of the Center is to develop resiliency in small and rural communities through strengthening their water services infrastructure to withstand and quickly recover from natural or man-made disasters. One of the benefits of this program will be to enable West Virginia to assist persons from the National Capitol Region who migrate westward to escape the consequences of a massive terrorist event in the Region.

Introduction

My name is Gerald Iwan and I am the Executive Director of the National Environmental Services Center (NEEC) at West Virginia University. Our center is home to both EPA-funded and USDA-funded programs that provide comprehensive drinking water and wastewater environmental services to small communities and rural areas. Although located in West Virginia, we have worked with communities nationwide for the past 30 years to address their drinking water, wastewater, and community resiliency needs. We partner with the USEPA and USDA in providing information, training, and technical assistance essential each Agency's drinking water and wastewater mission.

Need

West Virginia's mountainous landscape is mostly populated by small and rural communities, many of which are economically disadvantaged. Among the State's abundance of natural resources, water ranks high in both quantity and quality. In contrast, West Virginia also has a legacy of inadequate drinking water and wastewater treatment in most communities, many of whose water supplies are contaminated by the chemical byproducts of coal mining. In addition to chemicals, many of West Virginia's waters are also polluted by untreated sewage discharged into surface water and groundwater by individual residences. Lack of basic water infrastructure has limited community growth and impeded economic development in areas outside of the State's few Standard Metropolitan Areas (SMA's).

Now, in the post-911 era, problems related to West Virginia's lack of small community water infrastructure reach beyond our State's borders. With all of its available land and water, West Virginia's water infrastructure cannot accommodate a mass influx of people

from the National Capital Region, as Congress has suggested, in response to a large-scale hazardous event. In fact, the additional demand placed upon our communities with their limited infrastructure would likely result in an additional public health crisis for our residents and those relocating from high threat areas. Negative outcomes from a mass evacuation could include:

- A shortage of drinking water
- Illnesses or deaths
- Public panic and fear of drinking the water
- Costs of rehabilitating, rebuilding, or decontaminating water systems
- Long-term contamination of water reservoirs and related resources
- Interruption of firefighting capability
- Interruption of sanitary services

The CWIC project proposes a center that will address West Virginia's water infrastructure resilience¹ issues from a community, state, and regional perspective. Many of the capabilities developed under our program will be applicable to small and rural communities nationwide.

Implementation and Deliverables

Foundation expertise of the National Environmental Services Center includes information clearinghouses, training, technical assistance, field assistance, community planning and drinking water & wastewater technology demonstrations. We will apply our expertise to carry out core activities to promote resilient water infrastructure within small and rural communities. CWIC teams will work with the State of West Virginia, its counties and municipalities, and other relevant stakeholders, to inventory and assess the condition of West Virginia's water quality and infrastructure, and those factors that contribute to degradation. Much of the data currently exists, some data sets need to be collected, and some data sets need to be formatted for use, accessibility and integration with other data sets.

We will conduct outreach, partnering and planning programs with local and state government, with volunteer and nonprofit groups, such as those invested in watershed management, and with industry, to raise and encourage awareness and implementation of best practices for developing a sustainable and resilient water infrastructure. CWIC teams will be comprised of NESC staff, WVU's Multidisciplinary Task Force members, and members of other partnering sector service provider organizations. Demonstration

¹ Resilience refers to the ability to withstand and recover from natural or manmade disasters. Resilient water infrastructure is characterized by its ability to maintain or restore service during and after an emergency, minimize system damage and loss to customers, minimize negative impacts on employees, maintain public health and safety, and minimize adverse effects on the environment. Additionally, the interdependence among the water sector and other sectors is recognized and supported. For example, the need for available water for fire hydrants to support first responder efforts [References: EPA, The Infrastructure Security Partnership (TISP), and the Water Environment Research Foundation (WERF)]

projects will be implemented to address specific problems and to showcase solutions and models that can be replicated in similar situations (for example, the integration of drinking water protection and wastewater treatment, as practiced in NESC's SMART about Water project).

Data gathered and synthesized by the project will be particularly useful to the State's Department of Homeland Security in assessing our water infrastructure's capacity to accommodate a mass migration, and to plan for and determine the areas of the State most able to receive the influx of migrating persons. CWIC will maintain a national presence through affiliation with partners such as the WARN System (Water Assistance Resource Network), and the State Onsite Regulators Alliance (SORA), and other national organizations, associations, and federal agencies.

Funding Authority

The Department of Homeland Security through the Federal Emergency Management Administration (FEMA) is charged with and funded through appropriations to provide for States' "planning, coordination, execution and decision-making related to mass evacuation during a disaster." West Virginia is mandated by Congress to be incorporated and integrated into activities associated with the evacuation of the National Capital Region, as defined in the Homeland Security Act of 2002. No funding for this mandate is provided for West Virginia in the bill, H.R. 2638, The Department of Homeland Security Appropriations Act, 2008, signed by the President on September 30, 2008, or through the Omnibus Appropriations Bill, 2009. DHS provides funding for specific projects through congressionally-directed appropriations. Based upon our experience, we believe this project has the potential to save lives and money, and can serve as a model for other states to help their small and rural communities prepare for and mitigate large-scale disasters.

Request

We request \$1.5 million in congressionally directed funding for the Community Water Infrastructure Center to undertake the program described above. Thank you for considering our request.

Contact Information

Community Water Infrastructure Center
West Virginia University
Gerald R. Iwan
304-293-4191 Ext. 5584
gerald.iwan@mail.wvu.edu

Richard A. Bajura
304-293-2867 Ext. 5401
richard.bajura@mail.wvu.edu

**Thomas Donlon
Director
New York State Office of Homeland Security**

**Testimony for the Record
House Appropriations Subcommittee on Homeland Security
“Securing the Nation’s Rail and Transit System”
March 13, 2009**

Chairman Price, Ranking Member Rogers, and Members of the Subcommittee, thank you for allowing the New York State Office of Homeland Security (NYS OHS) to submit testimony for the record on the state’s transit security activities.

I am pleased to share with the Subcommittee the steps NYS OHS has taken with its transit partners to better protect and secure New York City’s mass transit system. Securing a deliberately open system that must move millions of people quickly and easily each day is challenging, but we continue to make tremendous progress through multi-agency collaboration and support from Congress, the Transportation Security Administration (TSA) and the Federal Emergency Management Agency (FEMA).

As you are aware, the New York City metropolitan area has the largest collection of rail transit systems in the nation, providing service to over 8.5 million passengers a day. The Transit Security Grant Program (TSGP) is the region’s primary source of federal funding for securing this sprawling system. Prior to 2007, the NYC region determined its TSGP funding priorities based on “jump ball funding.” Dollar amounts were put on the table and the eight transit agencies threw projects up in the air in an attempt to get funding applied to them. There was no overall risk analysis guiding the security efforts for the NYC transit system.

In March of 2007, NYS OHS brought together the metro-NYC transit agencies to participate in the first classified, system-wide vulnerability and threat assessment. The threat assessment involved the heads of all the transit agencies as well as TSA and New York Police Department Counterterrorism Division. The meeting resulted in a fresh perspective on threat and vulnerability. The group agreed to conduct an unprecedented “red team” exercise to disclose vulnerabilities in the transit system.

The red-team exercise revealed gaps in security and the need for system-wide security enhancements. In August 2007, the transit agencies and TSA Administrator Kip Hawley together developed a plan for regional security enhancements. Among the enhancements were bomb dog teams, Behavioral Assessment Screening Systems and training exercises in counter-surveillance. Administrator Hawley was so impressed with the cooperative approach that he expedited the formal grant justification process and committed to funding the entire spectrum of needed-capabilities.

The state's transit security efforts led to rethinking its utilization of the National Guard. Following 9/11, the New York National Guard created Joint Task Force-Empire Shield (Empire Shield), an operational force of National Guardsmen that augmented security forces at New York's transit systems, airports, and nuclear power plants. Taking the lessons learned from the red-team exercise, Empire Shield was reconfigured in 2007 from a static force to a rapid response force based out of Fort Hamilton, Brooklyn.

The reconfiguration permits Empire Shield to provide a "surge" capability to protect critical infrastructure during periods of heightened threat and immediate access to military equipment and resources to address man-made and natural disasters. Empire Shield enhances the overall security posture of the entire NYC area and represents the only capability of its kind in the country.

Empire Shield participates in NYC's Multiple Agency Super Surge (MASS) program. In this capacity, Empire Shield works closely with the MTA to augment its security patrols at Pennsylvania Station, Grand Central Station, and MTA's bridges, tunnels and bus stations. Furthermore, Empire Shield provides a no-notice Quick Reaction Force (QRF) capability that supplements the current mission sets for MTA. The initial QRF can be deployed within 4 hours to support MTA incident or surge operations.

The value of Empire Shield to transit security in NYC cannot be understated. For example, between December 14, 2008 and January 15, 2009, Empire Shield provided the MTA with 994 total service-members and 7,952 hours on the ground around Christmas and New Year's Eve.

Fiscal Year 2009 Changes to TSGP

NYS OHS is concerned with the changes Congress made to TSGP in the FY09 Department of Homeland Security Appropriations bill, specifically the requirement that FEMA award TSGP grants directly to transit agencies and not notify OHS of the awards until after they have been issued.

NYS OHS opposes this change for two reasons. First, it removes OHS as the State Administrative Agency (SAA) and brings back "jump ball" parochialism to TSGP. As the SAA, the State is able to take a holistic and unbiased view of the security needs of NYC's interdependent transit systems and guide funding to the areas most in need. Removing New York State from the transit security funding process is counterproductive as it will reduce regional collaboration and make the tri-state's transit systems less secure.

We are pleased that our transit partners, notably the MTA, have recognized the importance of having OHS at the table. We strongly agree with the recommendation made by MTA Security Chief Bill Morange in his testimony before this Subcommittee, namely that OHS again be designated the SAA for TSGP and receive funding to cover its management and administrative costs.

The State also opposes the Congressional change to TSGP because Empire Shield's transit security operations have been supported, in part, by utilizing the state's 3 percent management and administrative share of TSGP. While TSGP allows law enforcement entities, such as NYPD and the Metropolitan Transportation Agency Police, to be eligible to receive funding under the program, attempts to have the New York National Guard listed as an eligible sub grantee for FY09 TSGP were blocked, reportedly, by the Office of Management and Budget (OMB).

Irrespective of the matter of the SAA, we hope that FEMA and TSA will continue to recognize the importance of funding operational packages through TSGP and work with OHS and the New York National Guard to make Empire Shield an eligible subgrantee for the transit security monies included in the American Recovery and Reinvestment Act and future fiscal years.

In conclusion, NYS OHS has taken an active role in helping to coordinate NYC's Regional Transit Security Working Group. The collaborative approach to transit security that the working group embodies has been recognized by TSA and FEMA as a best-practice. In fact, the FY09 TSGP grant guidance encourages all Tier I regions to emulate New York's model. With the Subcommittee's support, we will continue to build-on the progress we have made to date. Again, thank for providing NYS OHS with the opportunity to discuss our transit security initiatives.

WITNESSES

	Page
Ashley, W. R	1, 95
Bastian, Anthony	580
Buswell, Bradley	427
Cuellar, Hon. Henry.....	559, 568
Decker, Russell	604
Donlon, Thomas	652
Dragani, Nancy	629
Eckles, Jack	1
Ellison, Hon. Keith.....	559, 560
Halvorson, Hon. Debbie	559, 564
Holt, Hon. R. D.....	559, 575
Hornberger, Jack	582
Iwan, G. R	649
Kelley, C. M	622
Kraninger, Kathleen	347
McHugh, Hon. J. M	586
Millar, W. M	590
Miller, R. C	581
Mocny, Bob	347
Morange, Bill	1
Perkins, Douglas	583
Romanowich, J. F	584
Rossides, Gale	281
Sammon, John.....	1, 95
Schue, Charles	598

INDEX

SECURING THE NATION'S RAIL AND TRANSIT SYSTEMS, PART 1

	Page
Opening Statement of Chairman Price	1
Opening Statement of Ranking Member Rogers	7
Opening Statement of John Sammon, Assistant Administrator for Transportation Sector Network Management	12
Opening Statement of W. Ross Ashley, Assistant Administrator for Grant Programs	20
Opening Statement of Bill Morange, Deputy Executive Director and Director of Security, New York Metropolitan Transportation Authority	34
Opening Statement of Jack Eckles, Deputy Executive Officer for System Safety and Security, Los Angeles County Metropolitan Transportation Authority	44
Award and Funding Delays	58
State Administrative Agent Issue	60
Drawdown of Funds	61
Historic Preservation Requirements	61
TSA Role	62
TSA Modifications to Grant Language	62
Security Rankings	62
Interaction with the Transit Community	62
Funding Availability	64
2006 Funding Drawdown	65
Approval of the 2006 Budget	67
Process Improvements	67
Joint Administration by FEMA and TSA	67
Tier One Process	67
Cash Flow Report	68
METRA Request	68
Two Agencies in Charge	69
Applications Process	69
FEMA Fiduciary Responsibility	69
Expedite Grant Process	70
Report Requirement	70
Importance of Funding	71
Advice on Streamlining the Process	73
Report Clarification	76
9/11 Act Provisions	77
Agency Performance Assessment	77

SECURING THE NATION'S RAIL AND TRANSIT SYSTEMS, PART 2

Opening Statement of Chairman Price	95
Opening Statement of Ranking Member Rogers	100

	Page
Opening Statement of John Sammon, Assistant Administrator for Transportation Sector Network Management	103
Opening Statement of W. Ross Ashley, Assistant Administrator for Grant Programs	104
Approval of Projects Before Award and Backlog	111
TSA Approval of Backlog Projects	113
Interim Report and Final Report	114
Report: Transit and Rail Grant Programs	115
Funds for FY 2010	138
Unspent Funds	138
Congressional Direction to Accelerate Efforts	140
Obligation of Funds	140
Acceleration of Project Approval	141
Funding for FY 2010	142
Meeting with Grantees on Expenditures	142, 144
Rail Transit Security	143
Delays in Drawdown of Funds	144
Communication with Grantees	145
FEMA's Risk Formula	146
Draw-Down Figures for New York	146
Reducing Appropriations	147
Funding Priorities	147
Testing and Deploying Screening Equipment	148
Grant Program Administration	149
Questions for the Record Submitted by Chairman David Price to John Sammon	153
Transit and Passenger Rail Grants	153
Working with the Department of Transportation	155
Surface Transportation Inspectors	157
Visible Intermodal Protection and Response Teams	160
Ability of Transit Agencies to Meet Security Requirements	166
Secretarial Action Directives	167
Regional Transit Security Working Groups	168
9/11 Commission Act	169
Canine Teams	172
Toxic Inhalation Hazard	173
Research Programs Related to Surface Transportation Security	174
Management	175
Questions for the Record Submitted by Chairman David Price to W. Ross Ashley	260
Transit and Passenger Rail Grant Funding	260
Working with the Department of Transportation	262
Secretarial Action Directives	263
Questions for the Record Submitted by the Honorable Nita Lowey to W. Ross Ashley	264
Grant Program Expenditures	264
Transit Grants Allocation Methodology	264
Questions for the Record Submitted by the Honorable Nita Lowey to John Sammon	265
Grant Program Expenditures	265
Amtrak Security	265
Questions for the Record Submitted by the Honorable Lucille Roybal-Allard to John Sammon	266
Mismanagement of the Transit Security Grant Program	266
Allocation of TSA Resources to Safeguard Mass Transit	268

	Page
Questions for the Record Submitted by the Honorable Lucille Roybal-Allard to John Sammon —Continued	
Training for Transit, Rail and Bus Workers	268
Questions for the Record Submitted by Ranking Member Rogers to W. Ross Ashley	270
TSA Security Assessment of Largest Mass Transit and Rail Agencies	270
Anticipated Number of Additional VIPR Teams	270
Recent DHS IG Report on Surface Inspectors	271
Surface Inspectors Role in Larger Surface Security Strategy	271
TSA Pilot Program Within NYC Subway System	272
Questions for the Record Submitted by the Honorable Ken Calvert to John Sammon	273
Rail Car Tracking	273
Questions for the Record Submitted by the Honorable Ken Calvert to Jack Eckles	275
Closed Circuit Television	275
Grant Guidance	275
Questions for the Record Submitted by the Honorable Ken Calvert to Bill Morange	277
Grant Guidance	277
 IMPROVING THE EFFICIENCY OF THE AVIATION SECURITY SYSTEM	
Opening Statement of Chairman Price	281
Opening Statement of Ranking Member Rogers	285
Opening Statement of Gale Rossides, Acting Administrator, Transportation Security Administration	289
Air Cargo Screening Progress	300
Tamper-Proof Technology	301
Air Cargo Chain of Custody	301
International Air Cargo Screening	302
Equipment for Inspection of Air Cargo	303
Upgrade Security Equipment	303
Number of Screeners	306
Secure Flight	306
Mass Transit Security Help	307
FEMA Problems	308
Focus on Air Transportation Versus Other Modes	308
Employee Screening	309
Collective Bargaining for TSA Employees	310
Bus Travel	311
TSA Bus Security Activities	312
Securing Uniforms and Badges	313
Security of Airport Workers	313
Large Aircraft Security Program	314
Questions for the Record Submitted by Chairman David Price to Gale Rossides	317
Air Cargo Security	317
Checkpoint Technologies	323
Explosive Detection Systems (EDS)	327
Maintenance and Utility Costs for Screening Technologies	329
Transportation Security Officers	331
Aviation Regulation and Other Enforcement	336
Security at Foreign Repair Stations	337
Federal Flight Deck Officer and Flight Crew Training	338
Secure Flight	339

	Page
Questions for the Record Submitted by Chairman David Price to Gale Rossides—Continued	
Screening of Aviation Workers	340
Air Crew Screening	342
9/11 Act Expenditure Plan	343
School Bus Security Assessments	344
Transportation Security Support	344
Reception and Representation	347
Bonuses	347
Travel	348
Unobligated Balances	349
Questions for the Record Submitted by Ranking Member Rogers to Gale Rossides	351
Secure Flight	351
Large Aircraft Security Program	351
Questions for the Record Submitted by the Honorable John Abney Culberson to Gale Rossides	352
Canadian Bag Rescreening	352
Questions for the Record Submitted by the Honorable Ken Calvert to Gale Rossides	353
ARRA Funding for John Wayne Airport	353
Biometric Access Controls	353
Installation of New Technology at Airports	354
Redundancy in TSA Regulatory System	354

BIOMETRIC IDENTIFICATION

Opening Statement of Chairman Price	356
Opening Statement of Ranking Member Rogers	360
Opening Statement of Kathleen Kraninger, Deputy Assistant Director of Policy, DHS Screening Coordination Office	368
Opening Statement of Bob Moczny, Director, United States Visitor and Immigrant Status Indicator Technology	369
Passports Issued to GAO Investigators	382
Databases Managed by DHS	383
US-VISIT Identity Management Services	384
Secure Communities	385
US-VISIT Immigration Control or Inventory	385
Exit Solution	386
DoD Biometrics	387
Exit System	388
Two-Print and Ten-Print Data Collection	389
Biometric Storage System	389
Pilot Projects	390
Border Crossing By Car and on Foot	390
Border Crossing Baggage Check	392
Visa Waiver Program	393
Exit Strategy	393
Interaction with E-Verify Program	394
Biometric Identifier Attached to Social Security Card	395
Number of Individuals Processed Each Year	395
Next Exit Pilot Program	396
Eye Scan Technology	396
Potential Impacts on RFID Enabled Documents	397
Pass Card for the Mexican Border	398
Accuracy Issues	399

	Page
Exit System Add to US-VISIT	401
Global Entry Program	403
International Registered Travel Program	404
Questions for the Record Submitted by Chairman David Price to Kathleen Kraninger and Bob Mocny	405
US-VISIT and Overstay Identification	405
US-VISIT: Exit	406
US-VISIT—Migration to 10-Print Standard	408
US-VISIT Governance	410
Unique Identity	411
US-VISIT Performance	412
US-VISIT Staffing	412
US-VISIT Cybersecurity	413
Enrollment	413
DHS Biometrics Technology	414
Enumerator	417
Effectiveness	418
Impact on Travel and Trade	419
Proper Use of Data	420
Persistence of Data Presented by Individuals	421
IDENT/BSS	422
State Department Databases and DHS	422
DoD Databases and DHS and HSPD 6	423
HSPD 24	423
HSPD 12	428
Airport Credentialing and Biometrics	429
Global Entry	431
Registered Traveler	432
Questions for the Record submitted by Ranking Member Rogers to Kathleen Kraninger and Bob Mocny	433
TWIC	433
Screening Coordination	433
Screening Redundancy with TWIC and HAZMAT	434

**DEVELOPING AND TRANSITIONING HOMELAND SECURITY
RESEARCH PRODUCTS INTO USE**

Opening Statement of Chairman Price	436
Opening Statement of Ranking of Member Rogers	441
Opening Statement of Bradley Buswell, Acting Undersecretary for Science and Technology, Department of Homeland Security	446
Resilient Electric Grid	483
Engage the Private Sector	485
Non-Flammable Gasoline and Levee Break Fixes	488
Vehicle-Borne Improvised Explosive Devices	488
List of Capability Needs	489
Prioritization of S&T Efforts	490
Security of Capability Information	490
California Homeland Security Consortium	491
Liquid Detection Efforts	492
Private Sector Involvement	493
Unexpended Funds	494
Resilient Grid Project Cyber Vulnerabilities	496
Domain Name Security	496
NBAF Safety on Mainland	497

	Page
Information Availability	498
Container Security Devices	499
Strategic Plans	500
Cyber Intrusions	501
Foliage-Penetrating Radar	502
Questions for the Record Submitted by Chairman David Price to Bradley Buswell	504
BioWatch	504
Regional Biocontainment Laboratories	508
Chemical Programs	508
Counter MANPADS	509
Air Cargo	510
The Future Attribute Screening Technology (FAST)	512
Container and Advanced Container Security Devices	512
Supply Chain Architecture Project	513
Hybrid Composite Container	513
Technology Clearing House	514
Inclusion of Stakeholders	519
Border Inspection Technology Projects	526
International Agreements	526
Basic Research	527
Centers of Excellence	529
First Responders	532
Demonstration and Pilot Programs	533
National Bio- and Agro-Defense Facility (NBAF)	541
Test & Evaluation and Standards	545
Management	546
Contracts	559
Questions for the Record Submitted by Ranking Member Rogers to Bradley Buswell	564
Container Security Device	564
Counter IEDs	564
Screening Redundancy with TWIC and HAZMAT	434
MEMBERS REQUESTS HEARING DAY	
Opening Statement of Chairman Price	568
Opening Statement of the Honorable Keith Ellison	569
Opening Statement of the Honorable Debbie Halvorson	573
Opening Statement of the Honorable Henry Cuellar	577
Opening Statement of the Honorable Rush D. Holt	584
Testimony of the Honorable John M. McHugh	585
OUTSIDE WITNESS TESTIMONY	
American Public Transportation Association	599
UrsaNav	607
International Association of Emergency Managers	613
Fleet Reserve Association	619
National Congress of American Indians	628
National Treasury Employees Union	631
National Emergency Management Association	638
National Environmental Services Center	658
New York State Office of Homeland Security	661