THE FISCAL YEAR 2010 BUDGET FOR THE NATIONAL PROTECTION AND PROGRAMS DIRECTORATE AND THE TRANSPORTATION SECURITY ADMINISTRATION

HEARING

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION

OF THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

JUNE 10, 2009

Serial No. 111–23

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE

51–494 PDF WASHINGTON : 2011

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

Bennie G. Thompson, Mississippi, *Chairman*

Loretta Sanchez, California
Jane Harman, California
Peter A. DeFazio, Oregon
Eleanor Holmes Norton, District of Columbia
Zoe Lofgren, California
Sheila Jackson Lee, Texas
Henry Cuellar, Texas
Christopher P. Carney, Pennsylvania
Yvette D. Clarke, New York
Laura Richardson, California
Ann Kirkpatrick, Arizona
Ben Ray Luján, New Mexico
Bill Pascrell, Jr., New Jersey
Emanuel Cleaver, Missouri
Al Green, Texas
James A. Himes, Connecticut
Mary Jo Kilroy, Ohio
Eric J.J. Massa, New York
Dina Titus, Nevada
Vacancy

Peter T. King, New York
Lamar Smith, Texas
Mark E. Souder, Indiana
Daniel E. Lungren, California
Mike Rogers, Alabama
Michael T. McCaul, Texas
Charles W. Dent, Pennsylvania
Gus M. Bilirakis, Florida
Paul C. Broun, Georgia
Candice S. Miller, Michigan
Pete Olson, Texas
Anh "Joseph" Cao, Louisiana
Steve Austria, Ohio

I. Lanier Avant, *Staff Director*
Rosaline Cohen, *Chief Counsel*
Michael Twinchek, *Chief Clerk*
Robert O'Connor, *Minority Staff Director*

SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION

Sheila Jackson Lee, Texas, *Chairwoman*

Peter A. DeFazio, Oregon
Eleanor Holmes Norton, District of Columbia
Ann Kirkpatrick, Arizona
Ben Ray Luján, New Mexico
Emanuel Cleaver, Missouri
James A. Himes, Connecticut
Eric J.J. Massa, New York
Dina Titus, Nevada
Bennie G. Thompson, Mississippi *(Ex Officio)*

Charles W. Dent, Pennsylvania
Daniel E. Lungren, California
Pete Olson, Texas
Candice S. Miller, Michigan
Steve Austria, Ohio
Peter T. King, New York *(Ex Officio)*

Michael Beland, *Staff Director*
Natalie Nixon, *Deputy Chief Clerk*
Joseph Vealencis, *Minority Subcommittee Lead*

CONTENTS

Page

STATEMENTS

WITNESSES

APPENDIX

THE FISCAL YEAR 2010 BUDGET FOR THE NATIONAL PROTECTION AND PROGRAMS DIRECTORATE AND THE TRANSPORTATION SECURITY ADMINISTRATION

Wednesday, June 10, 2009

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON TRANSPORTATION SECURITY AND
INFRASTRUCTURE PROTECTION,
Washington, DC.

The subcommittee met, pursuant to call, at 2:15 p.m., in Room 311, Cannon House Office Building, Hon. Sheila Jackson Lee [Chairwoman of the subcommittee] presiding.

Present: Representatives Jackson Lee, Luján, Cleaver, Himes, Massa, Dent, and Lungren.

Ms. JACKSON LEE. The subcommittee will come to order.

Let me indicate that my delay was related to some security concerns that are occurring in and around the Capitol.

Some of you may have heard that there was a shooting at the Holocaust Museum. The information I have is that two persons may have lost their lives. We don't have all the facts. But, hearing no objection, I would like for us to just have a moment of silence before we start this hearing.

Thank you.

The subcommittee will come to order. The subcommittee is meeting today to receive testimony on the fiscal year 2010 budget for the National Protection and Programs Directorate and the Transportation Security Administration. Our witnesses today will testify about the budget request of their respective components for fiscal year 2010.

At the onset, I would like to thank the witnesses for appearing before us today. Because schedules are hectic and the Deputy Under Secretary must leave before 3:00 p.m., I would like to proceed as quickly as possible. In addition, I would ask the indulgence of the Deputy Under Secretary if we are a few minutes beyond, but we recognize his scheduling issue.

STATEMENTS OF PHILIP R. REITINGER, DEPUTY UNDER SECRETARY, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY AND GALE D. ROSSIDES, ACTING ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION, DEPARTMENT OF HOMELAND SECURITY

Ms. JACKSON LEE. Without objection, I would like to request that the witnesses' testimony be considered as read so that we can move directly to questions. Hearing no objection, it is so ordered.

[The statements of Mr. Reitinger and Ms. Rossides follow:]

PREPARED STATEMENT OF PHILIP R. REITINGER

JUNE 10, 2009

Good morning, Chairwoman Jackson Lee, Ranking Member Dent, and Members of the subcommittee. Thank you for the opportunity to appear before you to discuss the progress the National Protection and Programs Directorate (NPPD) has made and how the President's budget request for fiscal year 2010 will position us to support the overall Department mission to protect and secure our Nation. I will also take this opportunity to highlight some of the Directorate's accomplishments.

NATIONAL PROTECTION AND PROGRAMS DIRECTORATE BUDGET OVERVIEW

The fiscal year 2010 budget request for NPPD is $1.959 billion and includes 2,710 Federal positions. This is an increase of $801 million over the fiscal year 2009 appropriated amount of $1.158 billion.

The primary driver of the budgetary and personnel increase arises from the requested transfer of $640 million and 1,225 positions of the Federal Protective Service (FPS) to NPPD from U.S. Immigration and Customs Enforcement (ICE). The proposed transfer aligns the FPS mission of Federal facilities infrastructure protection within the NPPD mission of critical infrastructure protection. Further, NPPD chairs the operations of the Interagency Security Committee, a group that includes the physical security leads for all major Federal agencies and whose key responsibility is the establishment of Government-wide security policies for Federal facilities. These missions are complementary and mutually supportive, and the alignment resulting from the transfer improves and advances the mission effectiveness of both FPS and NPPD.

To ensure a smooth transition pending congressional approval, NPPD, ICE, and FPS have formed a joint transition team. The transition team is reviewing a recently completed inventory of the financial, procurement, and administrative support services that ICE currently provides for FPS, along with the annual costs ICE charges for those services. Services that can be provided by NPPD or DHS Under Secretary for Management (USM) will be transferred from ICE. In those cases in which it is determined that ICE should continue as the service provider for fiscal year 2010, a Service Level Agreement between FPS and ICE will be established to ensure there is no disruption to operations during the transition until such time that services can be fully transferred to NPPD or USM in fiscal year 2011.

Filling vacant Federal positions and right-sizing the Federal and contractor staff ratio across NPPD is my upmost priority. NPPD has made great strides in filling critical positions, but much work remains to build out a cadre of Federal staff across the Directorate. NPPD has brought on board 300 new employees over the last 12 months, and currently has approximately 800 Federal employees on board out of the 1,064 fiscal year 2009 positions. We are projecting bringing on board another 200 by the end of fiscal year 2009. The fiscal year 2010 budget request includes 350 additional Federal staff across the entire Directorate offset by funding decreases in contractor support funding. The fiscal year 2010 request also includes 71 new positions mainly to support infrastructure security compliance and cybersecurity. This will bring NPPD to a total workforce of 2,710 in fiscal year 2010.

I would now like to highlight some NPPD accomplishments as well as review the fiscal year 2010 requested budgets for the Office of Infrastructure Protection, the Office of Risk Management and Analysis, US–VISIT, and the Office of Cybersecurity and Communications.

Office of Infrastructure Protection

The Office of Infrastructure Protection (IP) leads the coordinated national effort to reduce risk to our critical infrastructure and key resources (CIKR) posed by acts of terrorism; it also enables national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency. IP has achieved a number of key milestones in the past year, such as:

- Assigned preliminary risk tiers for facilities covered by Chemical Facility Anti-Terrorism Standards (CFATS), a comprehensive set of regulations that protect high-risk chemical facilities from attack and prevent theft of chemicals for use as weapons.
- Provided physical security and risk data to 5,000 registered Homeland Security Information Network—Critical Sector (HSIN–CS) users responsible for critical infrastructure and key resources security in a coordinated national effort to reduce risk posed by acts of terrorism and natural disasters. This included the development and deployment of targeted baseline critical infrastructure and key resource protection information-sharing capabilities.
- Assisted the Government of Trinidad and Tobago (GOTT),[1] as well as private sector owners and operators, in identifying vulnerabilities throughout the liquefied natural gas system, providing recommendations for enhanced security and protective measures to mitigate risk. This operation was DHS' first comprehensive, system-based vulnerability assessment of a foreign nation's infrastructure system and has become the model for international CIKR security engagements for both DHS and other departments.
- Integrated the State, Local, Tribal and Territorial Government Coordinating Council into the full cycle of national infrastructure protection planning and reporting. The Council is a forum for its representatives to engage with the Federal Government and CIKR owners and operators. The Council integrates Council stakeholders into the national level National Infrastructure Protection Plan (NIPP) framework, its Critical Infrastructure Partnership Advisory Council, and 18 Sector/Government Coordinating Councils. This evolution of the CIKR partnership model allows all levels of government to provide input into both the NIPP and Sector-Specific Plans as well as their implementation.
- Established State and local critical infrastructure protection training and technical assistance programs. Not only do these programs support standardized infrastructure and risk information, they also provide training to assist State and local law enforcement, emergency responders, emergency managers, and other homeland security officials in understanding the steps necessary to develop and implement comprehensive CIKR protection programs.

IP's fiscal year 2010 request is $333.3 million and includes 725 Federal positions. This request maintains critical capabilities; expands enforcement of the chemical security; supports development of final ammonium nitrate regulations; funds new nuclear reactor security consultations with the Nuclear Regulatory Commission; supports five Regional Resiliency Assessment Projects; and enhances coordinated national bombing prevention and improvised explosive device security efforts.

Infrastructure Security Compliance: Chemical Security and Ammonium Nitrate

The total funding requested for fiscal year 2010 to support the regulation of high-risk chemical facilities and establish ammonium nitrate regulations is $103.4 million, which includes 268 Federal staff.

The increased funding request supports the hiring, training, equipping, and housing of additional inspectors. Funding will also support the completion and publication of final ammonium nitrate regulations that will help prevent the use of ammonium nitrate in an act of terrorism through both required registration and verification processes and inspection and audit procedures.

As mentioned previously, DHS released CFATS and the final CFATS Appendix A rule, listing approximately 300 "Chemicals of Interest" and associated threshold quantities. Pursuant to CFATS, facilities possessing threshold amounts of Appendix A chemicals were required to complete a Top-Screen assessment within 60 days of the release of Appendix A (i.e., by January 22, 2008) or, if the facility acquires an Appendix A chemical subsequent to the release of Appendix A, within 60 days of the facility's acquisition of that chemical. Facilities preliminarily designated as high-risk based on the Top-Screen submissions were also required to complete Security Vulnerability Assessments, and, if that high-risk status is confirmed by the Security

[1] The United States imports approximately 70 percent of its liquefied natural gas from GOTT, and any disruptions to the system would have an immediate impact on domestic energy supply and security, particularly for the Northeastern United States.

Vulnerability Assessments, will be required to develop Site Security Plans and implement measures meeting DHS-defined risk-based performance standards.

To assist facilities in performing these obligations, the Department developed an on-line suite of tools known as the Chemical Security Assessment Tool, which includes, among other applications, the Top-Screen, Security Vulnerability Assessment, and Site Security Plan tools; a Risk-Based Performance Standards Guidance Document that facilities may use when developing their Site Security Plans; and a Help Desk to answer questions regarding CFATS. Additionally, upon request, the Department performs technical consultations and technical assistance visits for facilities with questions regarding the compliance process. To date, over 36,000 chemical facilities have submitted Top-Screens, with over 7,000 facilities preliminarily designated high-risk in June 2008 and required to submit Security Vulnerability Assessments. Due to changes facilities have made around chemicals of interest since the preliminary designations a year ago, the number of high-risk facilities as of June 2009 has gone down to 6,414 facilities.

The Department recently sent final notification letters to the highest risk (Tier 1) facilities, confirming the facilities' high-risk status and initiating the 120-day time frame for submitting Site Security Plan and implementing the associated security measures. The Plans are due back to the Department on September 15, 2009. The current projections for each type of facility are as follows: Tier 1—182; Tier 2—680; Tier 3—1,612; and Tier 4—3,940. Following initial approval of the Site Security Plans, the Department expects to begin performing inspections in the first quarter of fiscal year 2010, commencing with the designated Tier 1 facilities.

Vulnerability Assessments

An additional $3 million is requested in fiscal year 2010 to support Vulnerability Assessment Projects.

Section 657 of the Energy Policy Act of 2005 (Public Law 109–58) requires DHS to perform security consultations for Nuclear Regulatory Commission (NRC) new nuclear reactor license applications prior to the NRC issuance of the license. DHS is responsible for conducting site security consultations in cooperation with the NRC, local law enforcement, and private sector partners to provide a report that identifies the potential vulnerabilities and threats associated with the proposed reactor locations. The NRC has informed DHS that there are 10 facilities that have submitted license requests and two pending license requests that will require site-security assessments in fiscal year 2010.

Additionally, IP will pilot six Regional Resiliency Assessment Projects, each of which will involve a cooperative Government-led, interagency assessment of both the specific CIKR and a general regional analysis of the surrounding infrastructure. The intent of this program is to identify and evaluate infrastructure "clusters," regions, systems, and their key interdependencies. The outcome of the findings will support the development of coordinated protection efforts to enhance resiliency and address security gaps within the surrounding first responder communities and geographic region. The program's integrated approach will measure and provide metrics for risk mitigation to a region.

Bombing Prevention

A total of $14.8 million is requested to support bombing prevention efforts. The fiscal year 2010 request supports the completion of 16 out of the 22 Implementation Plan recommendations included in the National Strategy for Combating Terrorist Use of Explosives in the United States that are the responsibility of DHS. DHS is working closely with both the Department of Justice and the Department of Defense, who are leading the completion of the other six Implementation Plan recommendations, to carry out this National Strategy. The funding will support increased assessments of bombing prevention capabilities across the country and increased bombing prevention information services for Federal, State, local, and private sectors.

Office of Risk Management and Analysis

The Office of Risk Management and Analysis (RMA) is leading the Department's efforts to establish a common risk management framework to identify, assess, and manage homeland security risk. RMA seeks to enhance overall protection, prevention, preparedness, and mitigation of homeland security risks through risk analysis and risk management strategies. RMA has:

- Completed the prototype for the Risk Assessment Process for Informed Decision-making (RAPID) to support the Department's overall planning, programming, budgeting, and execution process. When fully developed, RAPID will support strategic policy and budgetary decisions by assessing risk, evaluating risk reduction effects of DHS programs, and evaluating alternative resource allocation strategies. In 2009, within the RAPID framework, detailed assessments in the chemical and biological threat spectrum are being used to inform the Department's Integrated Planning Guidance by: (1) Providing an analysis of DHS chemical/biological security programs; (2) evaluating the degree to which DHS chemical/biological programs are contributing to risk reduction; (3) identifying gaps; and (4) recommending strategies for better allocating resources to manage risk.

- Completed the interim DHS Integrated Risk Management Framework. This framework provides a foundation for institutionalizing integrated risk management in the Department by outlining an overall vision—as well as objectives, principles, and a process—for integrated risk management within DHS. It also identifies how the Department will achieve integrated risk management by developing and maturing policy, governance, processes, training, and accountability methods. Members of the Department's Risk Steering Committee developed the framework, which is supported by all DHS components, directorates, and offices.
- Managed and led the administration and operation of a Department Risk Steering Committee, to serve as the Department's risk management governance structure. The Risk Steering Committee is a three-tiered construct. Tier I consists of all heads of DHS components; Tier II consists of sub-directorate/component principals (e.g., assistant secretaries, senior officials, deputy directors); and Tier III consists of senior policy and analysis staff. The Risk Steering Committee and its working groups meet frequently to review and produce risk products for use by the entire Department.
- Produced the first set of analytical guidelines for risk practitioners across the Department. The Risk Management Analytical Guidelines provide a body of knowledge for DHS and its components to improve their risk management capabilities by promoting sound risk management processes and techniques. These primers capture and promulgate promising practices and lessons learned to promote convergence of DHS risk management activities and support education and training. Among the initial titles are Developing Risk Assessment Methodologies, Developing Scenarios, Assessing Vulnerabilities for Risk Assessments, and Analyzing Consequences.
- Published the DHS Risk Lexicon, which defines 73 key risk-related terms and provides a common vocabulary for the foundation of an integrated risk management capability within the Department.

The fiscal year 2010 budget request for RMA is $9.9 million and includes 25 Federal staff. Major programs planned in fiscal year 2010 for RMA expand on recent accomplishments and include:

- Leading a study group under the auspices of the Quadrennial Homeland Security Review that will define, frame, and establish a process for conducting a homeland security national risk assessment for the purpose of determining comparative all-hazards risk to the homeland and identifying opportunities to manage that risk. Following the completion of the study, RMA will implement the recommendations and begin conducting the first homeland security national risk assessment.
- RAPID II, to be completed by February 2010, will be the first evaluation of the risk reduction effectiveness of DHS programs against a broader spectrum of homeland security risk; it will be used to help inform the Department's fiscal year 2012–2016 resource allocation process.
- Continue development of a Risk Knowledge Center. The Center will serve as the central point for risk data collection and dissemination, as well as provide training to enable the building of a risk core competency across DHS and the broader homeland security enterprise. The Center will also provide technical assistance to help personnel within DHS (and eventually outside DHS) develop and/or apply risk assessment and management concepts, methods, tools, and resulting data. Further, it will support the application of advanced risk concepts developed by a broad range of sources—DHS' Science and Technology Directorate, academia, professional societies, and RMA staff—to current and future needs.

United States Visitor and Immigrant Status Indicator Technology Program

The United States Visitor and Immigrant Status Indicator Technology (US–VISIT) Program assists the Department in facilitating legal travel and protecting our Nation from dangerous people attempting to enter the country. Recent US–VISIT accomplishments include:

- Deploying 10-print scanner technology to all major ports of entry. This provides the capability to capture 10 fingerprints from 97 percent of travelers. Utilizing

10-print capture improves accuracy in matching fingerprints, increases the identification of high-risk individuals, and reduces interaction with low-risk travelers. Full deployment to 292 air, sea, and land ports of entry will be completed by the end of this fiscal year.

- Assisted State and local law enforcement participation in Secure Communities. Secure Communities is an ICE initiative that provides assistance in the identification of immigration violators that have been arrested by State and local law enforcement. Authorized Federal, State, and local government user agencies are provided with access to biometric data to identify and mitigate security risks.
- Supporting the U.S. Coast Guard in the use of mobile biometric services (biometrics at sea) off the coasts of Puerto Rico and Florida. This aids in identifying and prosecuting hundreds of illegal migrants at sea, including some wanted for human smuggling and murder.
- Enhancing the integrity of the immigration system through continued development of alien exit reporting. US–VISIT began biometric air exit pilots on May 28, 2009. Through July 2, 2009, U.S. Customs and Border Protection and Transportation Security Administration will conduct tests in the boarding area of the Detroit Metropolitan Wayne County Airport and the security checkpoint of the Hartsfield-Jackson Atlanta International Airport collecting biometric information from non-U.S. citizens.

The fiscal year 2010 budget request for US–VISIT is $356.2 million and includes 212 Federal staff positions. The request includes funding to support the growing identity management and screening services workloads resulting from the increase to 10-print identifications and verifications. The request also includes increased system operations and maintenance for the Automated Biometric Identification System (due to continued growth of existing programs and servicing new customer program needs), technology refresh for fingerprint matching hardware, and data center mirroring and migration.

Office of Cybersecurity and Communications

The Office of Cybersecurity and Communications (CS&C) comprises the National Cyber Security Division, the National Communications System, and the Office of Emergency Communications. Recent CS&C accomplishments include:

- The National Cyber Security Division (NCSD) assessed over 4,000 current external internet connections in the *.gov* domain and identified approximately 80 of those as consolidated internet access points.
- NCSD began deployment of the National Cybersecurity Protection System (NCPS) to enable data collection for the detection of potential malicious cyber activities on Federal networks and consequent coordination and analysis by US–CERT (United States Computer Emergency Readiness Team).
- During Hurricane Ike, the National Communications System (NCS) helped leaders in the Houston and Galveston areas communicate by prioritizing emergency calls over congested phone lines and facilitating the restoration of critical telecommunications services. The Government Emergency Telecommunications Service completed over 93 percent of the 2,200 priority calls placed across five States.
- DHS developed the National Emergency Communications Plan and approved 56 State-wide Communications Interoperability Plans.

The CS&C fiscal year 2010 budget request is $584.9 million and includes 419 positions.

- The fiscal year 2010 request for the NCSD is $400.7 million.
  - This request includes an increase of $75 million from fiscal year 2009 for the implementation of the Comprehensive National Cybersecurity Initiative to support the ability to develop and deploy cyber technologies to counter on-going, real-world national cyber security threats and apply effective analysis and risk mitigation strategies to detect and deter threats. NCSD will support the on-going reduction and consolidation efforts of external Federal access points, enabling more effective monitoring and alerting on suspicious activities occurring across the Federal enterprise.
  - The NCSD request also includes an additional $15 million to enhance outreach and coordination across all levels of government and the private sector. The fiscal year 2010 budget request allows for additional support to the private sector by funding 50 site assessment visits to CIKR facilities, increasing the ability to identify vulnerabilities in Industrial Control Systems across the 18 CIKR sectors. The fiscal year 2010 request also enhances the capability for DHS to sponsor and support cyber exercises with State, local, regional, and private sector partners, as well as with our international partners. NCSD also plans to conduct Cross Sector Cyber Assessments to support enhanced

cybersecurity for all 18 CIKR sectors. This project will analyze cross sector perspectives and activities on common vulnerabilities, protective measures, interdependencies, risk assessment methodologies, and mitigation strategies.

- The fiscal year 2010 request for the NCS is $140.2 million; this will fund 10 new Regional Communications Coordinator positions and development of a Continuity Communications Architecture to ensure, under all conditions, Federal executive branch cross-department and agency communications.
- The fiscal year 2010 request for the OEC is $44 million and includes additional funding to support approximately 100 site visits that will validate progress against the NECP goals, provide additional support to lower-achieving urban areas, and fund State-wide Communication Interoperability Plan workshops.

Office of the Under Secretary

The fiscal year 2010 budget request includes $34.7 million and 104 Federal positions for Directorate Administration and the Office of the Under Secretary. Priorities for fiscal year 2010 include integrating the Federal Protective Service into NPPD, consolidating NPPD financial data and reporting, coordinating with DHS to continue to streamline the hiring and security clearance processes for new staff, and conducting strategic assessments for use in developing future capability needs to combat new and emerging threats against infrastructure, cyber networks, and biometric technologies.

CLOSING

I appreciate the opportunity to discuss NPPD accomplishments and plans for fiscal year 2010 and look forward to answering any questions you may have.

PREPARED STATEMENT OF GALE D. ROSSIDES

JUNE 10, 2009

Good afternoon Chairwoman Jackson Lee, Ranking Member Dent, and distinguished Members of the subcommittee. Thank you for the opportunity to appear today to provide an update on the President's fiscal year 2010 budget request for the Transportation Security Administration (TSA).

I would like to begin by thanking the subcommittee for its support of TSA's ongoing efforts to improve transportation security. Your support positioned us well for a successful Presidential transition. I also want to thank the subcommittee for supporting the resources provided to TSA in the American Recovery and Reinvestment Act of 2009 (ARRA). These resources are enhancing our Nation's explosives detection capabilities in airports throughout the country by significantly accelerating the deployment of more effective and efficient technologies.

ENSURING AN EFFECTIVE TRANSITION

The Department of Homeland Security (DHS) has worked hard to ensure that TSA, as well as other DHS components, was 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, 7 days a week, and 365 days a year. TSA personnel participated in important transition efforts, including joint exercises with our DHS colleagues and other Federal agencies to ensure we could effectively prevent and respond to a potential terrorist attack during this period. Designating the Deputy Administrator at TSA as a career position also helps ensure continuity, and I am honored to serve in this position and as the agency's Acting Administrator.

BUILDING ON OUR JOINT SUCCESS

I have 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.

Under the oversight of this committee, 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 transportation security partners both domestically and around the world. We began with the challenge of hiring, training, and placing the first Federal screeners, known as Transportation Security Officers (TSOs), in airports where they intercepted prohibited items such as guns, knives, and razor blades. Now, TSA employs a highly-trained, professional, multi-skilled TSO workforce that conducts physical and behavioral screening to counter constantly changing threats and operates state-of-the-art screening equipment throughout airports and across multiple modes of transportation.

CONSTANT VIGILANCE

Continuing TSA's success is as important today as it has ever been. For example, the threat level for commercial aviation remains high and terrorists continue to pose a threat to aviation. But the threats we face are broader than just aviation and terrorism. TSA is focused on the wide variety of threats, including natural disasters and health pandemics, that face all of our transportation hubs and infrastructure. We must remain vigilant and never lose focus of our mission.

IMPLEMENTING ARRA FUNDING

Before I address the fiscal year 2010 budget, I want to update you on our plans for deploying the $1 billion in funding provided by Congress to TSA in ARRA. Using a risk-based approach, TSA is purchasing and installing explosives detection systems (EDS) and equipment that will greatly accelerate the deployment of new technologies in airports across the country. These ARRA funds will not only improve security, but also will create jobs and strengthen our economy.

Approximately $700 million of ARRA funding will be allocated to the Electronic Baggage Screening Program, which includes the procurement and installation of airport baggage handling systems. TSA approved funding for 15 airports in ten States, including several small and medium-sized airports, for optimal baggage screening solution projects. Additionally, we recently announced the award of $47 million for the purchase of 123 reduced-size EDS to be deployed at airports throughout the Nation.

Approximately $300 million of ARRA funding is going to the Passenger Screening Program (PSP) to improve explosives detection capabilities in passenger screening. For the PSP, TSA plans to use ARRA funding for the purchase of Advanced Technology X-rays (AT X-ray), of which we announced an award of nearly $3 million for 44 AT X-rays, and additional Whole Body Imagers (WBI), Universal Conveyor systems, Bottled Liquid Scanners (BLS), and Next Gen Explosives Trace Detectors. The ARRA funding enables us to accelerate our projected schedules toward full system operating capacity, greatly enhancing checkpoint security for the traveling public.

Finally, 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.

FISCAL YEAR 2010 BUDGET REQUEST HIGHLIGHTS

The fiscal year 2010 budget will strengthen current efforts to secure all modes of transportation and allow critical investments in key programs. Specifically, the fiscal year 2010 budget provides TSA $7.8 billion, which reflects a total gross increase of $800 million for transportation security initiatives.

The fiscal year 2010 budget includes funding to support various activities and requirements, including;

- $856.6 million for the procurement and installation of EDS at airports;
- $128.7 million for checkpoint and checked baggage screening systems at airports;
- $108.1 million for air cargo security;
- $80 million for Visible Intermodal Prevention and Response (VIPR) teams, which includes an additional $50 million for new VIPR teams dedicated solely to surface transportation security.

The fiscal year 2010 budget also includes the annualization of $30 million received in fiscal year 2008 and $20 million received in fiscal year 2009 for such activities as Security Regulations, Strategies, Reports and Studies, Vulnerability and Threat Assessments; Name-Based Checks Infrastructure, Inter-modal Security Training and Exercise Program; Information Sharing and Analysis Center for transportation security; General Aviation; and additional Surface Transportation Security Inspectors (STSI).

I would like to highlight a few programs from the fiscal year 2010 budget.

Visible Intermodal Prevention and Response Teams.—The $50 million for 15 additional VIPR teams increases our random and surge force protection capability at transit hubs and other surface transportation venues. VIPR teams are capable of protecting any mode of transportation through risk-based targeted or unpredictable deployment of TSA assets in coordination with State, local, and Federal officials. VIPR teams consist of any combination of TSOs, Transportation Security Inspectors (TSIs), Federal Air Marshals (FAMs), Behavior Detection Officers (BDOs), Explosives Security Specialists, Bomb Appraisal Officers (BAOs), as well as local, State, and Federal security and law enforcement partners.

Bomb Appraisal Officers.—The fiscal year 2010 budget also adds 109 BAO positions by the end of fiscal year 2010 to strengthen security at domestic airports. BAOs are highly skilled individuals who have undergone specialized training in the identification and disposal of explosives. BAOs provide continual interaction and formal training to TSOs to increase their ability to recognize potential improvised explosive devices (IEDs) and IED components. BAOs also assist in clearing suspicious articles presented at checkpoints, often avoiding the need to call bomb squads, which can result in lengthy airport delays.

Infrastructure for Identity Vetting and Credentialing.—The fiscal year 2010 budget provides an additional $64 million to modernize the information technology infrastructure used to vet the identity of travelers and transportation workers. The funding will enable TSA to strengthen and enhance the existing infrastructure used to conduct vetting operations in several of our key security programs, such as Secure Flight, 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 (9/11 Act).

EDS Procurement and Installation.—In addition to the funding levels enacted for fiscal year 2009 and through ARRA, the fiscal year 2010 budget requests $565.4 million to further accelerate facility modifications, recapitalization efforts, and the deployment of new electronic baggage screening technology systems.

Whisper Communications.—The fiscal year 2010 budget includes $5 million for additional Land Mobile Radios (LMRs) at TSA screening checkpoints. The LMRs enhance communications between TSOs with significantly less disruption to the passenger screening process.

Passenger Security Fee.—To better align the costs of aviation security with the beneficiaries, the President has proposed 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 (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 60 percent of the expense of civil aviation security in fiscal year 2008. In the same year, Passenger Security Fee collections covered only about 31 percent of the discretionary costs for civil aviation security and air carriers covered the remaining 9 percent. Beginning in fiscal year 2012, the Fee would increase by $1.00 per year through fiscal year 2014. Under the proposal, the maximum fee in fiscal year 2014 and thereafter would be $5.50 per enplanement and $11.00 per one-way trip. 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 while simultaneously reducing the burden on the general taxpayer. The administration and TSA ask for your support of this proposal and we commit to work closely with Congress to obtain the necessary authorization to begin the fee adjustments in fiscal year 2012.

IMPLEMENTING OUR ON-GOING SECURITY STRATEGY

An effective security system must constantly adapt to ever-changing threats in the variety of transportation security environments in which TSA operates. Our transportation security strategy begins with intelligence, a key driver in our risk-based approach to security. Our daily operational decisions are influenced by the latest intelligence and the risks that emanate from the constantly evolving threats we face. As an example of our constant adaptation, we are in the process of upgrading security effectiveness at all of our aviation checkpoints, including the most significant overhaul in passenger screening since 9/11.

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 fiscal year 2009 voluntary attrition rate of full-time TSOs is 5.2 percent—an improvement of more than 58 percent since fiscal year 2006. The number of workplace injuries has fallen over 75 percent from fiscal year 2004 to fiscal year 2008 and continues to decrease. For the first 7 months of fiscal year 2009 there has been a 16 percent decrease in workplace injury claims filed compared to the first 7 months of fiscal year 2008.

Every TSO working at a checkpoint has completed an extensive 16-hour retraining called ENGAGE!, which provides the latest information on intelligence, explosives detection, and human factors affecting security. This training is designed to develop a cadre of analytical security professionals. Additionally, all supervisory personnel have completed a second 16-hour training course called COACH! to help reinforce the ENGAGE! training and provide additional guidance to TSOs. We have revised our checkpoint Standard Operating Procedures to enable officers to use their judgment appropriately in achieving sensible security results.

As part of TSA's improved security measures, we are deploying our workforce where we can achieve the best security results, most efficiently, and with minimal hassle for travelers. These improvements include the Travel Document Checker (TDC) and Screening Passengers by Observation Technique (SPOT) programs.

The 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 SPOT program. The SPOT program uses non-intrusive behavior observation and analysis techniques to identify potentially high-risk passengers based on their behavior. The program originated from other successful behavioral analysis programs that have been employed by law enforcement and security personnel both in the United States 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 Nation-wide elected by their peers who 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.

Process.—TSA is continuing to implement innovations in the checkpoint process. 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 to create a better security environment with improved technology and enhanced training for our TSOs.

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.

Technology.—With the support of this subcommittee, we are expediting 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, 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. TSA will continue to deploy in 2009 Bottled Liquid Scanners that are used to ensure sealed containers do not contain threat liquids. Additionally, TSA is purchasing and installing 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 is working with the Science & Technology Directorate and the National Laboratories to stay ahead of terrorist tradecraft.

UPDATE ON SIGNIFICANT ON-GOING PROGRAMS

Before I conclude, I also want to update the subcommittee on some of our most significant programs.

9/11 Act Implementation.—I want to thank the subcommittee for its on-going support of $20 million in fiscal year 2009 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. The remainder of the fiscal year 2009 funding for 9/11 Act implementation will be used for surface security measures, including the hiring of an additional 50 TSIs for surface transportation, 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 the industry is meeting the 50 percent screening requirement. 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 voluntarily throughout the supply chain to improve security while minimizing the potential negative impact on the integrity and movement of commerce.

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.

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 industry can meet the ambitious timetable set by Congress, we continue to work with our international partners and the private sector to address these 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. We have developed an international air cargo inspection program that expands our on-going foreign airport assessment regime to include a risk-based prioritization of sites and assets. This international regulatory activity work plan for air cargo will enable us to better determine areas of focus for inspection and assistance with our foreign partners. We look forward to working with this subcommittee on this issue as the August 2010 deadline approaches.

Secure Flight.—Beginning with the fiscal year 2005 DHS Appropriations Act, Congress provided TSA with very specific guidance in the form of ten conditions to meet 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 in meeting those conditions. As verified in GAO's report on the Secure Flight program published last month, TSA generally achieved nine of the ten conditions and conditionally achieved the one remaining condition. Your oversight and our partnership with GAO in meeting these conditions made Secure Flight a better program and it is now poised to effectively fulfill the mandate of comparing passenger information against watchlists.

Specifically, Secure Flight provides a consistent watch list matching process across all aircraft operators; provides for earlier law enforcement notification and coordination; and better protects watch list data thanks to its limited distribution. The Secure Flight program utilizes the Cleared List, a product of the DHS Transportation Redress Inquiry Program (DHS TRIP), to ensure that individuals who have been previously misidentified and have applied for redress are promptly cleared and do not experience similar problems in the future.

The Secure Flight program began implementation with certain aircraft operators on selected flights on January 27, 2009. To date, four aircraft operators have successfully begun cutover and numerous others have begun testing. TSA truly appreciates the cooperation and assistance these volunteer aircraft operators provided to the program during its initial rollout.

Secure Flight has also embarked upon an aggressive public outreach campaign in partnership with the aircraft operators and the Ad Council to educate passengers about how the Secure Flight program makes air travel safer and easier for millions of Americans.

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.

Transportation Worker Identification Credential (TWIC).—I am also pleased to update you on the progress of the TWIC program that we jointly administer with the United States Coast Guard (USCG). TSA continues to operate over 149 enrollment centers located throughout the United States and territories to serve the maritime workers who will require a TWIC. As of May 25, 2009, TSA completed enrollment of 1,208,412 workers and over 84 percent of workers who had enrolled have been issued their cards. The USCG completed the phased compliance of enforcement of TWIC in Captain of the Port (COTP) Zones Nation-wide by April 15, 2009. TSA and USCG closely monitored progress during the transition period to ensure smooth compliance at the COTP Zones. To further improve security and enhance enforcement efforts in COTP Zones, TSA completed initial capability evaluations of TWIC readers and approved 17 readers for use in the TWIC pilot program; additional readers are expected to undergo testing and be approved for use in the pilot. Early Operational Assessment of readers began in Brownsville, Texas, in April 2009 when the port completed final installation of readers and began operations of TWIC readers at their MTSA-regulated facilities. Other pilot participants are expected to follow Brownsville later this year.

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. Through collaboration and partnerships, TSA promotes the implementation of effective global transportation security processes world-wide while ensuring compliance with international and TSA standards. Focusing on closing gaps and providing enhanced capabilities, TSA seeks to manage risks and work with our international partners to harmonize security measures.

We accomplish this daily on many international fronts, multilaterally and bilaterally, through Transportation Security Administration Representatives in 23 countries overseas; a cadre of inspectors working with stakeholders and officials at airports, air carriers and Foreign Repair Stations; technical assistance programs; and standard-setting organizations such as the European Commission and the International Civil Aviation Organization (ICAO.) We promote best practices, capacity building and information-sharing through other international organizations such as the Group of Eight, the International Working Group on Land Transport Security, the European Community, the Asia-Pacific Economic Conference; and numerous ICAO regional groupings in Europe, Asia, Latin America, Africa, and the Middle East.

Another example of our global efforts is our Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS) relationship with foreign air security partners. OLE/FAMS conducts training for foreign air marshals to combat international terrorism. As demonstrated during the United Kingdom August 2006 plot to use liquid explosives to take down passenger aircraft bound for the United States, TSA worked with our international partners to respond immediately.

The Aviation Security Sustainable International Standards Team (ASSIST) initiative is already showing positive results. 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, which launched in January. In April, the Republic of Liberia became the second ASSIST partner country and just last month TSA completed an intensive 2-week training program on aviation passenger screening there. In the coming months we look forward to continuing this effort in other locations.

CONCLUSION

Madam Chairwoman, thank you and this subcommittee for the resources you have provided in the past to achieve significant enhancements in our people, processes, and technology. Thank you also for the opportunity to discuss the President's fiscal year 2010 budget request for TSA and our plans for continuing to improve transportation security. I look forward to working together. I would be pleased to respond to your questions.

Ms. JACKSON LEE. Because this hearing will be abbreviated due to the scheduling, the subcommittee requests that each witness meet with staff soon after this hearing concludes to go over additional questions. I would like to indicate that Members of the committee will have the opportunity to submit their questions, as well. At that point, Ranking Member Dent and I may ask that you meet with us, as well.

Today's hearing is an important part of the subcommittee's oversight of the Department of Homeland Security. Specifically, it provides us with the opportunity to assess, discuss, and analyze the President's budget request for fiscal year 2010.

I do thank the acting director, member of the Transportation Security Administration for the meetings that our committee has been able to have with her. So I thank you very much.

As you all know, this subcommittee has jurisdiction over TSA and many elements of NPPD.

With respect to TSA, we have already done a great deal this year. The TSA authorization bill was passed out of the House in an overwhelmingly bipartisan manner just last week. I again thank the Ranking Member, Mr. Dent, for being my original cosponsor on this legislation.

When it comes to infrastructure protection and the other elements of NPPD, the committee is moving quickly to extend and comprehensively modify the Chemical Facility Anti-Terrorism Standards. In addition, the subcommittee will be working on an authorization packet for NPPD later this year. Some of our Members have asked about paying more attention to general aviation. A number of new issues will be coming to our attention.

With respect to TSA, the subcommittee is generally pleased with the budget request of almost $7.8 billion. For fiscal year 2010, TSA has requested an additional budget authority for adding bomb appraisal offices, travel document checkers, and behavioral detection officers to enhance aviation security.

In addition to the standard checkpoint and baggage screening operations, TSOs will continue to support security initiatives, such as screening of passengers by observation techniques, visible intermodal prevention and response teams, and the Aviation Direct Access Screening Program. TSA has also made heightened investments in technology, precisely what we need to keep the traveling public safe.

I am concerned about TSA's fiscal year 2010 budget request of $108 million for cargo security operations. This figure does not support an increase in FTEs for air cargo and reflects a 12 percent decrease from the fiscal year 2009 enacted amount. Even as TSA faces significant challenges with respect to air cargo security, it is imperative that TSA has significant resources to face these challenges.

The President's fiscal year 2010 budget request for surface transportation security at TSA totals roughly $128 million, which is more than double the fiscal year 2009 enacted appropriation. Although I have concerns about how these new resources are allocated, this request reflects a real investment in securing non-aviation modes of transportation and is consistent with the broader priorities of our authorization bill.

Turning to NPPD, there is much to applaud in this budget proposal. This directorate has a troubled history, and this budget attempts to unify an entity that contains several disparate components.

In fact, let me be very clear: Sometimes it is not understood what the infrastructure protection aspect of our jurisdiction is. The only thing that I can say to you that makes it as real and as viable and important as I believe it is, and I believe my Ranking Member believes it is, is to recognize the overall responsibility of this committee, including infrastructure protection, takes into account aspects of cybersecurity, which we know is shared by our other subcommittee, but also it deals with the very incident that we have just pointed to that happened today. Infrastructure is everything in America, and we must be concerned about it.

The committee welcomes the $87 million increase over fiscal year 2009 appropriations for the National Cybersecurity Division. This addresses an important function. We are pleased that the Deputy Under Secretary, who has a career of success in the cyber environment, is willing to serve in order to help protect the Nation.

We still need to better understand how the Department's efforts will interface with the rest of the Federal Government, especially with the creation of a new cyber coordinator in the White House. Because this subcommittee works a great deal with the 18 critical infrastructure sectors, we must ensure that the Department's cyber efforts are efficiently leveraging these important relationships.

I applaud the Deputy Under Secretary for his testimony that filling vacant Federal positions and right-sizing the Federal and contractor staff ratio across NPPD is his utmost priority. This subcommittee fully supports this effort. But I am concerned about the suitability protocols of NPPD. This subcommittee stands ready to assist you in your efforts to expedite the security clearance process for prospective employees.

The subcommittee is pleased with NPPD's request for $333 million for infrastructure protection. As you well know, we have done a lot of work in this important area, and the response to the Mumbai attacks shows that we have a long way to go. The increases for chemical site security and the ammonium nitrate regulations are also important steps.

However, the subcommittee is concerned about the cuts to partnerships related to the National Infrastructure Protection Plan. In this economic climate, it seems that we should be bolstering these efforts as the private sector, an important security partner, will have fewer resources.

I remain very concerned with the Office of Risk Management and Analysis. Staff has quarterly briefings with RMA, and it seems both underfunded and headed in too many different directions. As I said last spring, we need a strategic plan from RMA that puts it on a path to success. I look forward to introducing legislation that will clarify the roles and responsibilities of RMA.

Finally, the President's 2010 budget request proposes to move FPS out of Immigration and Customs Enforcement and into NPPD. The committee agrees that ICE was not the proper entity to house FPS but questions whether moving it to NPPD will address the problems encountered under ICE. And we look forward to hearing your thoughts about the proposed move today.

I look forward to our discussion today, and I will work with you and am willing to work with you in order to support the vital mission of both TSA and NPPD. Once again, I thank the witnesses for their participation today.

Let me also acknowledge the presence of the gentleman from California, Mr. Lungren; the gentleman from Connecticut, Mr. Himes; and the gentleman from New Mexico, Mr. Luján; and thanks them for their presence here today.

The Chair now recognizes the gentleman from Pennsylvania, Mr. Dent, for an opening statement.

Mr. DENT. Thanks, Madam Chairwoman.

Good afternoon. I would like to thank both our witnesses for joining us today. I know your time is in short supply, so I will respect that.

We understand that there is an inordinate amount of time senior officials of the Department spend answering too many different congressional committees because of Congress's dysfunctional jurisdiction over the Department of Homeland Security. However, since the Committee on Homeland Security is the principal authorizing committee in the House, we very much appreciate you being with us today. So, that said, in light of some of the time constraints, I would like to keep my remarks short.

As you know, the House passed the TSA Authorization Act last week. The bill was negotiated on a bipartisan basis. I thank the Chairwoman for her leadership on that issue. Also, the committee met with many different stakeholder for input. I believe it was a good bill, and I was happy to be an original cosponsor of the legislation.

The Republican Members of committee, however, believe that it was premature to bring the bill to the floor for consideration before a new administrator was named for the TSA. As you know, TSA did not provide any formal input into the bill, and that is unfortunate.

One of the casualties of TSA not being able to provide input to the TSA Authorization Act was the misguided adoption of the amendment that would have severely restricted the use of whole-body imaging technology. The adopted amendment will prevent TSA from using whole-body imaging technology for primary screening purposes at the airport checkpoints.

As you know, the committee has been very supportive of WBI technology because we know that it enhances aviation security. We understand that WBI technology can detect many things, such as small IEDs, plastics explosives, ceramic knives, and other objects traditional metal detection cannot detect.

This technology was developed with the backing of Congress because we know our enemies are looking to use certain explosives which are not detectable with metal detectors or magnetometers. Restricting the use of WBI technology at the airport checkpoint will put us in a vulnerable position, just as we were prior to 9/11. We simply can't allow that to happen.

I should note that I saw the WBI technology for myself last week at Reagan National. I think it is a great technology, and I am very satisfied with the privacy measures currently in place. I know you have taken a great deal of care to ensure that. I think there is a lot of inaccurate information out in the public domain, and many Members are misinformed on the technology.

As the TSA Authorization Act makes its way through the legislative process, it is my sincere hope, and for the sake of all Americans who fly, that TSA will weigh in and inform Congress on the advantages of WBI technology so we can ensure the use of this innovative and very necessary technology at our Nation's airport. My colleague, Mr. Lungren, was very eloquent on this issue. I wish more Members could have heard his comments on that amendment.

Moving to the National Protection and Programs Directorate, I am very glad to see that the administration is making cybersecurity a priority. I am encouraged by the increased funding request of $75 million over fiscal year 2009 to support the implementation of the Comprehensive National Cyber Security Initiative.

Mr. Reitinger, I understand you have an exemplary background in cybersecurity, and I look forward to the work you will do at the National Protection and Programs Directorate.

Thanks again for both of you being here today.

I will yield back the balance of my time.

Ms. JACKSON LEE. Let me thank the gentleman for his testimony.

I welcome our witnesses.

Our first witness is Philip R. Reitinger, who was appointed by Secretary Janet Napolitano to serve as a Deputy Under Secretary for NPPD on March 11, 2009. In this role, Reitinger leads the Department's integrated efforts to reduce risk across physical and cyber infrastructures.

Prior to joining DHS, Mr.—let me just ask, how do you pronounce your name?

Mr. REITINGER. Yes, ma'am, it is "Reitinger."

Ms. JACKSON LEE. It is "Reitinger." I just want to make sure. Thank you.

Prior to joining DHS—I wanted to make sure that we were not getting that smile because—you are just a smiling person.

Mr. REITINGER. Yes, ma'am.

Ms. JACKSON LEE. Thank you very much.

Mr. Reitinger was the chief trustworthy infrastructure strategist at Microsoft Corporation. I would suggest to you that you come widely applauded, because in his title of his previous position had the term "trustworthy". Is that correct?

Mr. REITINGER. Yes, ma'am, it is.

Ms. JACKSON LEE. I couldn't imagine that the Secretary could find a better selection. Thank you.

In that role, he worked with Government agencies and private-sector partners to enhance cybersecurity and infrastructure protection.

Our second witness, Ms. Rossides, is acting administrator of TSA. As acting administrator, Ms. Rossides oversees a workforce of 50,000 and the security operations of 450 Federalized airports throughout the United States, as well as the Federal security regime for highways, railroads, ports, and mass transit systems. Ms. Rossides was one of the six original Federal executives handpicked in 2002 to build TSA. We are certainly appreciative of your leadership on that issue.

As agreed to at the beginning of today's hearing, the witnesses' testimony will be considered as read so that we can begin to question our witnesses in the interest of time.

I will remind each Member that he or she will have 5 minutes to question the panel.

I will now recognize the Ranking Member for 5 minutes, Mr. Dent.

Mr. DENT. Thank you, Madam Chairwoman.

Just by way of commentary, I learned a long time ago—my middle name is W-I-E-D-E-R. My mother taught me, as a young person from Pennsylvania Dutch country, I-E is "E," E-I is "I." Mr. "Reitinger," there are a lot of names like that in my area.

But just a couple things, Mr. Reitinger. Is the Department aware that the Committee on Homeland Security and the Committee on Energy and Commerce are crafting legislation to authorize the Department's regulatory authority over chemical facilities?

Mr. REITINGER. Yes, sir.

Mr. DENT. Then, the Department did request a 1-year extension for the current CFATS regulations. Why did you do that knowing that the committees are engaged in legislation?

Mr. REITINGER. Thank you, sir. Let me first, before answering that question, thank the committee for the opportunity to testify today and for the kind words that both you and the Chairwoman said about me and about NPPD and the criticality of our mission.

To answer your question in particular, sir, the Department requested a 1-year extension of CFATS in the budget because we believe that 1 year would give us the time to work effectively with Congress for a permanent reauthorization of CFATS.

The Department supports the permanent reauthorization of CFATS, and a year seemed to be a reasonable amount of time to enable that discussion to take place and an action to be taken by Congress.

Mr. DENT. Do you believe that the current CFATS regulations are sufficient?

Mr. REITINGER. I believe the current CFATS regulations give us a good basis for going forward, sir.

As the Ranking Member knows, we are currently in the process of implementing the regulations, in tiering assets, and in executing the site security plans that are called for under the regulation. That activity will give us a lot of additional experience about the effectiveness of the regime, if there are holes in it.

So, while I am comfortable with the regime as it is, I believe we will have additional opportunities to learn about opportunities for improvement going forward. I look forward to working with the committee and staff on the most effective design for that program.

Mr. DENT. I have introduced legislation to extend the current CFATS regulations by 3 years. So thank you for that comment.

One of the issues Congress is grappling with is whether or not to require facilities to re-engineer their plants to use different and perhaps less dangerous chemicals in their manufacturing processes. Alternatively, plants could shift from on-site storage model to a just-in-time delivery model. A popular catchy phrase for this is called "inherently safer technologies," or IST.

If IST reviews were mandatory, how many Government employees who are professional IST experts capable of analyzing each of these facility processes does the Department have on staff? Any idea?

Mr. REITINGER. Well, sir, in terms of specific IST experts, I am not aware that we have any. We, of course, are in the process of hiring and training chemical experts, chemical inspectors, who would develop certainly expertise that would be applicable to that sort of activity, if not completely aligned with it.

One of the things I would say is that there is nothing about the current statutory regime, however, that forbids the use of what amounts to IST technologies, choosing to use different chemicals, choosing to use different technologies, in order to tier down or comply with the existing regime.

So the current regime allows use of those, it just doesn't mandate their analysis or use.

Mr. DENT. Does the Department's fiscal year 2010 budget request include any investment in IST expertise?

Mr. REITINGER. Not specifically, sir. It does, however, include authorizations to hire up to 139 CFATS inspectors, with an additional 20 ammonium nitrate inspectors who could be cross-trained, or with the upcoming addition of 40 chemical inspectors who could be cross-trained to do CFATS inspections.

Mr. DENT. Ms. Rossides, as you know, during the last week's authorization, TSA's authorization bill, the House adopted the amendment offered by Mr. Chaffetz and Ms. Shea-Porter, which would prohibit the use of whole-body imaging in primary screening positions. Of course, I opposed this amendment very strongly, as did Mr. Lungren.

As you know, I went to Reagan National last week and saw this technology first-hand. I was, as I mentioned, really very impressed by it. I saw an individual walk through a checkpoint with two weapons, and, without giving any detail, let's just say I was unnerved by the magnetometer's inability to detect them. However, the whole-body imaging showed both concealed weapons pretty easily.

Could you explain the Department's current privacy safeguards in place that govern the use of this technology? What would be the practical implications if the prohibition of using whole-body imaging technology for primary screening were to become law? You know, what capabilities would be lost?

Ms. ROSSIDES. Yes, sir.

First of all, with respect to the privacy issues, TSA took really great measures to protect the privacy concerns. We have a privacy impact assessment study that was published that reflects those measures.

But, very specifically, first of all, the passengers have a choice as to whether or not they go through the WBI or the walk-through metal detectors.

Second, the images that are viewed are viewed in a remote location, so that the officer that is viewing the image never sees the passenger and the officer that is assisting the passenger never sees the image. The face is blurred.

There is signage in the checkpoint advising the passengers of their options and what the image actually looks like. The technology itself does not store, it does not print, it does not transmit nor save the image. Once the image is deleted, it cannot be retrieved.

These are the measures that we have put in place. In the places where we have the technology, we have over a 95 percent satisfaction rate with the traveling public.

In all honesty, sir, based on the intel that I and the leadership team at TSA sees every single day, if we do not have the ability to deploy this technology and utilize it to the best of the abilities for the system, it will represent a severe limitation of our detection capability.

We know that those who intend to do harm today have moved way beyond metal items. They are, in fact, looking for things that they can conceal. They are looking for things that the walk-through metal detector cannot detect, and the whole-body imaging technology can.

Mr. DENT. Well, thank you. I hope somebody in the media is writing that down and they publish that tomorrow. It is a very good statement. I appreciate that.

Finally, on the LASP program, as you know, I have some real concerns about the proposed rulemaking. I noted that, with some comfort, the Department has recently conducted a couple of workshops of various stakeholder groups, and will soon hold a third, to consider future proposed rulemaking.

How is this process that you are conducting different than the process used to develop the initial rulemaking, which has given a lot of us, on a bipartisan basis, some real heartburn?

Ms. ROSSIDES. Well, sir, the initial rulemaking that we sent out, we actually did something that was rather unconventional with our regular rulemaking process in that we did have five public meetings on the initial rulemaking.

But after the extensive comments—and I believe we got over 6,000 comments from the public in general—we have held a series of meetings with major trade associations and other stakeholders. We held the first meeting in April, the second in May, and we have the third meeting scheduled for June 15. What we are looking at is those areas of concern by the external stakeholders and associations.

Once we have these meetings, we will look to see where the interests of those persons are and the TSA concerns and security interests are. Then we will go out with—we will reopen the notice of proposed rule making for a second round of comments.

I am hoping, and from the feedback we are getting from the associations, that is a positive step in the right direction, in terms of coming to agreement on how we close some of the security vulnerabilities we are concerned with and meet their concerns, as well.

Mr. DENT. I just think a lot of the Members here would be appreciative if the stakeholder input was not summarily dismissed.

Ms. ROSSIDES. It won't be.

Mr. DENT. Thank you.

I will yield back.

Ms. JACKSON LEE. Thank you.

Let me ask Mr. Reitinger again, how close to the 3 o'clock hour can you stay?

Mr. REITINGER. Thank you, Chairwoman. I have a speaking engagement at the Chamber of Commerce, where I know one of your Members is going later. I was supposed to leave at 2:45, but I will push it, as we need to, to respond to the committee.

Ms. JACKSON LEE. Well, let me do this. My questions are only going to be to you. I hope, if you give quick answers, I might be able to get Mr. Lungren in and Mr. Himes before you leave.

If I could ask Members to only question—we will be able to come back around for Ms. Rossides. If that can work for your questioning, it would be helpful, since he has an opportunity to leave.

Let me quickly ask the question about the NPPD. There have been a lot of discussions about the permanence of NPPD. As we all know, it is a disparate collection of entities that, in some cases, do not appear to a unifying focus beyond being security programs.

With that said, does this budget set the stage for the reorganization of the NPPD before or after the delivery of the Quadrennial Homeland Security Review next winter, Mr. Reitinger?

Mr. REITINGER. No, ma'am, it does not. The budget, in fact, is designed to help drive unity of NPPD by building an effective front office that will enable the organizations to move effectively and work together on its joint mission of mitigating threats to the homeland.

Ms. JACKSON LEE. Are you saying that you don't intend to begin to look at reorganization at this time or before the delivery of the Quadrennial Homeland Security Review, or are you going to do it after? What is the time frame for reorganization? What is the interest in reorganization?

Mr. REITINGER. Well, ma'am, an ultimate decision about reorganization I would leave to the Under Secretary, once confirmed by the Senate.

I believe we have a good basis going forward with NPPD. There are no current plans to reorganize NPPD, other than to move IGP up as a direct report to the Secretary. We intend to move forward effectively. As experience tells us whether the organization of NPPD is optimal, we would come back and work with the committee to make sure that could be done as effectively as possible and with minimal disruption to business.

Ms. JACKSON LEE. Well, let me just hope that you will convey to your leadership there that we are interested in seeing a plan for reorganization or at least some argument that it shouldn't be reorganized.

The subcommittee is concerned with the level of personnel NPPD employs. I am happy to learn from your testimony that many you brought on 300 new employees over the last 12 months and currently have approximately 800 Federal employees on board out of 1,064.

For that reason, I was pleased to learn from your budget request that you intend to bring on additional personnel. Could you describe NPPD's efforts to employ additional personnel, how this will affect current contracts at the Department?

Mr. REITINGER. Yes, ma'am. As you indicated in your opening statement, Madam Chairwoman, my No. 1 priority is bringing the right people on board. It is my personal belief that organizations succeed or fail based on the people that they have. Therefore, that takes the majority—of my time, I spend the biggest chunk of it working to make sure that we have effective processes in place to bring on the right people as rapidly as possible to supplement the excellent staff we already have.

To that end, we have aggressive hiring plans for the remainder of the fiscal year, and we will be bringing on additional people next year.

As my testimony also indicates, we are making efforts to, as you said, correctly right-size the contractor workforce so that we build up our Government personnel capabilities, create expertise in Government, and use contractors appropriately for the roles for which they are best suited, which includes scaling to meet needs and for getting particular expertise that is readily not available in the Government workforce.

That will, I think for the foreseeable future, remain my No. 1 priority, because I believe if we can do that effectively, everything else will come with it.

Ms. JACKSON LEE. I would like you to make yourself available for briefing for Members who may be interested and myself—I happen to be interested—on the progress of that effort and how you are approaching it, particularly since it relates to utilizing or non-utilizing of contractors. So if you could make note of that, I would appreciate it.

Mr. REITINGER. I would be happy to, ma'am.

Ms. JACKSON LEE. On the RMA, you heard my comments earlier. They have been meeting with our staff. We know that they have an ambitious agenda, ranging from a national risk assessment to the informing of budget cycles to a heavy presence working with the Quadrennial Homeland Security Review.

So how, then, is approximately $9 million enough for fiscal year 2010 for this particular subset? Staff was told last week that 19 of the 26 FTEs are filled; that means that you have seven that are not. How quickly can you get to full capacity, given the major hiring that you are trying to do within NPPD?

Mr. REITINGER. Well, ma'am, I believe that the budget request is reflective of what we believe we need to start to drive success with RMA; and, in particular, to have it lead the risk management study group within the Quadrennial Homeland Security Review.

I think, going forward, this and other areas will get additional knowledge about the scope of requirements and could come back to the committee or find the resources within DHS and reallocate personnel, if necessary, to accomplish the mission.

In terms of hiring, I believe that the number that you stated refers to—my recollection is we have 13 Government personnel onboard in FTE, with six offers outstanding, and 10 contractor personnel on-board. That is my current understanding. So we will be to be the number you said very soon. We are focusing just as much on RMA hiring as we are on hiring for other components. So we will bring on the additional FTEs as rapidly as possible to make sure that we can effectively execute the mission.

Ms. JACKSON LEE. Let me suggest that I appreciate the answer that you had to give. This should be an on-going review by those of us who are concerned that any cuts in the budget, when we are trying to build and ensure that the Department does have the staff, is of concern to us.

It follows that my next question about the $11 million cut from IP's national infrastructure protection program efforts, we are curious as to the rationale behind those cuts, particularly since we know the private sector are not regulated for security purposes. Many do not have the financial resources in this economic climate.

So I would appreciate it if you would explain whether other departments and agencies which partner with DHS under the NIPP will be providing resources to counter and to complement the losses of $11 million and to further security efforts under the NIPP and fiscal year 2010.

I think one of our biggest Achilles heels are the private sector, although they are aware of the responsibilities of securing their facilities, the question is, do we have it at a level that suggests that they are doing everything they can do? We are now cutting in this area.

Mr. REITINGER. Yes, ma'am. Let me answer that in several different ways, if I could. I will try to be as brief as possible.

First, it is not our intention to not do anything we were going to do with the cut of $11 million. We might simply have to push out particular products that we were designed from fiscal year 2010 to perhaps fiscal year 2011.

We are also going to have to rely on a more, as your question indicates, a more distributed model for resourcing the partnership. That seems, to me, appropriate because it is, in fact, a distributed process involving not just the Department of Homeland Security but multiple Federal agencies and literally thousands upon thousands of private-sector entities. We are going to need to rely more on them to help drive the NIPP partnership. I will be working personally and avidly to make sure other Federal agencies do their part in that process.

In addition, with regard to the private sector, as your question points out, it is a more difficult time for the private sector to devote things such as working to partnership with the Department of Homeland Security.

That said, I spent the last 6 years in the private sector, and I can personally testify to the fact that large portions of the private sector are deeply committed to the security of the United States and I believe, with the right partnership, with the right opportunities, are willing to go to even greater lengths to work with U.S.

Government, and DHS in particular, to more effectively secure the homeland.

Ms. JACKSON LEE. I thank the gentleman.

With that, I will end my questioning and yield to Mr. Lungren. I will reserve my questions for you, Ms. Rossides. Thank you.

Mr. Lungren.

Mr. LUNGREN. Thank you very much, Madam Chairwoman.

Mr. Reitinger, in the President's budget I think there is $19 million for the implementation or enforcement of the chemical security regulations. Can you give us an update on where we are in terms of the implementation of the chemical security regs?

Mr. REITINGER. Yes, sir. The most recent action—as I am sure you know, the original notice of rulemaking was published back in 2008, and initial tiering determinations were made. This is also reflected in my testimony.

Most recently, back in May, the tiering of the entities regulated under CFATS, the initial letters went out to those regulated under tier 1, the highest level. So, those have been notified of their need to develop a site security plan. So that effort is on-going. Further communications to the lower tiers will take place over the remainder of the year.

Mr. LUNGREN. The authority to regulate the chemical security expires in October of this year because of how we had to fashion legislation in the past. How long does the Department need to complete and review all the vulnerability assessments, the site security plans and site visits to the covered facilities?

Mr. REITINGER. Yes, sir, we believe that will be an on-going activity and would support reauthorization of CFATS. That is the reason that we ask for, in the budget request, the 1-year reauthorization, so we could discuss with Congress a permanent reauthorization of the CFATS regulatory regime.

Mr. LUNGREN. I want to stress that, because, you know, there is a lot of talk here on the Hill that we didn't do enough or we have to change it and so forth. You got the industry to buy into it. You had a cooperative effort with the industry to come up with regulations that, it appears to me, can actually work. I am worried about us starting the whole process again, not that we can't improve the process, but starting it again and losing all the good work that we had in the past.

Do you share that concern?

Mr. REITINGER. I certainly would not like to start again from scratch. We have made a lot of headway. We have done some extensive hiring. We are bringing the right expertise on board to be able to execute the regime. Zeroing out that program and restarting would be costly and inefficient.

Mr. LUNGREN. The budget request has $19 million in there to complete the ammonium nitrate regulations that were mandated some years ago. Can you give us the status of the regulations, when you expect those will be completed?

Mr. REITINGER. Yes, sir, I can. The advanced notice of proposed rulemaking came out last year, and comments were received. Based on those comments, which came in through December of last year, a task force was established by DHS in January of this year.

That body has been reviewing the comments, contacting internal and external stakeholders, and is working on developing an actual notice of proposed rulemaking that should be released some time in the fall, after review by OMB. The ultimate effective date of such a regulation will depend on a number of factors after that.

Mr. LUNGREN. Sure, I understand that. But I hope that you understand that we, in the Congress, are very concerned about the ammonium nitrate. It does appear to be a substance that is a favored substance used by terrorists. This Congress was concerned, with some sense of urgency, that do have regulations, so I hope that they will be completed sooner rather than later.

The committee will be considering chemical facilities security legislation next week. We have the issue of inherently safer technology, or IST. There is some issue—again, this goes back to the question about whether we start almost from scratch or revamping it again. Can you give us your thoughts on IST and its reasonable application to regulations?

Mr. REITINGER. Of course, sir. I will be brief on this subject, because, as you indicate, sir, there is a hearing next week specifically on the topic.

There is nothing in the current regime that prohibits a covered entity from implementing the use of inherently safer technologies to tier down or to comply with the existing regime. So the existing regime has the flexibility to allow regulated entities to use those sorts of technologies. It does not, however, mandate them.

I, and NPPD generally, would be happy to work with the committee going forward to make sure that any permanent reauthorization of CFATS or other statutory amendments most effectively allow meeting critical national needs around protecting chemical facilities and, at the same time, preserve the greatest degree of flexibility around risk-based performance so that covered entities can comply most effectively with the Federal requirements.

Mr. LUNGREN. I thank you. I appreciate that response.

I will return any time I might have.

Ms. JACKSON LEE. Let me thank you.

Before I just may be able to yield a minute or 2 to the next speaker, looking at the clock, Mr. Reitinger, I just want to make mention of the fact that our chemical legislation we have been working on for a very long time, so it would not be starting from scratch.

If we got momentum and saw this thing really formulating, would you welcome it getting done within the year?

Mr. REITINGER. I would welcome a reauthorization, a permanent reauthorization, as rapidly as possible of the CFATS regime, yes, ma'am.

Ms. JACKSON LEE. Thank you.

Mr. Himes, we have you for a moment.

Mr. HIMES. One minute, one question, Madam Chairwoman.

Mr. Reitinger, I am interested in the topic of cybersecurity, in particular. I have listened to people at DOD and elsewhere who are concerned with this issue make statements indicating they understand the threat. In all candor, it also seems like people are just now beginning to really think how to address that threat.

So my question is, looking at your budget request and also aware of the fact that the White House has developed this concept of naming a cyber coordinator, can you address how you are thinking about this, how you are coordinating this in an integrated fashion with DOD and other interested agencies and departments, and how you might relate to the White House cyber coordinator, and how your budget proposal reflects that possible integration?

Mr. REITINGER. Yes, sir, I can. We have a very strong interagency coordination process under the White House through interagency policy committees. They meet regularly to make sure that all of the agencies are moving forward jointly to address the issue.

In that vein, I would greatly welcome the appointment of a cyber coordinator in the White House, because it is my opinion, as the President indicated as the outcome of the 60-day review, that this is an issue of such national importance that we need White House leadership. We need White House leadership to continue to bring all of the agencies together as effectively as possible.

I pledge to you and the committee that DHS will be a part of that and will work effectively, not only with the White House but with all of our agency partners from DOD, through the Department of Commerce, the Federal Bureau of Investigation, and many others, to make sure we are effectively addressing the issues.

I believe our budget proposal reflects the increasing seriousness of the issue. As the Chairwoman noted, we are devoting substantial additional dollars to help do our part in DHS to help provide for cybersecurity both within the Federal Government and in the private sector.

Mr. HIMES. Thank you.

I yield.

Ms. JACKSON LEE. Thank you.

Mr. Luján is next.

Mr. Massa, did you have a question? Because you would have to ask Mr. Luján to yield.

Mr. MASSA. No, Madam Chairwoman. I will wait until we go around our first round.

Ms. JACKSON LEE. All right. Thank you.

I think he is ending his time. Mr. Luján, did you have a second of any comment?

Mr. LUJÁN. Well, Madam Chair, maybe not necessarily anything that the Under Secretary would have to respond to. I could probably make my point as the Under Secretary is packing up, so best to utilize his time. I know he has an important speaking engagement.

But, you know, the issue that we would have to visit about our report as well. But I would yield back to the Chairwoman and allow him to maybe be excused, and I could make my point as he is packing up.

Ms. JACKSON LEE. Well, I am yielding to you, Mr. Luján. You are ready to make your point.

Mr. LUJÁN. Okay. With that, Madam Chairwoman, thank you very much.

The one thing, to carry on what Mr. Himes was discussing pertaining to cybersecurity, is again that we have an invaluable asset in some of our NNSA laboratories, both Lawrence Livermore, Los

Alamos, and Sandia National Laboratories, of which they already process real-world experience, technology, Government, and private-sector interface to be able to be an immediate asset to these efforts and to this program.

I would hope that, as we look at DHS in conjunction with what the President's efforts are in this area, that we look to the NNSA laboratories for their expertise and to fully utilize their experience with the data sets that have been compiled, as well as other security measures that can be taken.

I yield back, Madam Chair. My other questions I can reserve until later on. Thank you.

Mr. REITINGER. Let me again offer my apologies that I need to leave and my thanks to the committee for understanding that I had a prior commitment and my commitment to come back and meet with you and/or staff at your convenience to address any additional questions that you have.

I would, in response to the last Member's point, say that I agree completely that this is a national problem and we need to bring all national capabilities to bear to address it. So I look forward to working with the committee and all elements of the Government to make that happen as effectively as possible.

Ms. JACKSON LEE. We are understanding of that. As you are putting your papers together, I don't want to—Mr. Cleaver, did you have a point you wanted to get on the record as he is packing up?

Let me suggest to the Members what I said earlier, that any additional questions we will provide in writing. Mr. Reitinger, you indicated that you would be willing or accepting the fact of sitting down with staff after this particular meeting to go over any additional points.

Mr. REITINGER. Yes, ma'am.

Ms. JACKSON LEE. Thank you very much.

We are somewhat out of order here, but let me find out, Mr. Luján, did you finish?

Mr. LUJÁN. Madam Chairwoman, I would yield back so we can go to the second round of questions.

Ms. JACKSON LEE. All right. So then I am going to go to Mr. Cleaver. The witness that you have before you is the acting administrator for TSA.

Mr. CLEAVER. I am concerned about—and I apologize if this issue has already surfaced. But the TSA has this mandate by 2010 to do 100 percent screening. Based on what happened with this existing budget, I am wondering if it is still realistic to have a 100 percent screening by 2010 if we are going to begin to cut back in the current budget?

Ms. ROSSIDES. You are speaking about the air cargo budget?

Mr. CLEAVER. Yes.

Ms. ROSSIDES. Yes, sir. First of all, let me explain the reduction, which is a reduction of $18 million that was in the 2009 budget that was for pilots of utilizing technology. Those dollars went out to various partners that were testing the technology. So, in essence, that was a one-time investment that was made in 2009. So, in essence, the budget is a flat budget, you know, the same investment in terms of the program dollars from 2009 to 2010.

With respect to the screening and the mandate for the 100 percent screening for both domestic and international by August 2010, we are absolutely certain that, on the domestic side, we will meet that mandate.

We do believe that it is going to be a significant challenge to meet the international mandate by August 2010. Because, in essence, you have 98 countries that are importing to the United States via air cargo, and it is going to be a challenge to get all of those in compliance by the August 2010 deadline.

Honestly, sir, that is not necessarily a function of the dollars that TSA has, but it is the limitations we have with some of those foreign governments in getting them to comply with that mandate.

Mr. CLEAVER. So you do believe that, with the existing revenue funding stream, that domestically, at least, you will be able to meet the deadline?

Ms. ROSSIDES. Yes, sir.

Mr. CLEAVER. Now, then what needs to be—there is nothing that needs to be done congressionally to deal with the international?

Ms. ROSSIDES. No, sir. What we are doing is we are visiting these countries, we are giving them our standards. We are assisting them with teams of TSA experts that are going there and assisting them to try to get their supply chains to meet the U.S. standards.

It is not that we are not going to get quite far towards that 100 percent; we are estimating today that we will get about 80 to 85 percent of the way. But there will be some countries where it is going to be difficult to get to that August 2010 date.

Mr. CLEAVER. Where are we now? What percentage——

Ms. ROSSIDES. We are over 50 percent, both domestically and internationally, as of today.

Mr. CLEAVER. You have no reservations whatsoever——

Ms. ROSSIDES. For the domestic side, yes, sir.

Mr. CLEAVER. But your projection is perhaps under 90 percent.

Ms. ROSSIDES. For the international, that is right.

Mr. CLEAVER. Madam Chairwoman, one other question that is related to this, because I am concerned that when the budget shows a reduction—and I am not sure how it can be addressed—but when the budget shows a reduction like this—and I don't want you to make up stuff and pad it—you wouldn't do it anyway. But, you know, it does create some concern, and I am not sure how to address it.

Are you familiar with H.R. 2200?

Ms. ROSSIDES. Uh-huh.

Mr. CLEAVER. Was the congressional action taken in that legislation helpful in addressing this issue?

Ms. ROSSIDES. Yes, sir, in a way, it does——

Mr. CLEAVER. Internationally.

Ms. ROSSIDES. It extends the time frame, but that legislation actually does not change the mandate that we have under the 9/11 Act, which is for the August 2010 deadline. That legislation is still in effect, and that is the target date we are working towards. That is the date we are working towards with our international partners, the August 2010 date.

Mr. CLEAVER. All right.

Thank you, Madam Chairwoman.

Ms. JACKSON LEE. I thank the gentleman from Missouri.

That last point that you made, could you restate it and clarify it for me, please?

Ms. ROSSIDES. Yes, ma'am. It is my understanding that, although the provision to provide for the 2 years from the date of the enactment of the TSA reauthorization bill recognizes—this is what the counsel is advising me—that the mandate under the 9/11 Act to meet the August 2010 date doesn't change. Now, I may be incorrect on that, but that is my understanding, that we still have an August 2010 mandate under the 9/11 Act.

Ms. JACKSON LEE. That is for domestic?

Ms. ROSSIDES. I believe it is both domestic and international.

Ms. JACKSON LEE. We will pursue that further.

Let me recognize Mr. Massa for 5 minutes.

Mr. MASSA. Thank you, Madam Chairwoman.

Thank you, Secretary, for being here today. I would like to return to one topic with a follow-on question.

You very adroitly answered a question about whole-body imaging. Paraphrasing what you said, I believe the word was "critical" for the security of the agency to fulfill its mission.

Ms. ROSSIDES. Yes, sir.

Mr. MASSA. Am I understanding your opinion of that process correctly?

Ms. ROSSIDES. Yes.

Mr. MASSA. You also stated that passengers in all cases would participate voluntarily.

Ms. ROSSIDES. Right.

Mr. MASSA. Can you help me understand how a voluntary program could therefore be critical to the security of the on-going operations, since there is no way to screen or determine who is going to be participating since they self-select?

Ms. ROSSIDES. No, sir, the way the system is designed is the passenger would be given the option to go through the whole-body imaging technology. If they pass through that technology, then that technology is so superb at detecting anything on the body that it will not require us do an officer do a pat-down.

Mr. MASSA. No, I understand that. Although I would never want to inflict anyone on my participation in this program, my point here is, you may the statement that the deployment of this technology is critical to the overall improvements in the security of TSA.

Ms. ROSSIDES. Yes, sir.

Mr. MASSA. But you also outlined and have now confirmed that participation by passengers is voluntary. That, to me, is a fundamental disconnect in logic.

If I say that we have to do that to this group to increase security and then I say to this group it is voluntary to participate and no one opts in, how could that technology thereby be considered to be crucial to the increase in security of the group?

Ms. ROSSIDES. Well, sir, it is because the majority of the passengers are opting in, No. 1. No. 2, in order to do what we have to do every day, we have to be able to deploy as many tools as possible to help us in the screening process.

Mr. MASSA. Is it a question of speed?

Ms. ROSSIDES. It is a very effective process to screen people very quickly. It is much quicker to go through the whole-body imaging than it is to do a pat-down. So one is a passenger throughput, but the primary goal is the ability to detect without ever having to touch the passenger.

Mr. MASSA. So a second point I would like to ask, if you could just give me a few moments on this, it is my understand—and I apologize that I arrived late; it may have been addressed before my arrival—that we are preparing to fulfill a requirement to increase security in corporate aviation.

That brings the presence of air marshals, the screening of passengers, and the handling of corporate, in fact all private aircraft over a certain weight limit, to the standards that we have come to be familiar with as the general public, myself included, flies.

Is that program continuing, as had been previously briefed?

Ms. ROSSIDES. It is subject to continuous discussions currently with the stakeholders. We are going to go out with a second round of proposed comments and a second round of a notice of proposed rulemaking. The goal is to listen to and address the concerns that the stakeholders have, but also to close the gap in what we see as some security vulnerabilities with the general aviation population.

Mr. MASSA. Is part of that enhanced security in corporate aviation entailed in the embarkation of air marshals on those aircraft?

Ms. ROSSIDES. It is one of the elements. Whether that ultimately ends up in the final decision, you know, that is to be determined. But it was one of the elements, to know, to have a law enforcement security official on board.

Mr. MASSA. So one of the concerns I have with this potential mandate is, where will these people come from? It is my understanding—and I apologize, I am just a country guy from upstate New York—but it is my understanding, from the reading of the information I have been given, that we kind of are looking for people anywhere and we are facing some shortages in that particular endeavor.

Where will we find all the additional officers necessary to fulfill this requirement in general and corporate aviation?

Ms. ROSSIDES. I believe that the proposal would allow those corporations to employ their own, and then we would train them or offer training to a certain standard.

Mr. MASSA. Well, I would offer an observation that if a company is buying and training their own, we have kind of lost control of that particular aspect of the security operation.

So it is my opinion, as a pilot, I am very dubious of the enhanced security that this particular mandate, in all of its factions, will bring. I am concerned about its cost-benefit analysis and detracting from other areas that are a much more significant potential threat.

I am open to participate and offer any insight, as a guy with an awful lot of hours behind the stick, as to what this is going to mean to general and corporate aviation and to the traveling corporate world. This is an incredibly important tool to them. I don't want to put any more burdens on business when we don't have to.

Ms. ROSSIDES. We would be happy to sit down and talk to you and actually brief you on the comments as we go through the period of working with the associations.

Mr. MASSA. Thank you.

Thank you, Madam Chairwoman. I yield back.

Ms. JACKSON LEE. Let me query my colleague, because he does have a lot of information.

Before I do that, Ms. Rossides, let me suggest to you that we are going to look at the jurisdictional question of 9/11 versus H.R. 2200. I would offer that clarification.

Before Mr. Massa leaves, I wanted to query Mr. Massa before I move us to our next round.

Because of your experience behind the stick, could you just articulate for the committee the point that you are making? Were you suggesting the impact on general aviation?

Mr. MASSA. Thank you, Madam Chairwoman.

Ms. JACKSON LEE. So our witness can hear it, as well, maybe in a clearer manner.

Mr. MASSA. Certainly. So my concerns about this particular proposed enhancement of security on aircraft—and I think it is over 18,500 pounds; I may be off on that number, but it is almost everything that flies—has to do with not only its impact on general aviation, which I believe, if fully implemented, will basically terminate general aviation, but also on the ability to use corporate aircraft as an extensive business tool.

I fully understand that a three-engine Intercontinental jet or a Gulfstream 5 or any of the larger corporate jets potentially represents an aviation threat as per the nightmares that we have lived through in the last decade. But every individual on a corporate flight is self-identifying and self-selecting. That airplane will never get off the ground unless everybody on the airplane knows everybody else on the airplane. That is the fundamental difference between corporate aviation and the general traveling public.

Likewise, in light general aircraft it is much the same. If the airplane is small enough, you can't put the security measures inside of a Cessna 150 or a Cessna whatever.

So I am very, very concerned about the impact on this industry. It represents a significant sector of our economy. We have, you know, whole cities, literally, for whom the construction of light and corporate aircraft is a key element.

I do not presuppose or recommend that the current briefings I have received get enacted into law. This is going to be very, very, very problematic. Again, I am speaking to this as a guy who has done a lot of flying.

So I offer those viewpoints, and I stand ready to help in any way possible. Although I will counsel there are a lot of people on this that are a lot smarter than I am. But I know the questions.

Ms. JACKSON LEE. I wanted you to restate your concerns on the record and just to say to you that, on that particular question, we are going to have a general aviation hearing so that we can respond to being helpful to TSA. TSA's regulations have been, if you will, somewhat challenging. I happen to err on the side of wanting more security, but I also want to be balanced and responsible.

So I wanted you to be able to articulate that on the record again. Also indicate to you, Mr. Massa, that we will be having a hearing on this question overall of general aviation security.

I would just ask the agency to be prepared, because we will be asking you to respond to your framework for security in that instance. I thank you.

We are going to start a second round that I am going to start with and then yield to you, Mr. Dent. I am going to focus my questions on cargo and a number of other issues.

I would appreciate, Madam Administrator, if you would explain to us the reduction in light of the upcoming August 2010 100 percent cargo screening deadline for cargo on passenger aircraft. The reduction I am talking about, the fiscal year 2010 request for air cargo security programs is less than the enacted fiscal year 2009.

Can you describe how the budget is changing with respect to the number of inspectors, as well as the resources being allocated to certify shippers' screening facilities?

I have visited a number of our airports; I think I relayed that to you. One of the issue was the certification of the shippers' screening facilities, which can be helpful in moving cargo.

Would you provide us with your understanding of that?

Ms. ROSSIDES. Yes, ma'am. The enacted 2009 cargo budget was for $123 million, and the request for 2010 is $108 million, and that difference, which is actually $15 million, represents a reduction from 2009 to 2010 for a one-time investment in technology to be deployed in pilot locations with these cargo facilities to test in the cargo environment the technology.

With respect to the number of inspectors, the program level from 2009 to 2010, it remains the same. In fact there is a small increase for the cost of living for the payroll for the employees in the program area.

The work that we are doing in the air cargo program is a very strong partnership with the external business cargo facilities, those who are becoming certified shippers, and that is on-going and we are actually making very, very good progress, particularly here in the United States, with certifying those facilities and those certified shippers so that we are quite confident that we will get to the 100 percent by August 2010 here in the United States.

With respect to the international partners, we are doing a lot of work internationally, visiting those countries, really training them, educating them about the process that the United States Government has put in place here, and gaining compliance that way with our international partners.

So from a budget standpoint from 2009 to 2010, that reduction was a one-time technology investment that does not impact the strength of the program from 2009 to 2010.

Ms. JACKSON LEE. That seems to be a limited window. You are suggesting that the work that you do between 2009 and 2010 is not going to be diminished. What about perspective planning, needing more staff to prepare for after 2010? How does this budget relate to those issues?

Ms. ROSSIDES. The projection is once we gain compliance with the mandate by 2010. Then those resources will be in an audit role. They will go out and they will visit, and we will have a series of ways of looking across the system, looking at compliance and then selecting for audit those locations where we believe we may have a concern. But the program will shift from educating to gain compliance and certification to an audit process.

Ms. JACKSON LEE. So what you are saying is you have enough personnel to certify, and you use a formula to audit and to check to see whether or not they are functioning properly?

Ms. ROSSIDES. That is correct, after they have been certified.

Ms. JACKSON LEE. Let me put a hold on that point and just raise the issue of whether or not I am comfortable with security being done by audit. So I know some information has to be gained that way as well. Why are there no new FTEs or funding increases for the purpose of building and expanding the expertise and workforce for surface transportation programs? I hope you and the staff will review extensively H.R. 2200 because it does have a lot of positive aspects for surface transportation security.

Ms. ROSSIDES. First of all, let me say that we do appreciate the fact that with the TSA reauthorization bill, there is direction to TSA to focus on surface modes of transportation.

With respect to our budget in 2010, it is for $128 million. That actually represents an increase of about $65 million over our enacted 2009 level. Most of that is going towards our VIPR teams, which are—this will create 15 permanent VIPR teams that will be deployed in the surface modes of transportation. In addition, that supports 225 surface inspectors who work across the system in the surface areas doing the inspection work and working with those industries in terms of meeting certain security standards that we put out across the system.

Also, our surface program includes canines, which currently we have 86 teams which cover 15 different mass transit locations and ferries as well on a random basis.

Ms. JACKSON LEE. Let me just pursue the VIPR teams, which have their fans and nonfans. When you say deploy 250, are you talking about over various surface transportation systems?

Ms. ROSSIDES. Yes, ma'am. Working with our State and local partners, we would go into various modes of transportation. For example, we would work in the rails with Amtrak, we would work in mass transit in some of the major cities, working with them to put these VIPR teams, which we have found to be an excellent deterrence. The success of these, for example, in the last couple of years we have probably executed about a thousand VIPR team deployments, and about 45 percent of those have been in the surface areas. It is very much a partnership with the local mass transit police departments, local mass transit authorities, and we have done work in collaboration with the Coast Guard with the ferries in the Pacific Northwest.

Ms. JACKSON LEE. We have the funding to deploy them and have them remain in place for a period of time?

Ms. ROSSIDES. They would be strategically situated around the country to work in an area in the mass transit in those areas.

Ms. JACKSON LEE. Targeted or to remain on-going?

Ms. ROSSIDES. It would be an on-going process.

Ms. JACKSON LEE. So they would be assigned to a specific area when we have funding to keep them on duty?

Ms. ROSSIDES. Yes.

Ms. JACKSON LEE. Just for my own edification, are there various oversight in terms of back at headquarters on issues dealing with civil liberties and civil rights in terms of how these teams will be acting?

Ms. ROSSIDES. Yes, ma'am. They all have a supervisor on the site with them, and they have been through the training. Our Office of Civil Rights and Civil Liberties does monitor their activities, and any instances of concern are immediately investigated.

Ms. JACKSON LEE. Thank you.

Last year working with Assistant Secretary Hawley, we discussed checkpoint evolution as TSA's new way of modernizing checkpoints across airports. This initiative was started at the end of the previous administration. Outside of BWI, it does not appear that many of the elements have been implemented in other airports. What is the status of Checkpoint Evolution?

Ms. ROSSIDES. Well, I am very happy to say that as of end of April, we have completely trained all 50,000 frontline officers in the training which we called "Engage and Coach," which was a combination of providing them enhanced IED detection capabilities.

Ms. JACKSON LEE. So you are saying it is across all airports?

Ms. ROSSIDES. Yes, ma'am. We have trained the entire workforce by the end of April.

The other part of the evolution strategy is to continue to focus on the training of our supervisors, which we are in the process of doing now. Then the third element really is the technology, which is the major investments in technology that we are making to bring the entire system at the checkpoint up in terms of our advance technology X-ray and continuing to improve the in-line baggage systems.

Ms. JACKSON LEE. What methods are you using to measure to check to see whether or not the Checkpoint Evolution is working? What are your benchmark standards?

Ms. ROSSIDES. The benchmarks and standards include, we have a pilot program on-going where we are asking the traveling public for feedback as soon as they have passed through the checkpoint. We have piloted that at BWI.

We also are developing surveys in conjunction with several of the carriers to ask about passenger experience that they have had.

When we have deployed any of the new technology in, for example, the WBI in the pilot modes, we do surveys right there with passengers to ask them for their feedback, and we are developing a series of pulse surveys that we will provide to the workforce that continues to focus on their ability, their quality of work life issues within TSA, all of which goes towards their ability to better do the job.

Ms. JACKSON LEE. These are good benchmarks. Do you have someone reviewing this and making assessment?

Ms. ROSSIDES. Yes, ma'am. The senior leadership team of TSA, and particularly our managers in our security operations, look at these measures and they drill them down to every airport in the country.

Ms. JACKSON LEE. Let me yield now. Thank you very much. Let me yield now to the gentleman from Pennsylvania, Mr. Dent.

Mr. DENT. Thank you, Madam Chairwoman.

The Inner City Bus Security Grant Program has provided grant programs to private over-the-road buses for the past 5 years. The President's fiscal year 2010 budget request, however, proposes the elimination of this grant program. Can you tell us why the Inner City Bus Security Grant Program is being eliminated in this year's budget?

Ms. ROSSIDES. Sir, the proposal was to shift the focus from the grants funding per se to the work with what we call an ISAAC, which is an interagency advisory committee. In the course of looking at the entire grants process this year, those were not funded for 2010.

Mr. DENT. Also, section 1604, the implementing recommendations act of the 9/11 Commission Act required that airports that have incurred eligible costs associated with the development of partial or completed in-line baggage systems before enactment of the implementing recommendations act of the 9/11 Commission Act be included in the TSA prioritization schedule for airport security improvements projects. The President's budget request includes a significant funding increase of $565 million from the 2009 level for in-line explosive detection systems, procurement, and installation.

Can you tell us how much of that funding will go towards the reimbursement of airports for in-line systems that airports themselves installed and paid for?

Ms. ROSSIDES. No, sir, at this point I can't give you an exact figure on that. I will tell you that we do, through a rather extensive process, have the airports apply, but I can predict the breakdown of that right now.

Mr. DENT. The final rule for the Secure Flight was announced in October of last year. Can you give us an update on the Secure Flight implementation?

Ms. ROSSIDES. Yes, sir. The Secure Flight Program began to actually what we call cutover air carriers at the very end of January. As part of the building of this program and the work to bring it on-line, we have done an extraordinary amount of work with the Government Accountability Office, which has been a terrific partner in getting us to a program level that is really quite exceptional. We have met all 10 conditions that the GAO set before we launched the program.

As of today, we have four or five carriers that are now providing their passengers' names, and TSA is screening them under the Secure Flight Program, and we are working with all of the domestic carriers to provide the dates for when they will begin cutover. The goal is to have all domestic carriers cut over and operating fully under Secure Flight by March 2010. We are working with them now on those schedules for the cutover. The ultimate goal is the international carriers will be all covered under Secure Flight by the end of 2010.

Mr. DENT. Thank you. I yield back the balance of my time.

Ms. JACKSON LEE. I thank the gentleman.

Mr. Luján for 5 minutes.

Mr. LUJÁN. Thank you, Madam Chairwoman.

One of the questions I have in and around, and I guess most of my questions center around, in and around surface transportation, with how we are able to fully screen vehicles, trucks. We go back to 1995 with the Oklahoma City bombing, how we are screening vehicles and the importance of looking at container vehicles and those vehicles delivering packages to homes and business, and what we truly can do to ensure we are providing adequate screening for these vehicles.

How is the Department ensuring that these vehicles, there is adequate support for surface transportation going forward?

Ms. ROSSIDES. Part of the dynamic is what is the TSA role versus the State and local role with respect to surface transportation, the truckers, and we do this through a series of assessments. We have a model where we are assessing each of the industries in terms of their abilities to provide training to their workers. We do have programs in place where we vet the drivers and we also have an extensive work through our grants administration which goes to surface in general, particularly with respect to rail. It is a matter of our providing them certain standards to meet rather than we are in there actually inspecting.

Mr. LUJÁN. I talk about our laboratories quite a bit. I think they are an immense resource. But there are laboratories that are developing technology for quick screening but it is very effective screening that I hope we look to employ. One of the concerns that I have is a few of the programs that are related to surface transportation. One is the First Observer Program, which appears to be getting reduced, although there is the Highway Information Sharing Analysis Center, which is getting an increase, but it is part of the First Observer Program which appears to be getting cut. I would like to know how that is going to truly work or provide support from a surface perspective.

Then related to the efforts with utilizing some of the VIPR teams, one of the concerns that I have, and I will quote from some information here, that the surface transportation security and efforts to analyze functions established in the 9/11 Act, it is troubling that the additional funds and personnel are not targeted to any of the most urgent needs or gaps in TSA's execution of its surface transportation security mission, such as the Surface Transportation Security Inspection Program, the Transit Security Grant Program, and building up surface transportation security personnel and expertise.

Although we are seeing more support with surface transportation or with the VIPR programs, the resources don't appear to be going toward the surface transportation security inspectors, and I may have that unclear and if I need to clear that up, please let me know. But when we are utilizing these programs to assist or offer the initial support with transit or with surface, why is it that the training that is taking place is maybe those who have more expertise with air as opposed to those on surface, where in fact that program is to be managed a bit by the entity with the air marshals?

Ms. ROSSIDES. If I understand your question, on the surface side what we do is we help design training, we help put standards out. We work with whatever the mode is, whether it is rail, mass transit, highways, to provide training conferences. But a lot of that is done as part of creating a baseline of a standard for that particular industry.

The VIPR program is utilizing TSA resources, TSA personnel, to assist, to complement, to help provide as a deterrence in those surface areas.

I don't know if I have answered your question. We can go back and I can give you a total picture of what we are doing in the highway area with the ISAAC and how that is viewed as one of the strong partnerships between TSA and the Federal sector, is the work that we are doing with the highway and the motor carriers. But I am not sure that I am being responsive to your question and that I am answering your question.

Mr. LUJÁN. Madam Chairwoman, I will submit the question in writing.

Can you include where are the most urgent needs or gaps in TSA's execution of its surface transportation security mission exists to the committee? I think that will assist us in providing the needed resources and they are being targeted to areas where we are making sure that we are keeping our surface areas the safest.

Thank you, Madam Chairwoman.

Ms. JACKSON LEE. Thank you. We would be happy to have the gentleman meet with representatives from TSA going forward, or the gentleman can engage the committee staff and we can be sure that his questions receive an answer in writing. That may be helpful to the gentleman.

I am delighted now to recognize the gentleman from California, Mr. Lungren, for 5 minutes.

Mr. LUNGREN. Thank you, Madam Chairwoman.

Registered Traveler, Congress likes the idea. Congress says they like the idea. Congress repeats they like the idea. Congress puts it in legislation; and TSA says, What? What does it take for Congress to convince TSA and whatever administration it is that we are serious about Registered Traveler?

Ms. ROSSIDES. Well, sir, I think we know that you are serious about it, and I think one of the things that we are looking at is how do we create the kind of process that is first focused on security; second, enables us to ensure that we don't have what we are concerned about with respect to clean skins?

Second, one of the things that the Secretary now is looking at is Registered Traveler-like programs across the whole Department, and how do we maybe bring some alignment with those and how do we employ those in a risk management way?

One of the areas that will make all of our jobs easier at some point down the road, and hopefully in the not-too-distant future, is the use of biotechnology and biometric cards and things like that so we have a confidence in who is presenting that you don't have a fraudulent form of identification and that you create a program where you are maximizing the security benefits as well as the customer service benefits.

We don't have the program today, and I will tell you that the Secretary is committed to looking at this as well as other RT-like programs across the Department.

Mr. LUNGREN. What I can't understand is we use now, we use the license you get from a State. Some States do a better job than others in making sure that the person who gets it is the person who says he or she is. I have always thought that part of the equation of risk is threat consequence—threat vulnerability and consequence, and the only way you know the threat is by gathering information or intelligence. The whole idea of registered travelers is people expose themselves to more information checking for you than the average person. Presumably a one-time or twice-a-year person getting on the airplane is not going to be as interested in it as a regular traveler. So presumably you can do the vetting of these people or have the company that does the Registered Traveler Program do the vetting of these people on a regular basis and you would have more information. I don't understand. Why does giving you more information make it more likely that they are more of a threat than less information? I can't get over that. I understand you folks say we don't understand it, but I just don't understand that. I mean, I presume if you have more information upon which to check against somebody's bona fides, that is better than not having the information, isn't it?

Ms. ROSSIDES. It is. It is. As I said, the goal going forward is to look for what kind of a protocol, what kind of a security clearance, and what kind of a card could you have that would benefit the interest of folks that are looking for an RT versus our interest for screening.

I would say it is still an issue on the table and we just haven't gotten the solution yet.

Mr. LUNGREN. I understand the Behavior Detention Program at the checkpoints have been very effective?

Ms. ROSSIDES. Yes, sir.

Mr. LUNGREN. Can you give us a status update on the program? What do you think we will be doing in 2010 funding to further improve the program?

Ms. ROSSIDES. It is basically a flat budget for behavior detection officers, and they are the folks that are trained to observe passenger behavior and then refer to the officers at the checkpoint if they see any anomalies in those behaviors.

We also have a slight increase of about 55 FTE for our bomb appraisal officers. These are two complementary skill sets around the checkpoint that help with detection. Both of these programs have been terrific internal to TSA from a security standpoint, but also they have given our officers a career path to move from a transportation security officer up to a behavior detection officer or a bomb appraisal officer.

Mr. LUNGREN. So from your standpoint and from your administration's standpoint, you think these have been successful programs?

Ms. ROSSIDES. Yes.

Mr. LUNGREN. They have come through well under the testing and we ought to integrate them as a regular part of our program, correct?

Ms. ROSSIDES. Absolutely.

Mr. LUNGREN. I don't think these programs are that well-known here on the Hill, and I think we need to do a better job of letting Members know exactly what this is and the basis upon which you have made the evaluation so that you will have the support for it that I think it deserves.

Ms. ROSSIDES. I would be happy to brief the committee.

Mr. LUNGREN. Thank you very much.

Ms. JACKSON LEE. I thank the gentleman very much, and I want to thank Mr. Cleaver for his patience, and I yield the gentleman 5 minutes for questioning.

Mr. CLEAVER. Thank you.

Let's go back and revisit the whole issue of cargo. I have three quick questions. With H.R. 2200, TSA was given additional time to move up to 100 percent of the cargo internationally. Perhaps I should have asked this question a little better when we had our earlier exchange because I am not sure whether you said you still don't believe that we will get up to 100 percent internationally after the additional time?

Ms. ROSSIDES. At this point, the additional time would be beneficial to have. I just can't say sitting here today what countries will be the last to come into compliance and by what date we will be able to get that date. If it is August 2010, December 2010, that is part of the work with these international partners that we are trying to do. I will check and we will provide, I am happy to provide the committee a specific schedule by country when we think we will have compliance. But I can't answer the question right now.

Mr. CLEAVER. It would be important for me to know that because I remember when we had the onslaught of public criticism, as I am sure you do, so this is an important issue out in the world.

I am a former mayor, and we have all of our police officers, when they stop individuals they always refer to them as "Mr." and "Mrs." because people don't like to be stopped so you have got to be as courteous as possible. I am familiar with police departments, primarily in Missouri, but the chances are that is the case around the Nation, for the same reasons. That is not a part of the training for TSA officers?

Ms. ROSSIDES. Yes, it is, sir. We put a lot of emphasis on the courtesy, the professionalism, the respect that they should pay passengers. We even go so far as to recommend specific statements that they should be making when they are approaching the passengers, when they are patting them down. We do focus on the communication with passengers.

Mr. CLEAVER. Yes, I flew out of an airport yesterday in Springfield, Missouri, and Bentonville, Arkansas, have a joint airport, and there was an older gentleman who was being screened and the TSA office kept saying, "Bob, just come over here and sit down." I wanted to say something, but of course I thought better of it and I think I was probably smart in not saying anything. It just occurred to me that may not be a part of the training, but you are saying it is?

Ms. ROSSIDES. It is, sir. But there is always room for improvement for a workforce of 52,000 people.

Mr. CLEAVER. Yes, and that is exactly where I am going now because there is an increase in the training budget this year. Is there a certain area where you intend to go in terms of improving training or creating training with the additional money that is appropriated or will be appropriated?

Ms. ROSSIDES. Yes. Our focus is on their ability to detect small improvised explosive devices, and those training dollars go principally to continue to train them in that area. However, the training that I just described we finished to all 52,000 employees, actually a good deal of that was on how you engage the passenger and how you communicate with them. One of the things we are looking at as well is continuing to put out training on that side of the equation because for the officer, honestly, if they have a calm passenger and they get in the proper kind of conversation with the passenger where they remain calm as they are going through the screening process, we actually get a higher level of screening as a result. So it is very much a part of the training for both improvised explosive device training as well as how they engage with the passengers, how they communicate with the passengers.

Also, we put a tremendous amount of focus on dealing with people with disabilities and training for persons in wheelchairs and other disabilities because such a great percentage of our traveling population either is persons with disabilities or persons with artificial hips or persons with pacemakers, and so that is also a part of the training.

Mr. CLEAVER. I have a missing knee, my left knee, and so I go through it twice a week. I am perfectly willing and happy to do that, and I am glad that the training is moving in that area because this gentleman that I spoke of earlier, he was irritated and a little confused and then I became irritated and confused, as were others around me. But I held back because if you are a Member of Congress and you say something, you end up on the front page of the newspaper, maybe even get the chair, the electric chair.

Ms. JACKSON LEE. Would the gentleman yield?

Mr. CLEAVER. Yes.

Ms. JACKSON LEE. The gentleman has articulated a concern that has been constant. My recollection, Mr. Cleaver, is that we worked very hard to secure TSA officers or TSOs after 9/11. It was a massive plus-up, a surge. I am grateful for the wonderful Americans that rose to the cause. I think as we have thanked them for their service, and there are probably a number of individuals he might know in his own airport that he sees on a regular basis and says thank you, but this training issue has come up a number of times.

Professional development, I would like to call it. I would like to work with the gentleman. In fact, we are going to be writing free-standing legislation on this whole question of professional development. I thought we had more of it in H.R. 2200, but we had so much to do.

Let us put this on your mind. What the gentleman has been saying and what we have all been saying, one of the reasons we went to behavioral assessment, and that information was given to me by another TSO who was trying to be responsive, that behavioral person didn't have all of the manners that I think they should have. Security should not be conflicted with manners.

I would just like to join the gentleman. He made a simple point which is he could call this person mister, whoever the TSA officer was, but that is in a line of circumstances that we seem to find, and I am just going to put—I am used to putting gorillas on the record. No Member is asking for special privileges, it is not about us. But what I would say is what the gentleman has indicated, if we were or a good citizen were to offer a suggestion, think what the gentleman is saying, that our suggestion would be taken out of context and there is no question as to there is some doubt as to how it would be received and whether or not there would be a supervisor there that would welcome Congressman Cleaver's calm assessment of the circumstance. That is all in training and that is all in professional development, and at the same time balancing and making sure that terrorists and the shoe bomber and some other creative person doesn't get through.

When we first started this, Congressman Mayor, you were a mayor and read about this. The baby formulas were maligned and mothers who were breast feeding had issues. Then we had issues with the hip, the artificial hip. We were just getting it together.

So, Madam Administrator, as we move into this new administration, as we plus up on the numbers of TSOs because we need them, as we prepare to provide them, and this is not your issue, but provide them opportunity for workforce rights that they have been asking for, I think it is important for you to note, and I will yield back to the gentleman, as someone who has been involved either on this subcommittee for a number of years since 9/11, this is an issue that we must confront. We confront it all of the time in our law enforcement, but this is a new team. It looks like on this new team we should be able to make as much progress as we possibly can.

I yield to the gentleman.

Mr. CLEAVER. Thank you, Madam Chairwoman. You said much more eloquently and clearly what I was hoping to convey. Whenever we increase training dollars, it seems to me that is a perfect opportunity to expand the teaching of courtesy.

I yield back.

Ms. JACKSON LEE. Thank you very much for your astuteness and eloquence, Congressman.

Let me conclude by giving us an update on the Secure Flight Program implementation. It looks like there is very little in the budget requested for this program, and we would like to have the assurance from TSA that you are budgeting appropriately for this program since it is supposed to be completed in fiscal year 2010?

Ms. ROSSIDES. Yes, Madam Chairwoman. We are making excellent progress on Secure Flight. The system is built and we are in the process now of working with the carriers to begin the transference of their system of vetting over to TSA. There is a schedule in place. We are working very hard with the carriers to keep that schedule so that the U.S. carriers have been cut over and their passenger records are being vetted under the Secure Flight Program by March of 2010, and again the international carriers by the end of 2010.

We have had great success with those carriers, albeit they are small carriers, and our capability to vet them under the Secure Flight Program. There is a very strong management team in place, and as I stated earlier, we have met all of the conditions under the Government Accountability Office for this program to be a very strong program. We will keep the committee apprised of the progress we are making as we are bringing the major carriers into the system.

Ms. JACKSON LEE. I appreciate if you would keep us informed. It is very important. I also ask, we have language in H.R. 2200 on these foreign repair stations. This has been a continuing issue for this committee. We want to see TSA take our interests seriously and begin to look at the structure that you need to put in place and the requirements that you need to put in place.

There is no doubt that every time a catastrophic incident happens in the air, or one that happens on the ground, such as Mumbai, which was our latest, and we had Spain and some other areas, that was surface transportation, but the recent Brazilian Air France air crash, those of us on this committee's immediate response is not to be hysterical but it is to think of anything so catastrophic, disappearing, no evidence, at least in the most recent hours, begin to think of all kinds of unfortunate incidents. Those foreign repair stations are one of the stopgaps to that kind of unfortunate circumstance possibly occurring, as it was with the question of interline bags that we addressed, tragically probably too late in the case of Pan Am 103, which was preceding 9/11.

So what is the hold-up or the issue with the foreign repair stations?

Ms. ROSSIDES. Madam, the rule is within review still within the administration, and we are working very diligently to get it out so that it will be something that we can work on. We are staying in very close touch with the FAA on it, and it is a matter of getting it through the review process currently within the administration.

Ms. JACKSON LEE. I want to leave these points on the record. Mr. Reitinger has gone and this is not in his absence, but if you can convey to him, I think I made a point about being apprised and kept in sync with what you are doing on outreach. I know that TSA, the whole agency is looking to provide, to ensure that they have the right kind of staffing. Some people would say, as I mention this on the record, that I am speaking the obvious because there is possibly new attitudes here in Washington, and I respect that and I am excited about it, but I hope that we are keeping in mind diversity, and that includes region, that includes ethnicity, racial. Sometimes that overlaps. That includes both, if you will, gender, that is diverse, so we will look in far ranges of opportunities.

I hope that we will look at the Nation's colleges. The class of 2009 is now ready to work. There are small and large universities. I am always hearing from my constituents, they didn't come to ABC, 2,500-student campus, I know you can't do that, but with e-mail and outreach, I frankly believe some notice should be at all of the campuses across America, at least those that may have programs, and that includes historically black colleges, Hispanic-serving colleges, and any other college, community colleges, Ph.D., MIT, all those that have a range of diversity.

I think the other point of it is that goes to the idea of contracting. H.R. 2200 gives some impetus or push to science and technology that has not been very responsive. There are all sorts of small inventors and others with creative ideas that need to be before you and need to be on your list if they are adequate. That needs to be diverse as well. Talent is diverse. Maybe we will have an opportunity for us to get back and show some data that indicates that you have seen the light as you move forward to building your team and obviously getting all of the personnel that the Secretary needs at DHS.

Ms. ROSSIDES. Thank you, Madam Chairwoman. I would love to come back and brief you on specifically the initiatives TSA has put in place on diversity. We have some superb programs with colleges and programs where we are offering our officers associate degrees. We have extensive intern programs now that are in place, and I would love to be able to brief you or the committee and your staff on those programs.

Ms. JACKSON LEE. We will be delighted, and you will get your chance.

Ms. ROSSIDES. Thank you.

Ms. JACKSON LEE. Let me ensure that I have no further questions. I think I have asked the question on Secure Flight.

I thank the witnesses for appearing before us today and the Members for their question. The Members of the subcommittee may have additional questions for the witnesses, and we ask that you respond to them expeditiously in writing.

Hearing no further business, let me thank you very much for your presentation. The subcommittee now stands adjourned.

[Whereupon, at 3:58 p.m., the subcommittee was adjourned.]

APPENDIX

Questions From Chairwoman Sheila Jackson Lee for Phillip R. Reitinger, Deputy Under Secretary, National Protection and Programs Directorate, Department of Homeland Security

Question 1. There has been a lot of discussion about the permanence of NPPD. As we all know, it is a disparate collection of entities that, in some cases, do not appear to have a unifying focus beyond being security programs. With that said, does this budget set the stage for a reorganization of NPPD before or after the delivery of the Quadrennial Homeland Security review next winter?

Answer. The National Protection and Programs Directorate (NPPD) is a diverse organization with a vital cross-cutting and unifying mission of risk reduction. The Directorate works to reduce risks to the Nation through five mission areas: Protect the Nation's citizens and visitors against dangerous people, protect the Nation's critical infrastructure, protect and strengthen the Nation's cyber and communications infrastructure, strengthen the Department's risk management platform, and strengthen partnerships to foster collaboration and interoperability.

NPPD has just passed the 2-year anniversary of the establishment of the organization and much has been accomplished during this time to solidify NPPD as a permanent organization within the Department. While building an organization that is best aligned to meet critical mission needs is always under review, there are currently no plans to eliminate or reorganize NPPD before the delivery of the Quadrennial Homeland Security Review (QHSR). The findings of the QHSR will be incorporated during the fiscal year 2011 and 2012 budget cycles. It is premature at this time to speculate whether the QHSR findings will impact the organizational make-up of NPPD.

The fiscal year 2010 President's budget request included the proposed transfer of the Federal Protective Service (FPS) to NPPD from U.S. Immigration and Customs Enforcement. The proposed transfer aligns the FPS mission of Federal facilities infrastructure protection within the NPPD mission of critical infrastructure protection. Further, NPPD chairs the operations of the Interagency Security Committee, a group that includes the physical security leads for all major Federal agencies and whose key responsibility is the establishment of Government-wide security policies for Federal facilities. These missions are complementary and mutually supportive, and the alignment improves and advances the mission effectiveness of both FPS and NPPD.

Question 2. As you can imagine, the subcommittee is concerned with the level of personnel NPPD employs. The subcommittee was happy to learn from your testimony that NPPD has brought on-board 300 new employees over the last 12 months, and currently has approximately 800 Federal employees on board out of the 1,064 fiscal year 2009 positions. We were pleased to learn from your budget request that you intend to bring on additional personnel. Please describe NPPD's efforts to employ additional personnel and how this will affect current contracts at the Department.

Answer. There are additional personnel coming on-board each pay period. The National Protection and Programs Directorate (NPPD) has 859 employees on-board as of July 6, 2009. There are an additional 184 selections in the pipeline, which are currently in the tentative job offer, security, or final job offer phases of the hiring process.

Additional efforts to increase NPPD's staffing include:

1. Within the past 100 days NPPD has switched their contract for hiring support from Booz Allen Hamilton to the Office of Personnel Management (OPM). In addition to a cost savings, OPM's processes have streamlined several of the hiring steps and have provided NPPD with a more comprehensive tracking system, which allows a more accurate identification and determination of where

delays are occurring in the hiring process as well as the ability to quickly address the underlying cause(s) for those delays.

2. The Deputy Under Secretary has implemented internal procedures that ensure appropriate coordination and hiring decisions are made within defined timelines.

3. An improved process has also been implemented to review requests by candidates for recruitment incentives.

4. There have been a number of steps undertaken by the Office of Security to streamline the clearance process. In addition to those steps, NPPD has received approval to assign a Federal employee full-time to coordinate the preliminary checks to abbreviate the amount of time required for a completed security package to get from the candidate to the security adjudicators.

5. Since there have been frequent delays in the amount of time selectees take to complete their security paperwork and have their fingerprints taken, tentative job offer letters now require candidates to complete their security paperwork and fingerprinting within a week of receiving the pre-appointment letter. If the required documents have not been submitted with a week of the offer letter the individual is called to determine if they need any assistance in completing this requirement and provided with 1 additional week if there is a reasonable justification for their delay. At that time they are also informed that if the paperwork is not completed within the second week, the job offer will be rescinded and DHS will need to go to the next candidate under consideration. Additional extensions are only approved for extenuating circumstances.

6. The Director of Resource Administration is also working with the components and the Human Capital Office to ensure that standard or existing position descriptions (PDs) are being utilized to fill current vacancies. The length of time required to draft, review, and acquire approval for PDs prior to announcing a position has been identified as a significant point of delay in the hiring process.

Based upon on board strength, the current list of candidates within the pipeline and the additional process changes undertaken, NPPD expect to be able to reach a required staffing level of more than 1,000 for fiscal year 2009, with selections made against another 10% of existing vacancies.

In regard to " . . . how this will affect current contracts at the department"; as FTE positions are filled with Federal employees it will reduce NPPD's reliance on contractors. As NPPD hires additional Federal personnel we are validating if contractor support positions need to be replaced. Once this determination is made NPPD will coordinate with the Office of Procurement Operations to request appropriate contractual action (i.e. reevaluating exercising contract of options periods and/or de-scope the contract requirements, etc.)

Question 3a. As you know, the subcommittee has been quite concerned about the progress and authority of the Office of Risk Management and Analysis. As directed, RMA has been providing quarterly updates to staff. From these updates, it appears that RMA has quite an ambitious agenda, ranging from a national risk assessment to the informing of budget cycles to a heavy presence in the development of the Quadrennial Homeland Security Review.

How, then, is approximately $9 million enough for fiscal year 2010?

Answer. The Office of Risk Management and Analysis (RMA) has two strategic objectives: (1) Establish an integrated approach to risk management within the Department of Homeland Security (DHS); and (2) conduct systematic, rigorous risk analysis methodologies to execute assessments in support of Department-wide decision-making. To work towards these objectives, RMA has planned and budgeted for the drafting of an Integrated Risk Management Framework and development of supporting materials and processes; execution of the Risk Assessment Process for Informed Decision-making (RAPID) tool; and leading a study, under the auspices of the Quadrennial Homeland Security Review, to develop a process and identify the level of required resources to produce a Homeland Security National Risk Assessment (HSNRA) which will serve as a tool to provide strategic guidance and inform high-level Departmental resource allocation in a meaningful way. Following the HSNRA study, RMA will review the scope of requirements and with guidance from Department leadership reevaluate the resources needed to accomplish their mission.

Question 3b. Staff was told last week that 19 of 26 FTEs are filled. How quickly can it be at full capacity, given the vast hiring bureaucracy at NPPD?

Answer. RMA has 13 Government personnel on board and 11 on-site contractors. In addition, 7 applicants have accepted FTE offers. Five of the 7 accepted offers are Presidential Management Fellows. The remaining vacancies within RMA are not due primarily to the perceived limitations of the hiring business process within DHS, but rather, the difficulty of finding qualified applicants with the technical and scientific expertise required for conducting risk analytics. RMA has the National

Academies and individuals from the private sector and academia assisting with the recruitment efforts. RMA is also considering filling at least one of the technical billets using an Intergovernmental Personnel Assignment (IPA).

Question 4. The President's budget request cuts $11 million from IP's National Infrastructure Protection Program efforts. Please explain the rationale behind these cuts, given that most companies are not regulated for security purposes and many do not have the financial resources in this economic climate.

Please also explain whether other departments and agencies—which partner with DHS under the NIPP—will be providing resources to further security efforts under the NIPP in fiscal year 2010.

Answer. The Department of Homeland Security (DHS) must prioritize limited resources towards the highest priority programs. The reductions to the National Infrastructure Protection Plan (NIPP) program efforts were required to fund other critical DHS responsibilities.

Maintaining the greatest possible degree of engagement and information-sharing with our private-sector critical infrastructure and key resources (CIKR) partners and coordination with the Sector Specific Agencies (SSAs) will continue to be a main focus of the Office of Infrastructure Protection (IP).

These funding reductions will result in DHS relying more heavily on its sector-specific partners to use their own existing expertise and sustain service capabilities. SSAs will need to assume a greater role in managing, developing, and producing sector programs, reports, and metrics. The private-sector is actively engaged in the public-private partnership. They contribute their subject-matter experts (SMEs) and bring corporate representatives to the table at their own cost and time. Several of the partnership trade member associations have taken on some of the sector support responsibilities including planning, analysis, and writing support for tailoring products to their members' interests. DHS will work diligently with remaining resources to ensure that the value found in information sharing and coordination remains high between DHS and our private-sector partners.

Although DHS will not be able to provide the same amount of in-person interaction with the private-sector and State, local, Tribal, territorial, and regional governments and organizations, the Department is promoting on-line conference capabilities and delivering web-based training on the Homeland Security Information Network for Critical Sectors. DHS will continue to foster relationships with private-sector entities while promoting mutual-aid agreements within and among CIKR partners in the industry.

The SSAs outside of IP provide funding to develop and implement a wide range of CIKR programs. The budget requests for each of these sectors are at least partially captured in their Sector CIKR Protection Annual reports. Due to the reduction, DHS will no longer provide on-site contract SME support to departments and agencies with SSA responsibilities, and they will need to assume a greater role for the development, coordination, and final submission of the sector metrics, Sector CIKR Protection Annual Reports, Sector-Specific Plans (annual reviews and triennial rewrites), and other required information.

Question 5. As you know, the expiration of the Chemical Facility Anti-Terrorism Standards is of great import to this committee. Is the Department prepared to ask for an extension of the legislation? If so, what resources are needed for fiscal year 2010 for CFATS? Your testimony requests $103.4 million for fiscal year 2010, which includes 268 Federal staff, and this is to be allocated for high-risk chemical facilities and to establish ammonium nitrate regulations. Under this request, how much is going to the CFATS program?

Answer. The President's budget submission included a request to extend authorization of the Chemical Facility Anti-Terrorism Standards (CFATS) for a period of 1 year to give us time to evaluate what is needed for a permanent authorization. For fiscal year 2010, the Department of Homeland Security has requested funding in the amount of $103.4 million to continue its efforts under CFATS and to develop ammonium nitrate regulations.

The Department's fiscal year 2010 request included 268 FTP and 246 FTE Federal staff. Of the requested $103.4 million in funding, the Department has proposed to direct $33.5 million to salaries and benefits, $55.5 million to CFATS and $14.4 million to ammonium nitrate regulations.

Question 6. As you know, the committee championed the resilience-based approach to critical infrastructure protection during the last Congress. Your testimony and the budget request highlight five Regional Resiliency Assessment projects at IP. Please describe these projects, their resources, and their objectives.

Answer. Much of the Nation's critical infrastructure and key resources (CIKR) are not part of a single, integrated system that can be controlled and monitored from a single location. High-priority CIKR are a complex "system of systems"—a loosely woven network of localized infrastructure, each with unique characteristics and vulnerabilities. Recognizing this, the Office of Infrastructure Protection (IP) has adopted a resilience-based approach to protecting Nationally significant CIKR. This shift is reflected in the *2009 National Infrastructure Protection Plan (NIPP), Partnering to Enhance Protection and Resiliency,* which focuses on protection and resiliency as National priorities. Resilience of critical infrastructure focuses on systems as a whole—particularly on investments that make a system better able to absorb the impact of an event without losing the capacity to function. The resilience of critical infrastructure also includes the protection and physical survivability of key National assets and structures. Because of the regionally clustered distribution of CIKR, the protection of component assets is best planned, coordinated, and executed locally. The Department of Homeland Security (DHS) developed the Regional Resiliency Assessment Program (RRAP) to analyze and build resilient assets, systems, and communities at the regional level.

The RRAP is a cooperative Government-led assessment of designated CIKR facilities and regional analysis of the surrounding infrastructure. It provides Federal, State, local, Tribal, territorial, and private sector stakeholders with an awareness of the geographic area's National and regional impact, vulnerabilities, dependencies, interdependencies, resiliencies, and necessary protective measures. The RRAP:

- Examines vulnerabilities, threats, and potential consequences from an all-hazards perspective using enhanced assessment methodology;
- Identifies CIKR dependencies, interdependencies, resiliency characteristics, and gaps;
- Evaluates the prevention and protection capabilities of owners/operators, local law enforcement, and emergency response organizations;
- Supports required grant applications;
- Provides baseline examination of risk and metrics to measure mitigation; and
- Coordinates and integrates other protection programs, including assessments, training, economic analysis, IED awareness, geospatial products, information sharing and exercises.

The RRAP analyzes gaps using multiple assessments and surveys including Site Assistance Visit (SAV)[1] and Enhanced Critical Infrastructure Protection (ECIP)[2] assessments, Buffer Zone Plans (BZPs),[3] the Computer-Based Assessment Tool (CBAT),[4] independent subject matter expert analysis, Emergency Services Capabilities Assessment (ESCA),[5] System Recovery Analyses (SRA),[6] Multi-Jurisdiction Improvised Explosive Device Security Planning (MJIEDSP),[7] National Capabilities Analysis Database (NCAD) assessments,[8] and other tools designed to capture the region's dependencies, interdependencies, and resiliency characteristics. The results are used to enhance the overall security posture of the facilities, the surrounding communities, and the geographic region using short-term improvements and long-term investments in equipment, planning, training, and resources to mitigate risk.

Each RRAP produces an Integrated Protective Measures Analysis (IPMA) Report and a self-executing CBAT multi-media file for use as a State and regional planning and response tool. The IPMA and CBAT multimedia file documents the resiliency of critical nodes in the region; dependencies and interdependencies among the assets

[1] SAVs are facility vulnerability assessments focused on identifying security gaps and recommending protective measures. SAVs are conducted by DHS/IP in coordination with other Federal, State, and local government entities and CIKR owners and operators.

[2] ECIP visits are conducted by DHS/IP in coordination with facility owners and operators and other Federal, State, and local partners to assess overall site security and recommend protective measures at facilities, track implementation of new protective measures, and build public-private relationships.

[3] BZPs are strategic documents developed by local jurisdictions with support from DHS that assist State and local law enforcement and other first responders in developing site-specific preventive and protective measures that make it more difficult to successfully target and attack CIKR sites.

[4] CBAT blends vulnerability assessment data, structural schematics, and other relevant site data with 360-degree spherical color video of facilities, surrounding areas, routes, and other areas of interest to create an interactive visual guide of any location.

[5] ESCA examines the region's emergency services capabilities in the context of all-hazard events such as natural disasters or terrorist attacks.

[6] SRA examines the region's interdependencies in the context of a tailored scenario, such as large-scale system failures or industrial accidents.

[7] MJIEDSP examines the region's IED security plans in the context of integration of assets and capabilities from multiple jurisdictions and emergency service sectors, providing DHS officials and regional authorities and responders with an accurate picture of current preparedness and response capabilities for IED security.

[8] NCAD assessments of bomb squads, explosive-detection canine units, SWAT teams, and public-safety dive teams use a task-based model to examine IED security operations capabilities and readiness.

and possible cascading effects from loss, destruction, disruption, or degradation of one or more of these systems; gaps and corresponding options for consideration, to be used for continued planning to buy down risk; and individual assessment reports and plans.

The IPMA can be used by the State to inform their Buffer Zone Protection Program (BZPP) grant applications. RRAP-identified gaps and options for consideration are mapped directly to the multi-jurisdiction Vulnerability Reduction Purchasing Plan (VRPP) required as part of the BZPP application. In this way the RRAP supports more effective resource allocation decisions. For each RRAP BZPP grant funding is used address RRAP-identified planning and equipment needs of the local law enforcement agencies responsible for protecting the CIKR sites.

Five (5) RRAPs will be completed in fiscal year 2009. RRAP locations were selected by DHS in coordination with the States based on relative risk profile and feasibility of the assessment process. Programmatically, each RRAP costs between $596,500 and $686,500 for DHS to conduct. This cost does not include BZPP grant funding, which are funds provided directly to local law enforcement.

Based on the budget request for fiscal year 2010, IP will conduct six (6) RRAPs. The regions will be selected by DHS based on input from the States through the Tier 1 and Tier 2 data call. The revised data call allows States to nominate "critical clusters" that meet the Tier 1 and Tier 2 criteria. Critical clusters are groups of similar infrastructure that can be disrupted through a single incident, whether natural or manmade, and the disruption of which could cause Nationally or regionally critical consequences meeting the Tier 1 and Tier 2 thresholds. IP is currently assessing high-risk clusters across the U.S. as well as preparing guidance and a data call to States. Potential locations for the fiscal year 2010 RRAP include: Detroit International Transportation Hub, Colonial Pipeline (Atlanta Hub), Louisiana Highway 1 (LA1), Port of Long Beach, Las Vegas Strip, and Henry Hub Pipeline in Louisiana.

(NPPD) OEC

Question 7. Within NPPD sits the Office of Emergency Communications (OEC), which has, among many responsibilities, ownership of the Integrated Wireless Network, or IWN. This is supposed to be an interoperable communications network for all Federal law enforcement officials—including DHS, DOJ, and Treasury. To date, however, OEC has done nothing to advance the implementation of IWN. In your view, is interoperability a priority for Federal law enforcement officials? If so, what role do you believe OEC should play in that effort? How should this office work with the Office of the CIO, as well as the CIOs of DHS components, to advance interoperability within DHS?

Answer. The Office of Emergency Communications (OEC) and Federal law enforcement officials recognize the importance of interoperability with other Federal, State, local, and Tribal agencies. However, existing Federal tactical wireless infrastructure is outdated, resulting in an inability to meet both intra- and inter-agency communications needs. Federal tactical wireless capabilities must be modernized and basic operability shortfalls addressed before interoperability can be achieved. Historically, these modernization efforts have been underfunded, which limits interoperability efforts.

The Department of Homeland Security (DHS) believes that the original Integrated Wireless Network (IWN) concept of a single, Nation-wide, consolidated network is no longer viable due to funding limitations and the disparate requirements of Federal law enforcements users. OEC and the Office of the Chief Information Officer (OCIO) are working together to implement the underlying IWN concepts of intergovernmental partnerships, joint requirements gathering, and integrated short- and long-term planning to improve mission-critical wireless capabilities and promote interoperability while reducing costs. OEC's inherent interagency and intergovernmental roles and responsibilities are appropriate to drive joint requirements development, planning, and implementation efforts. However, this can only be achieved with a true stakeholder-driven approach in concert with Federal users and managers from partner agencies and components.

OEC, the DHS OCIO, and the DHS Component OCIOs are working together through the Wireless Working Group to develop a consolidated Departmental strategy for the modernization of DHS tactical wireless infrastructure. This strategy will address immediate mission-critical tactical voice requirements while driving toward an integrated interoperable long-term solution. OEC supports the Department's strategic planning efforts by identifying opportunities for resource sharing with external agencies across all levels of government and by helping to define and shape interoperability standards and external relationships for long-term coordination.

Through the Emergency Communications Preparedness Center, OEC is advocating the need for Federal tactical wireless communications modernization and will elevate the issue to senior officials throughout the Federal emergency communications community. In addition, OEC is adding value to Federal efforts by sharing its knowledge of State and local activities across the Nation to help identify opportunities for resource sharing across various levels of government.

Question 8. The stimulus bill signed earlier this year provided $60 million for Customs and Border Protection to procure and deploy tactical wireless communications equipment. How is OEC working with CBP to ensure that this money is spent on equipment that would fit within the DHS vision of IWN and within the DHS vision for having an interoperable communications system for all its law enforcement officials?

Answer. In the case of the stimulus bill, the Office of Emergency Communications (OEC), the Office of the Chief Information Officer (OCIO), and the Department of Homeland Security (DHS) Wireless Working Group are working closely together to ensure development of a common strategy for both Customs and Border Protection and U.S. Immigration and Customs Enforcement that improves interoperability and cost efficiencies through the acquisition of standards-based technologies (e.g., Project 25) while promoting the sharing of resources, to include spectrum, infrastructure, engineering, and acquisition. Per DHS Management Directive 4100.1, OCIO is responsible for the internal coordination of wireless investments across the Department, which it does through the DHS Wireless Working Group. OEC identifies opportunities for DHS components to coordinate with other Federal, State, local, Tribal, and territorial agencies external to DHS.

Question 9. IWN has been under the purview of OEC for several years now. As you have become familiar with the work of NPPD during your time at DHS, what, if anything, have you seen done to date by OEC on IWN? Do you think that OEC has a role in overseeing a Department-wide effort to build an interoperable communications system for Federal law enforcement officers, given the lack of operational expertise in the Office?

Answer. The Department of Homeland Security (DHS) believes that the original Integrated Wireless Network (IWN) concept of a single, Nation-wide, consolidated network is no longer viable because of funding limitations and the disparate requirements of Federal law enforcements users. OEC and the Office of the Chief Information Officer (OCIO), through the Wireless Working Group are working together to implement the underlying IWN concepts of intergovernmental partnerships, joint requirements gathering, and integrated short- and long-term planning, thereby improving mission-critical wireless capabilities and promoting interoperability while reducing costs.

OEC works through the DHS Wireless Working Group and the OEC-chaired Federal Partnership for Interoperable Communications for operational expertise. OEC plays an important role in the Department-wide effort to build an interoperable communications system for Federal law enforcement officers. OEC's core roles and responsibilities are appropriate to drive joint requirements development, planning, and implementation efforts. However, this can only be achieved with a true stakeholder-driven approach in concert with Federal users and managers from partner agencies and components. OEC provides comprehensive knowledge and understanding of requirements and activities across departments and various levels of government to identify opportunities for resource sharing and to help define and shape external relationships for long-term coordination. Through the Emergency Communications Preparedness Center, OEC is advocating the need for Federal tactical wireless communications modernization and will elevate the issue with senior officials throughout the Federal emergency communications community.

Question 10. In the DHS response to the GAO Report on Radio Communication (report number 09–133, dated December 2008), the reason giving for abandoning the joint IWN program was, "Because DOJ and DHS have different regional priorities—a common system will not work at a national level . . . " Given that, why has DHS not at least embraced IWN within its own Department? Wouldn't the IWN program provide the cost savings, efficiencies, and interoperability needed between DHS agencies, such as CBP, ICE, Coast Guard, and others?

Answer. The Department of Homeland Security (DHS) believes that the Integrated Wireless Network (IWN) concept of a single, Nation-wide, consolidated network is no longer viable both for DHS and as part of an interagency partnership because of cost and schedule constraints. The Office of Emergency Communications (OEC) and the DHS Office of the Chief Information Officer (OCIO) are working together through the DHS Wireless Working Group (WWG) to implement the underlying IWN concepts of intergovernmental partnerships, joint requirements gathering, and integrated short- and long-term planning, thereby improving mission-critical wireless capabilities and promoting interoperability while reducing costs. Each of these organizations includes representation from U.S. Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP), and the U.S. Coast Guard (USCG), as well as the other DHS components.

OEC, the DHS OCIO, and DHS components including CBP, ICE, and USCG are integrating these concepts as they develop a consolidated departmental strategy for the modernization of DHS tactical wireless infrastructure through the DHS WWG. This collaborative effort will result in a strategy that addresses immediate mission-critical tactical voice requirements while driving toward an integrated interoperable long-term solution. A key element of the DHS strategy is to ensure that investments are coordinated with internal and external partners and that opportunities to share resources are appropriately considered. In addition, DHS components including CBP, ICE, and USCG are examining common architectures and standards so as not to preclude future interoperability or resource sharing if current operational priorities dictate the need to modernize independently in some areas.

Question 11. The White House Web site states the Federal Government will "support efforts to provide greater technical assistance to local and state first responders and dramatically increase funding for reliable interoperable communications systems." Given the minimal budget change in the President's fiscal year 2010 request for the Office of Emergency Communications, how does NPPD intend to meet the increasingly high demand for technical assistance across the country?

Answer. The National Protection Programs Directorate/Office of Emergency Communications (NPPD/OEC) Interoperable Communications Technical Assistance Program (ICTAP) provides direct support through the development and delivery of training, tools, and on-site services to State, Tribal, territorial, regional, and local agencies for the implementation of the National Emergency Communications Plan (NECP) and the advancement of public safety emergency communications, operability, and interoperability capabilities.

NPPD/OEC technical assistance is provided at no cost to States/territories with the stipulation that the services support the implementation of the State's Statewide Communication Interoperability Plan and promote achievement of the NECP goals. Using the NPPD/OEC Technical Assistance Catalog, the States may submit up to five requests for services annually (an average State has more than 30 applicable initiatives). Although participation by the States/Territories is voluntary, during fiscal year 2009 all 56 States/Territories have requested (or indicated that they will request) NPPD/OEC technical assistance, with more than 90 percent submitting the maximum five service requests. Nation-wide, 240 technical assistance requests have been (or will be) submitted. In considering these requests, NPPD/OEC uses a needs-based approach, incorporating the State's risk and communications capability, to determine how best to allocate its technical assistance resources.

The President's fiscal year 2010 budget request includes an additional $3.8 million for OEC. If enacted, the increased funding will provide some additional support to State and local interoperable communications technical assistance. Specifically, assistance will be provided to State and local governments to achieve response-level emergency communications by the designated goal deadlines.

The fiscal year 2009 NPPD/OEC budget for State-requested technical assistance was $5.2 million. OEC's strategy for meeting the current demand is based on innovative restructuring and the re-scoping of services. We try to minimize the travel cost by working remotely or conducting multiple engagements during a single trip. During the project-planning phase, OEC scopes the engagement in the most cost-effective manner. Our project managers look for additional cost-cutting measures by leveraging personnel with broad skill sets that allow them to conduct multiple facets of a Technical Assistance delivery, minimizing the need to send additional personnel. Lastly, we look to other programs to transfer applicable requests, such as the Public Safety Interoperable Communications Grant Program. Our diligent efforts to maximize the productivity of each Technical Assistance dollar enable us to fulfill more than half of the States' fiscal year 2009 requests.

Although it remains unclear how many ICTAP requests NPPD will receive for fiscal year 2010, we are confident that strong program management, responsible and creative engagement scoping, and the leveraging other programs will maximize the available fiscal year 2010 funding to ensure that State, territorial, local, and Tribal governments receive critical Technical Assistance services to address key emergency communications gaps.

Question 12. Nearly 8 years have passed since the tragic attacks of 9/11 and 3 years since the devastating storms of Hurricane Katrina. Congress responded and created the Office of Emergency Communications at DHS to be the focal office responsible for emergency communications in the Post-Katrina Emergency Management Reform Act of 2006. Despite efforts made by Congress, I remain very concerned by the various components at the Department with stronger influences over first responder communications capabilities. For example, some argue that the relationship between the OEC and FEMA Disaster Emergency Communications (DEC) is a complementary relationship, while others view their missions as overlapping, identical, or competing. Can you explain how you intend to strengthen the OEC within this budget request and streamline interoperable emergency communications issues at the Department and within the Federal Government?

Answer. Secretary Napolitano has made unifying the Department of Homeland Security (DHS) as "One DHS" a top priority. Within the Department, the Office of Emergency Communications (OEC) is the focal point for National planning and coordination for interoperable emergency communications, and Departmental leadership will continue to support OEC's efforts to strengthen and coordinate emergency communications activities both within the Department and across other Federal Government agencies.

The Department plans to facilitate intra- and inter-departmental coordination on emergency communications and interoperability issues. Inter-departmental coordination will occur within the Emergency Communications Preparedness Center framework. Intra-departmental efforts will occur within the framework of a DHS-wide working group, led by OEC and dedicated to coordinating emergency communications issues across the Department. The intra-Departmental working group will include components such as OEC, the Federal Emergency Management Agency, the National Communications System, and the Command, Control and Interoperability Division of the Science and Technology Directorate.

Question 13a. As you know, PKEMRA created the Emergency Communications Preparedness Center (ECPC) to serve as the focal point and information clearinghouse for Federal interagency emergency communications efforts. However, in order for the ECPC to be established, DHS, through the OEC, must complete a charter with the signatures from all the appropriate Department heads across the Federal Government. The ECPC charter was due to Congress last year, but it has yet to materialize.

What assurances can you provide to the committee about the Department's commitment to taking the issue of operability and interoperability seriously both at DHS and throughout the Federal Government?

Answer. The Department of Homeland Security (DHS), through its Office of Emergency Communications (OEC), is fully committed to establishing the Emergency Communications Preparedness Center (ECPC) as the focal point for interagency efforts and as a clearinghouse for intergovernmental information to support and promote communications operability and interoperability. OEC created an ECPC working group in September 2007 as the primary collaborative mechanism to establish the ECPC and facilitate its activities. In its first action, the ECPC working group solicited and coordinated Federal agency input to the National Emergency Communications Plan (NECP), which was published in July 2008. The ECPC working group also drafted and internally approved an ECPC Charter. The Charter was approved by the DHS Secretary on June 8, 2009, and distributed to member departments and agencies for approval and designation of their official representatives.

With the approval of the ECPC Charter by the Secretary of Homeland Security and continued planning within the OEC, the committee can be assured that DHS is seriously addressing the issues of operability and interoperability. OEC is actively supporting the following actions:

- Close coordination with ECPC member agencies to gain approval of the Charter and to identify representatives to serve on the ECPC executive and steering committees. To date, the Charter has been approved by six of the 12 ECPC member agencies;
- Content development and agenda planning for the inaugural ECPC executive committee and steering committee meetings to be convened upon final charter approval by member agencies;
- Development and testing of "beta" version of a secure emergency communications clearinghouse capability for rollout in January 2010;
- Continued execution of targeted focus group activity in the area of emergency communications technical assistance and grant guidance coordination. For example, the technical assistance focus group has successfully cataloged Federal Technical Assistance programs and begun identification and sharing of best practices for effectively administering Technical Assistance; and
- Execution and completion of the initiatives and milestones identified in the NECP.

DHS is optimistic that full approval of the ECPC Charter by member agencies will be achieved by September 2009.

Question 13b. From your assessment, what are some of the major hindrances to OEC fulfilling this requirement?

Answer. Approval of the Charter and designation of formal representatives to the ECPC have been delayed because of the impact of the Presidential transition and the resulting Departmental appointments and confirmations of personnel needed to review and approve agreements. We believe this to no longer be an issue.

Question 13c. What Congressional assistance is needed for the Department to complete this requirement?

Answer. We believe that progress is being made more quickly now with the ECPC Charter and the designation of representatives from the Federal agencies. In addition, we will continue to develop the agenda for the initial ECPC session.

(NPPD) CYBER

Question 14. How will the President's announcement of the creation of a new "cyber coordinator" in the White House affect the Department's cybersecurity mission?

Answer. As the Nation becomes ever more dependent upon cyber networks, we must address cybersecurity strategically. Overcoming new cybersecurity challenges is a difficult task requiring a coordinated and focused approach to better secure the Nation's information technology and communications infrastructures. President Obama's Cyberspace Policy Review reaffirms that cybersecurity is among the most significant issues facing the Nation's economy and national security, and it solidifies the priority that the administration places on improving cybersecurity.

The Department of Homeland Security (DHS) believes the creation of a senior-level cyber position within the White House will help ensure coordination and collaboration across Government agencies. No single agency is responsible for cyberspace and the success of our cyber mission relies on more than one department. As such, the many Government players with complementary roles—including DHS, the intelligence community, the Department of Defense, the Department of Justice, and other Federal agencies—require coordination and leadership to ensure effective, and efficient execution of the overall cyber mission.

DHS will continue to have a preeminent role in ensuring the cybersecurity of the Federal domain and collaborating with the private sector to improve the security of private sector networks, and it will have a significant role in accomplishing near-term actions outlined in the report, including updating the National strategy, strengthening private sector and international partnerships, increasing public awareness and preparing a National response plan. The operational goals of the comprehensive National strategy will include better coordination, response, recovery, and mitigation across stakeholder communities.

Furthermore, DHS works closely with its Federal partners, and the leadership and staff of the National Security Staff in the development and continued tracking, coordination, and execution of the Comprehensive National Cybersecurity Initiative. The Department also maintains close working relationships with the 18 Critical Infrastructure and Key Resources (CIKR) sectors, and their Federal sector-specific agencies, under the National Infrastructure Protection Plan Partnership Framework.

Question 15. How does the Department intend to work with other relevant agencies to secure the electric grid from cyber attack?

Answer. In May 2004, DHS created the Control Systems Security Program (CSSP) within the National Cyber Security Division (NCSD) to lead a cohesive effort focused on reducing the cyber risks to the control systems within critical infrastructure. A control system is a general term that encompasses several types of systems, including Supervisory Control and Data Acquisition, process control, and other automated systems that are most often found in the industrial sectors and critical infrastructure. These systems are used to operate physical processes in industries such as electricity, oil and gas, water, and critical manufacturing. Control system security in the electric power grid is particularly important because of the significant interdependencies inherent with the use of electricity in all other critical infrastructure sectors. In addition, operations of Federal, State, and local government rely on the electric grid. Therefore, assessing risk and effectively securing industrial control systems is vital to maintaining the Nation's strategic interests, public safety, and economic prosperity.

The CSSP currently partners with several Federal, State, and local agencies to provide analysis capabilities for technologies affecting control systems that impact the electric grid. Among these organizations are the Army Corps of Engineers, Department of Defense, Department of Energy, Department of Justice, Department of the Navy, Department of the Treasury, Department of Transportation, Environmental Protection Agency, Federal Energy Regulatory Commission, Nuclear Regulatory Commission as well as representatives from law enforcement and the intelligence community. These relationships provide reciprocal coordination on efforts as emerging technologies, and the cyber issues affecting critical infrastructure, are evaluated. Most importantly, the CSSP's Advanced Vulnerability Discovery facility, funded by DHS and housed at the Idaho National Laboratory, offers a world-class test environment where technical experts continuously evaluate nearly every major control system used in the critical infrastructure.

In 2006, DHS issued the National Infrastructure Protection Plan (NIPP) that identified the CSSP as responsible for coordinating activities to reduce the likelihood of success and severity of impact of a control systems cyber attack against CIKR sectors through risk mitigation activities. DHS recognizes that control systems exist across sectors and must be secured from cyber attacks, the effects of which could result in significant consequences. To address this, the CSSP has built a culture of reliability, security, and resiliency by partnering with government agencies, industry, and international entities to reduce the cyber risk to all 18 CIKR sectors. The CSSP leverages the risk management framework and partnership model described in the NIPP, which provides a mechanism for coordination among CIKR stakeholders, Government, and industry associations.

To assist public and private sector partners in identifying and mitigating the risks to their control systems, the CSSP provides leadership and subject matter experts through partnerships with key stakeholders. It develops recommended vulnerability mitigation strategies, practices, informational products, and assessment tools and delivers focused training. Recognizing that stakeholders must be involved in the process of identifying vulnerabilities and developing strategies to improve their security posture, the CSSP developed the first widely available control system cybersecurity self-assessment tool, which employs a systematic and repeatable approach for owners and operators to assess the security of their industrial control systems network. It also offers recommendations based on industry standards that are customized to the operating characteristics of each control systems facility.

While valuable products and tools such as these allow asset owners to understand the cyber risk to their control systems, it is also imperative that all stakeholders have a full understanding of the underlying fundamentals of control systems security. Consequently, the CSSP developed an advanced training center at the Department of Energy's Idaho National Laboratory that includes functional models of critical infrastructure equipment. This center provides hands-on training in a realistic, scenario-based environment. Since the program's inception, more than 14,000 professionals have received training through both classroom and web-based instruction.

To execute its mission and lead a cohesive effort between Government and industry, the CSSP created two overarching initiatives: The Industrial Control Systems Cyber Emergency Response Team (ICS–CERT) and the Industrial Control Systems Joint Working Group (ICSJWG). The ICS–CERT, in coordination with the United States Computer Emergency Readiness Team (US–CERT), is an operational entity that responds to and analyzes control systems-related incidents, conducts analysis on vulnerabilities and malicious software, or malware, and disseminates cybersecurity guidance to all sectors through informational products and alerts. The ICS–CERT provides more efficient coordination of control system-related security incidents and information-sharing with Federal, State, and local agencies and organizations, the intelligence community, private-sector constituents including vendors, owner-operators, and international and private-sector CERTS.

The ICSJWG follows a structured approach supported by the NIPP Partnership Framework and the Critical Infrastructure Partnership Advisory Council to continue the successful efforts of the Process Control System Forum to accelerate the design, development, and deployment of more secure industrial control systems. This group held its inaugural meeting on March 25, 2009 and is comprised of industry representatives from both Sector and Government Coordinating Councils under the NIPP Partnership Framework. The ICSJWG will provide a vehicle for communicating and partnering across all CIKR sectors among Federal, State, and local agencies, and private asset owner-operators of industrial control systems. CSSP engages through the ICSJWG with several Federal agencies on the issues of cybersecurity and industrial control, which include matters impacting legacy electric grid technologies and the enabling technologies used to deploy the "SMART GRID" systems. Departments and agencies participating in the ICSJWG include the Army Corps of Engineers, Department of Agriculture, Department of Defense, Department of Education, Department of Energy, Department of Health and Human Services, Department of Justice, Department of State, Department of the Interior, Department of the Navy, Department of the Treasury, Department of Transportation, Environmental Protection Agency, Federal Aviation Administration, Federal Energy

Regulatory Commission, Food and Drug Administration, National Institute of Standards and Technology, National Science Foundation, and the Nuclear Regulatory Commission as well as representatives from law enforcement (FBI, Secret Service) and the intelligence community.

DHS identifies vulnerabilities and works with the vendors, owners, and operators of control systems to develop mitigation strategies tailored to their use and application in each of the critical sectors. There can be a gap between identification of a vulnerability and development of a vendor patch or full solution. To address this, the CSSP has developed a Vulnerability Management Process operated by the ICS–CERT, in conjunction with trusted partners, to identify interim mitigation and consequence management approaches. CSSP also engages with other Federal partners in this process—such as the Departments of Defense and Justice and the intelligence community—to address equities and mitigate risks as vulnerability identification, risk assessment, mitigation development, and promulgation of these mitigation efforts are advanced.

(NPPD) FPS

Question 16a. The fiscal year 2010 budget request proposes the transfer of the Federal Protective Service (FPS) from Immigration and Customs Enforcement (ICE) to the National Protection and Programs Directorate, with level funding for FPS. FPS was previously transferred from the Government Services Administration (GSA) into DHS on March 1, 2003; a move that brought with it a number of management and contracting issues, as well as budgetary shortfalls. Even prior to the transfer, GAO noted in a 2004 report that GSA could not collect sufficient funds through fees to pay for FPS security services and had to provide FPS with supplemental funding from the GSA Federal building fund in order to cover the FPS deficits. Once under DHS, the Office of the Inspector General repeatedly identified poor contract oversight as another major issue for FPS, and a major cause of FPS' budget problems. In hearings held by this committee and reports to congressional appropriators, FPS identified methods of cutting costs that revolved around increasing fees, reductions in its staffing, and reductions in the hours those Federal employees work, but not in a reduction of contract guards.

Given that FPS has been plagued by problems with financial management throughout its time in the Department of Homeland Security, how does NPPD plan to address these issues?

Question 16b. Does NPPD project FPS to run a budget deficit in its first fiscal year under NPPD?

Question 16c. Does NPPD plan to continue cost-cutting measures for FPS? If so does NPPD plan to use the ICE model for cutting costs, or will it create its own plan to address the financial problems at FPS?

Question 16d. Does NPPD have a plan for improving the contract guard procurement process?

Answer. The National Protection and Programs Directorate (NPPD) is working with U.S. Immigration and Customs Enforcement (ICE) and the Federal Protective Service (FPS) to ensure FPS' critical operation and management functions continue without interruption during the transition. NPPD already uses ICE as its service provider for the accounting and financial system services. ICE will continue to provide these services to NPPD, and subsequently to FPS, if Congress approves its transition. NPPD is also evaluating FPS' processes and internal controls in the areas of budget and financial management. NPPD has already identified several improvements that will be implemented beginning in fiscal year 2010. Based on current cost and revenue projections, NPPD does not expect FPS to run a budget deficit next year.

NPPD is evaluating the operating costs of FPS to identify areas where there is insufficient funding. NPPD is also studying where funding might be better utilized for improved operations. NPPD is also evaluating the FPS staffing and workforce composition to ensure that FPS has the appropriate level and mix of Federal staff and contractors. NPPD is not considering cutting FPS operational staff. NPPD has identified FPS billing and collections as an area that can be staffed more effectively to provide better customer service. Additionally, NPPD is reviewing the historical amounts of outstanding FPS collections to determine if the collections process can be improved.

ICE and FPS are currently developing and implementing improvements in the areas of acquisition and contract oversight staffing, training, and policy development. ICE and FPS are also working on a number of standardization initiatives to address challenges in contract guard oversight and management. The proposed transfer of FPS to NPPD, if approved by Congress, will not delay or otherwise alter the steps currently being taken by ICE/FPS.

In addition, DHS is conducting a major coordinated review regarding the way forward with FPS in light of the recent GAO report. The DHS review will be provided to Congress in the next several weeks.

(NPPD) IP/RMA

Question 17. How are you expediting the security and suitability review process at NPPD? I hear that wait times for a clearance to be transferred can take as many as 6 months. Can Congress help expedite this process?

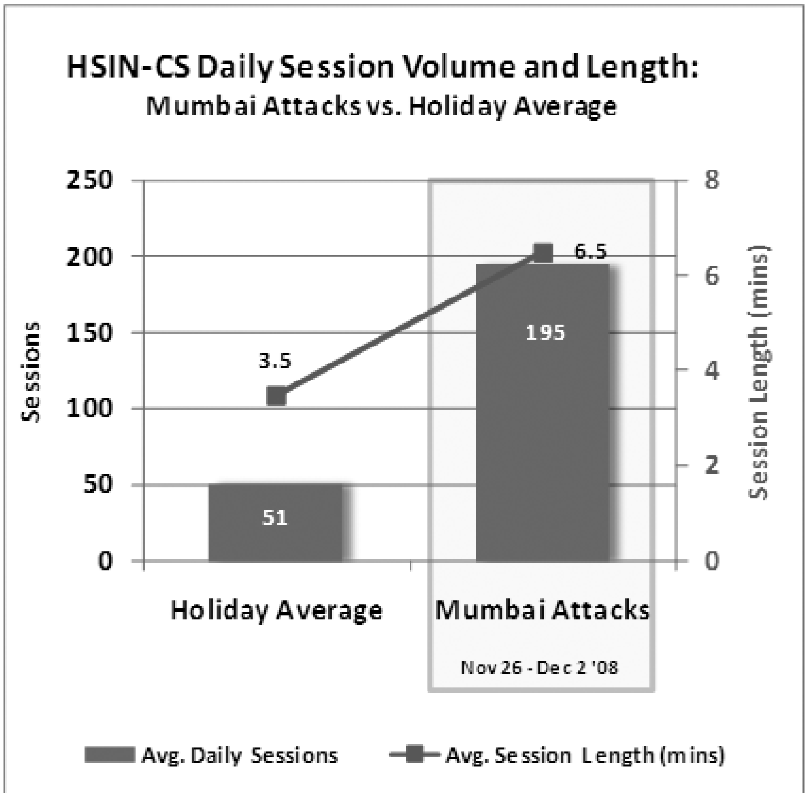
Answer. The National Protection and Programs Directorate (NPPD) faces many challenges in the security and suitability clearance processes. While we have made progress in on-boarding Federal employees, we still face a large backlog of people we need to bring on-board. However, we are working to increase the number of people assigned to the staffing process to expedite hiring. That said, work also remains to be done in reconciling the suitability process specific to the Department of Homeland Security (DHS) with the overall security clearance process. While this one instance of what NPPD is doing internally to accelerate the process, we are receiving assistance from DHS in improving the process.

The Under Secretary for Management is also committed to working with NPPD to resolve these issues, and we continue to work together to coordinate our efforts. For example, we implemented a system wherein NPPD is responsible for the initial steps in the clearance process, including inviting the candidate to access the on-line system to enter required information and loading candidate information into the Integrated Security Management Systems (ISMS), the Office of Security's tracking database. This has shortened the timeline form the issuance of a tentative job offer to the entry of personal data into ISMS, which initiates the background investigation. Additionally, the Office of Security no longer requires original signatures before initiating a background investigation. This will shorten the time associated with mailing original signatures and improve timeliness of decisions. Collectively, these changes should significantly impact the wait times for a clearance.

Question 18. In your testimony, you say that IP has "[p]rovided physical security and risk data to 5,000 registered Homeland Security Information Network-Critical Sector (HSIN–CS) users responsible for critical infrastructure . . . ." Our hearing on the Mumbai attacks in March revealed that DHS' response—in terms of outreach to the private sector—was hobbled and confused. Can you demonstrate the satisfaction of these users with HSIN–CS?

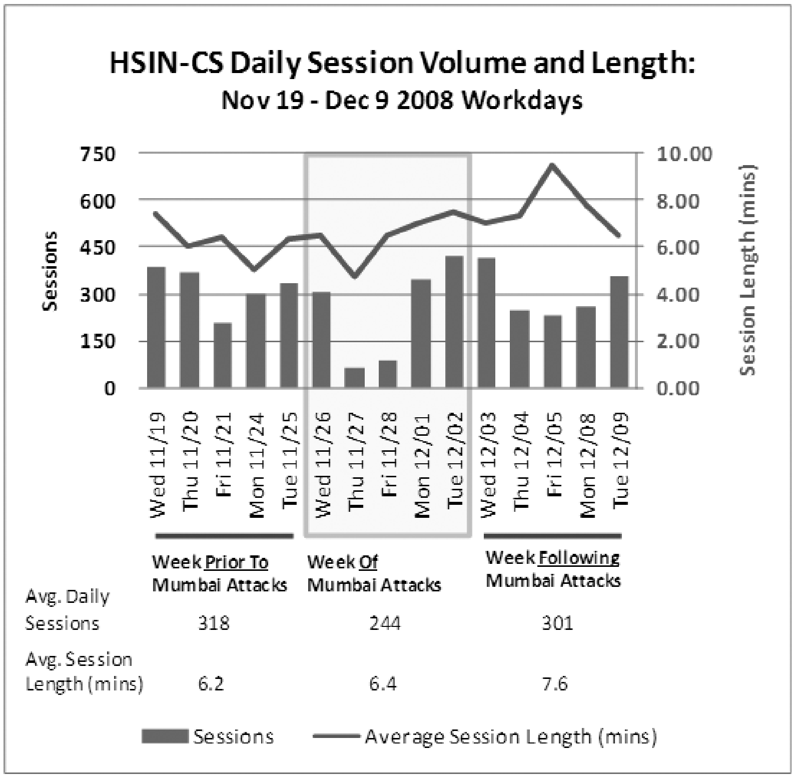
Answer. The Mumbai attacked occurred over the Thanksgiving holiday weekend on November 26–29, 2008. During the Mumbai attacks, DHS provided the private sector incident-related documentation and reports via the Homeland Security Information Network—Critical Sectors (HSIN–CS). HSIN–CS housed 26 documents related to the Mumbai attacks, including sector-specific vulnerability reports for the Transportation and Commercial Facilities sectors. Content also included post-incident analysis, protective measure reports, and future threat analysis. DHS posted the Office of Intelligence & Analysis' warning product, "(U//FOUO) Islamic Militant Group Attacks Multiple Locations in Mumbai, India" on HSIN. Once a clear picture of the attacks emerged after the initial chaos, products such as the Technical Resource for Incident Prevention's (TRIPwire) "Analysis of Mumbai Combined Arms Operation and Recommended Protective Measures" were posted.

As indicated in the graph below, during the week of the incident period (notably a holiday timeframe) stakeholders accessed HSIN–CS content 280% more (195 sessions/day) and remained on-line 86% longer (6.5 minutes) than is typical during a holiday. The length of a session reflects the user's interest in accessing relevant content.



The second graph below (HSIN–CS Daily Session Volume and Length: Nov 19–Dec 9 2008 Workdays) provides further context of HSIN–CS usage during the Mumbai attacks as compared to the weeks immediately before and after the incident.

As not all private entities in the Commercial Facilities Sector are registered users of HSIN–CS, DHS communicates using a variety of methods. The Commercial Facility SSA directly contacted private sector partners in the immediate aftermath of the Mumbai attacks, in particular the Lodging Subsector. The Commercial Facility SSA urged private sector partners to review their protective posture and electronically re-distributed awareness tools such as the “Active Shooter” materials (booklet, poster, wallet cards).



(NPPD) US–VISIT

Question 19. The committee understands that DHS has begun piloting two different biometric collection methods at airports for the US–VISIT program, one involving TSA at the checkpoint and the other using CBP officers at the gate. We are aware that the program has roughly $30 million in carry-over monies to use for the pilots, but we are concerned it may need additional funds. If the pilots indicate that the CBP or TSA collection methods are optimal, will you have the funding necessary to implement biometric exit in fiscal year 2009 or fiscal year 2010?

Answer. Approximately $28 million remains available from prior-year appropriations for testing technological solutions with pilot scenarios for the Biometric Exit project. The Department of Homeland Security (DHS) originally intended the collection of biometrics—with the costs involved—to be borne by the commercial carriers. DHS published this intent in a notice of proposed rulemaking (NPRM) in the Federal Register on April 24, 2009.

Congress included a provision in the *Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009,* that restricted DHS from obligating US–VISIT funds for a final comprehensive air exit solution until additional tests were completed. US–VISIT conducted pilot tests with the Transportation Security Administration (TSA) at the security checkpoint in the Hartsfield-Jackson Atlanta International Airport and with U.S. Customs and Border Protection (CBP) at the boarding gate in the Detroit Metropolitan Wayne County Airport. After a review within DHS, the results of the CBP and TSA pilot tests will be reported to the House and Senate Appropriations Committees and reviewed by the Government Accountability Office. Both pilots began on May 28, 2009, and concluded on July 2, 2009—a period of 35 days.

Based on the results of the pilots and comments to the NPRM, DHS plans to publish a final rule, tentatively scheduled for March 2010, which will direct the implementation of new biometric procedures for non-U.S. citizens departing the United States via airports and seaports.

If DHS goes forward with a final rule implementing the solution as stated in the NPRM—that commercial air carriers and vessel carriers will collect and transmit biometrics—no further funding would be required to implement Air/Sea Biometric Exit. If the evaluation and analysis of the air exit pilots recommend selection of a Government-operated option, such as CBP at the boarding gate or TSA at the security checkpoint, US–VISIT anticipates that additional funding will be required to implement such a recommended option. In that case, US–VISIT needs to develop a new cost estimate to determine the amount of additional funds required.

Question 20a. Last year's DHS appropriations bill required the Department to complete two biometric exit pilots at airports: (1) Where the airlines collect and transmit biometric exit data and (2) where CBP collects such information at departure gates. It is our understanding that the Department has yet to partner with any airline but that it has moved forward with the CBP pilot as well as an additional pilot performed by TSA personnel.

What can you tell the committee about the exit pilots currently being performed by US–VISIT?

Answer. US–VISIT conducted a pilot with Customs and Border Patrol (CBP) collecting biometrics at boarding gates at the Detroit Metropolitan Wayne County Airport in Detroit, Michigan, and another pilot with the Transportation Security Administration (TSA) collecting biometrics at a security checkpoint at the Hartsfield-Jackson Atlanta International Airport in Atlanta, Georgia. Both pilots began on May 28, 2009, and concluded on July 2, 2009—a period of 35 days.

CBP operated at the departure gate at Detroit Metropolitan Wayne County Airport. This pilot evaluated the operational impact of collecting biometric information from, and verifying the identity of, passengers at the departure gate before leaving the United States for a foreign destination. CBP collected biographic and biometric information from in-scope travelers near the departure gate. The biometric information collected consisted of electronic fingerprints: Either a right-hand, four-finger scan or two single-finger scans. The biographic information was collected from travel document information—such as name, date of birth, document issuance type, country, and document number—all of which are contained in the document's machine-readable zone of a machine-readable travel document.

CBP used two different biometric collection devices during the Air Exit pilots: The 3M RT mobile passport and ID reader; and the portable Cross Match Guardian R Jump Kit. CBP used both collection devices to determine which device type would better serve the needs of its collection staff. CBP followed its established reporting requirements regarding the air carriers and processes to minimize interference with the air carrier boarding process.

TSA operated at the security checkpoint at Hartsfield-Jackson Atlanta International Airport. This pilot evaluated the operational impact of collecting biometric information from, and verifying the identity of, passengers at TSA security checkpoints before leaving the United States. Those foreign passengers with an international destination were directed to an area within the checkpoint where the biographic and biometric information were collected. The biometric information collected consisted of two electronic single-finger scans. The biographic information was collected from travel document information—such as name, date of birth, document issuance type, country, and document number—all of which are contained in the document's machine-readable zone of a machine-readable travel document. TSA chose to use the 3M RT mobile passport and ID reader device for biometric collections.

A total of 34,485 transactions were collected from May 28 to July 1, 2009.[9] CBP collected 10,903, and TSA collected 23,582. Passengers were compliant and familiar with the process because of their experience with biometric collection and verification at ports of entry upon their entry to the United States. The results of this test are currently under evaluation at DHS.

Question 20b. What progress has DHS made in addressing the air carriers' concerns?

Answer. The Department of Homeland Security (DHS) officials reached out to the airline industry on numerous occasions to address its concerns and to identify poten-

[9] The biometrics were collected from passengers through July 1; none were collected on July 2, 2009. The processing of the collected biometrics through US–VISIT systems continued through July 2, and the decommissioning of the devices was completed that day. Thus the air exit pilots began on May 28, 2009, and were completed on July 2, 2009.

tial partners for biometric air exit pilot efforts. Despite on-going US–VISIT discussions with the Air Transport Association and its member carriers, no airline volunteered to participate in the biometric exit pilot required by the fiscal year 2009 DHS Appropriations Act. The airline industry made clear in many forums its concerns about DHS requiring the collection of biometrics by carriers.

Question 20c. If DHS is unable to complete the air carrier pilot, what will be the Department's next steps?

Answer. Based on the results of the exit pilot tests and the comments received from the notice of proposed rulemaking, DHS will determine which methodology for collecting biometrics best addresses the dual needs of security and facilitation. Once a solution is identified, DHS will publish a final rule and deploy the solution at the air and sea ports.

Question 21. Secretary Napolitano's Southwest Border Initiative calls for the installation of license plate readers on outbound lanes throughout the southwest border. These readers will be instrumental in controlling the exit of smugglers attempting to move drugs, weapons, and cash out of the country and into the hands of the cartels. What role, if any, will US–VISIT play in gathering and analyzing the exit information that is collected from the license plate readers?

Answer. US–VISIT does not play any role in gathering or analyzing the exit information that is collected from the license plate readers. The US–VISIT Arrival and Departure Information System (ADIS) is a person-centric system.

ADIS does not receive license plate reader information from U.S. Customs and Border Protection (CBP). However, ADIS is currently in a planning stage for creation of an interface this year with TECS, a CBP database to receive Western Hemisphere Travel Initiative/Vehicle Primary information.

QUESTIONS FROM CHAIRWOMAN SHEILA JACKSON LEE FOR GALE D. ROSSIDES, ACTING ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION

Question 1. The fiscal year 2010 request for air cargo security programs is less than the enacted fiscal year 2009 amount. Can you please explain this reduction in light of the upcoming August 2010 100% cargo screening deadline for cargo on passenger aircraft?

Can you describe how the budget is changing with respect to the number of inspectors, as well as the resources being allocated to certify shippers' screening facilities?

Answer. The fiscal year 2010 budget submission was built on the fiscal year 2009 enacted appropriation, which included a one-time increase of $18 million to expand air cargo screening technology pilots. The $18 million increase was not mandated to recur in the fiscal year 2010 budget. As a result, the fiscal year 2010 request of the Transportation Security Administration (TSA) was lower than its fiscal year 2009 enacted budget. The funds requested for fiscal year 2010 are adequate for TSA's current initiatives. Currently, TSA's workforce of 450 Transportation Security Inspectors for Air Cargo (TSI–C) cover air cargo operations at 121 main hub airports and their spoke operations. These inspectors provide inspection oversight, respond to air cargo related incidents, provide outreach and industry support, and conduct investigations into violations of security programs and regulations for 1,500 domestic and international carriers operating in the United States, and over 10,000 indirect air carriers. Considering the current number of regulated entities, TSA has adequate resources for fiscal year 2010.

TSA expects to issue an interim final rule this fall to meet the 2010 statutory deadline. The rule is expected to increase the number of regulated entities by approximately 8,000 as TSA certifies additional cargo screening facilities. It is important to note that it will take time to certify these facilities. After certification of all new regulated entities and upon full implementation of the Certified Cargo Screening Program (CCSP) in 2011, the current number of TSI–C will be re-evaluated to determine if additional TSI–C are needed to continue their current air cargo oversight mission as well as oversee the new CCSP program.

Question 2. In light of significant delays in issuing regulations and processing grant awards and applications, combined with the imbalance of expertise in surface transportation modes compared with aviation, why were there no funding or FTE increases requested for "Surface Transportation Security Operations and Staffing"?

Answer. The fiscal year 2010 budget request for the Transportation Security Administration (TSA) for surface transportation security includes an increase of $64,985,000 and 192 Full-Time Equivalents (FTE) over the fiscal year 2009 enacted levels for surface transportation security. The request includes a funding increase of 25 percent for "Surface Transportation Security Operations and Staffing", and would substantially expand TSA's field expertise in surface transportation security and capability to conduct joint security augmentation operations in the surface modes. Of the proposed increase, $50 million will be used to support an additional 15 Visible Intermodal Prevention and Response (VIPR) teams (comprised of 169 FTEs) to enhance the security of the Nation's surface transportation modes. The teams will be dedicated to conducting VIPR operations. In addition, the fiscal year 2010 budget request annualizes increases in the fiscal year 2009 surface transportation security appropriation made to further implement the 9/11 Act requirements. This includes the increase of 50 additional surface transportation security inspectors, and additional funding for exercises with surface transportation providers.

The responsibility for processing grant awards and applications relating to the Transit Security Grant Program (TSGP) lies with the Federal Emergency Management Agency, Grant Programs Directorate (GPD). GPD received funding in FEMA's fiscal year 2009 budget to hire additional FTEs. GPD is in the recruitment and selection process and plans to triple the size of staff managing this program by the end of the current fiscal year.

Question 3a. Last year, Assistant Secretary Hawley discussed Checkpoint Evolution as TSA's new way of modernizing checkpoints across airports. This initiative was started at the end of the previous administration. Outside of BWI, it does not appear that many of the elements have been implemented at other airports. What is the status of Checkpoint Evolution?

Has it been implemented across all airports?

Question 3b. What elements of Checkpoint Evolution provide TSA with metrics by which to measure enhanced security at airports?

Answer. Checkpoint Evolution was the term used to brand the approach to aviation security that the Transportation Security Administration (TSA) is implementing at airports across the country. While TSA included many discreet elements at Baltimore/Washington International Thurgood Marshall Airport (BWI) to accomplish as part of a security strategy, TSA is continuing many elements to evolve and enhance our security performance by developing our officers and leaders, fielding new technology, and adjusting the approach to deploying these assets to evolving threats.

The installation at BWI included a range of security elements, many of which have been developed for Nation-wide deployment. The following reports on the implementation of those elements throughout the TSA screening workforce:

- Enhancements for Employees:

  Over a 6-month period ending in April 2009, two training courses, developed to improve security and increase engagement with passengers, were given to the more than 50,000 front-line TSA employees. The response to the training classes called ENGAGE! and COACH! was overwhelmingly positive as officers leveraged their experience and used newly developed skills to calm down unruly travelers at checkpoints and better detect those with hostile intent.

  TSA has also improved the career development and employment of our Transportation Security Officers (TSOs) by increasing the Behavior Detection Officers (BDO) program, fully implementing training programs, and incorporating passenger engagement as part of our mandate to verify travel documents, which we assumed from the airlines. When officers demonstrate attentive, interactive, and appropriate command presence, a passenger's common, natural anxieties associated with the screening experience are calmed. Passengers who have hostile intent see engaged interactions as a threat to their goals, making their behaviors stand out and easier to detect by officers trained to spot anomalies. Engaged TSOs present a far more formidable opponent to those with harmful intent than technology and process can offer alone. TSA is also using our field intelligence officers, shift briefings, and other communication approaches to enable TSOs to perform their jobs efficiently and effectively.

  As we make strides to improve the professionalism of our officers, one aspect of that effort has been the conversion to new uniforms on September 11, 2008. These uniforms were developed to enhance the professional appearance of the screening workforce and to recognize their vital role in securing the Nation's commercial aviation system.

  TSA continues, through passenger feedback and surveys, to evaluate impact and public perceptions of security measures and officer performance. These internally and independently executed measures will provide additional information on security impact to which Evolution enhancements are a contributor.

- Enhancements to Process:

  One element of the Evolution training was to empower the TSOs to use their experience and intelligence-driven intuition to mitigate the threat by utilizing additional screening techniques described in the standard operating procedure (SOP) or by involving other members of their security network. This empowerment of critical thinking by the front-line officer is a key element of the dynamic security at the heart of Evolution.

- Enhancements to Technology:
  Additional technology solutions, such as imaging technology and Advanced Technology X-Ray were part of the BWI installation and continue to be rolled out at airports Nation-wide. Technology to help identify fraudulent documents was also deployed at the Travel Document Checker position. TSA has piloted and is now prepared for Nation-wide deployment of "wireless whisper" radio communications equipment to airport checkpoints. This technology will improve officer communication capabilities and reduce the background noise levels, allowing for enhanced threat detection and improved security. TSA also continues to pilot new technologies that enhance security and improve passenger movement through checkpoints, including mobile boarding pass scanners.
- Security Metrics:
  Completion and measured reinforcement of ENGAGE! training and principles should be viewed as a predictive measure for employee engagement and security effectiveness. Training completion rates and reinforcement efforts are actionable items that address known symptoms of security performance and effectiveness. Though they are lagging indicators, survey ratings, standardized performance assessments, ASAP results, Red Team results, TIP scores, absentee rates, attrition rates, numbers and types passenger complaints, numbers and types of Ombudsman contacts, numbers and types of disciplinary actions, numbers of behavior-initiated detections or security incidents, etc., can all be influenced by the delivery and application of ENGAGE! training and the consistent reinforcement of its principles. The principles taught in the Evolution training address the root causes of issues in all the lagging indicators listed above. Compliant delivery of Evolution training and principle reinforcement is a high-impact driver of performance in all aspects currently evaluated with lagging indicators.

TSA continually adapts to stay ahead of the threat. Other specific initiatives include:

- Capturing best practices by aggregating successful ideas for training sustainment and distributing them to other airports Nation-wide;
- Utilizing employee surveys, to determine the degree to which Evolution training principles have been adopted by the workforce; and
- Tracking of technology deployment, which will lead to enhanced detection and improved security.

Question 4. Please provide detail on the Secure Flight program implementation. There is very little in the budget request on this program, and the subcommittee would like assurance that TSA is budgeting appropriately for this program, as it should be completely implemented in fiscal year 2010.

Answer. The Transportation Security Administration (TSA) is pleased to report that Secure Flight implementation is currently underway and the fiscal year 2010 budget request contains sufficient funds to continue its implementation. Initial deployment began in late January 2009 with four aircraft operators. TSA continues to follow a structured implementation plan that systematically adds additional aircraft operators and flights as the program stands up in order to limit risk. Domestic implementation is scheduled to be completed by the end of the first quarter of calendar year 2010. International implementations will begin in late calendar year 2009 and are scheduled to be completed by the end of calendar year 2010. The fiscal year 2010 Secure Flight budget request supports the schedule of implementation activities during that period. Those activities include coordinated implementation with aircraft operators by government and contractor staff, operation and maintenance of the Secure Flight system/Secure Flight Service Center, and support for the Secure Flight IT systems development. They also include funding to support the high standards of privacy, security, Independent Validation and Verification, and other program management services required by the program. Aircraft operators covered by the Secure Flight final rule are required to modify their systems and procedures to send and receive Secure Flight passenger data within scheduled time frames that are keyed to the Secure Flight implementation schedule. There is no mandate to completely implement Secure Flight in fiscal year 2010. The TSA PLAN is to complete implementation by calendar year 2010 which the Secure Flight fiscal year 2010 budget supports.

Question 5a. According to GAO, the DHS Inspector General, and multiple stakeholders, the role, purpose, and activities of the VIPR program with respect to surface modes are ambiguous and often poorly communicated to relevant transit agencies. With the exception of surface inspectors, each of the components named in your written testimony has little to no role or expertise in securing surface modes. In fact, the program is housed and managed by an aviation security component, comprised almost totally by aviation security personnel, and lacks any defined objectives or meaningful performance measures specific to surface modes. Accordingly:

Please explain in detail how TSA determined that allocating virtually the entire increase in funding and FTEs for surface transportation security to the VIPR program is the best way to maximize these security resources, given the severe backlog of transit security grant awards and overdue regulations, as well as an understaffed surface inspection program.

Question 5b. Please explain how such an allocation of resources is consistent with a risk-based strategy for securing surface transportation systems and facilities.

Question 5c. Please explain the delay in submitting to the Committee on Appropriations the report on performance standards and resource allocation for the VIPR program, as required in the report accompanying the fiscal year 2009 Appropriations Act, and provide information on the status of that report.

Answer. The requested additional funding will specifically address the inherent vulnerabilities of our Nation's surface transportation systems and better position the Transportation Security Administration (TSA) to more readily and proactively perform its surface security mission as outlined in the 9/11 Act. With the requested funding, TSA plans to add an additional 15 Visible Intermodal Prevention and Response (VIPR) teams to be based in strategic locations throughout the country. Each of the dedicated teams will support a distinct region, which include airports and other transportation venues. This will allow the teams to be cognizant of their respective regional needs for enhanced security and law enforcement operations within the entire transportation domain, while allowing them to be scalable and flexible to respond and surge based on on-going threat streams. The full complement of dedicated VIPR Teams (25) will focus their efforts in the surface modes of transportation, consistent with the Secretary's vision for transportation security.

Working with the TSA's Office of Intelligence, the VIPR Program develops intelligence-driven deployment plans based on credible threat intelligence. Through the use of risk management principles, VIPR teams are deployed to implement flexible and nimble security operations at high-risk transportation assets. Utilizing the Department of Homeland Security (DHS) Risk Analysis Model, VIPR teams are deployed to surface and aviation modes to implement security operations at high-risk transportation sites. To date, the primary focus of these efforts has included the Focus 40 Airports (Category X and Category I), the identified 60 High Threat Urban Areas and the 20 High Threat Maritime Cruise Ship Ports.

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 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 occurrences of national or regional significance that raise security concerns. Use of VIPR teams in this manner builds a trained and tailored security augmentation capability for deployment in periods of heightened threat or in response to security incidents.

VIPR teams are deployed through deliberate planning using a risk-based approach to work with Federal, State, and local security and law enforcement officials for the purpose of augmenting resources in response to an intelligence-driven threat or to provide a deterrent presence. The program optimizes the ability to leverage a variety of resources quickly to supplement local aviation, passenger rail, cruise line and mass transit agency security capabilities.

VIPR allows TSA to respond quickly to unplanned or incident-driven events and execute its response and recovery capabilities. Most VIPR team activities are scheduled in advance to cover high-risk infrastructure, address intelligence-driven threats or support special event operations. These core elements dictate VIPR deployments across transportation sectors.

Although TSA recognizes that additional work is needed to complete hiring of its Transportation Security Inspector workforce, TSA's Office of Security Operations has been moving aggressively to perform the necessary recruitment. As planned, all inspector positions will be filled in fiscal year 2010 and these positions will be working as an integral component of VIPR deployment operations. TSA is also working with the Department and key stakeholders to address regulatory and grant management issues to provide additional security and efficiencies to the surface transportation domain.

Although earlier reports generated by Government Accountability Office and DHS Office of Inspector General have detailed issues regarding planning and execution of VIPR operations in collaboration with transportation stakeholder/partners, TSA has made great inroads with transportation stakeholder/partners all across the Nation and provides the bridge to all key components for VIPR operations. There have been over 1,600 VIPR operations conducted in the surface modes since inception. TSA now enjoys a robust relationship with its stakeholders/partners, State, local and international due to the proven capabilities that it brings to the enhancement of security and law enforcement capabilities at all transportation modes.

Transportation stakeholder/partners have reacted positively to the VIPR concept and often request TSA to augment their forces. TSA provides proactive public affairs information in locations were VIPR operations occur.

The fiscal year 2009 report to Congress regarding VIPR deployment and performance measures was recently submitted to the Senate and House Appropriations Committees on June 25, 2009.

Question 6. Earlier this year, GAO released a classified technology report highlighting some of the certification and deployment challenges faced by TSA regarding checkpoint technology. The report indicated that, since 2003, over $700 million has been invested in the development, procurement, and deployment of checkpoint technologies. What mechanisms are in place to ensure that adequate investments are made in technologies and that proper and timely certification, procurement, and deployment of checkpoint screening technologies are carried out by TSA?

Answer. The Transportation Security Administration (TSA) has developed a comprehensive Passenger Screening Program (PSP) that encompasses a collection of threat detection devices and projects in various states of exploration, development, and deployment based on commercial availability and program requirements. The program has a mixed lifecycle of technology to include legacy systems, systems in the process of deployment, and future systems that are undergoing testing and evaluation. The program focuses on deploying screening equipment with improved detection capabilities in addition to the lifecycle maintenance and replacement of existing (legacy) locations and equipment.

PSP continues to use a sound methodology to procure new emerging technologies. As a requirement of the Department of Homeland Security (DHS) Acquisitions Directive (AD) 102, projects are required to generate Life Cycle Cost Estimates (LCCEs) based on known and estimated costs that are presented at prescribed instances, known as Acquisition Decision Events (ADEs), to the proper reviewing authority along with documentation displaying the benefits of the technology. On an annual basis, the PSP participates in both TSA and DHS Acquisition Review Boards to review specific project costs and benefits.

The Program works with the respective stakeholders to develop a tailored plan for each project that identifies primary objectives, risks, as well as schedule and execution strategies for the procurement and deployment of technology. To that end, the PSP must be flexible and able to adapt quickly to changes in terrorist tactics. The PSP strives towards optimizing technological investments based on thorough analysis and risk management principles, as well as the collaborative testing and evaluation of new technologies.

The PSP has implemented a formal testing process as documented in our Test and Evaluation Master Plan (TEMP), which establishes a framework of the testing processes followed for all PSP technology investments to ensure products meet specifications, are safe and are operationally effective. TSA is in the process of improving the already robust Testing and Evaluation (T&E) paradigm to ensure that operational effectiveness and suitability of candidate security technology systems are evaluated prior to deployment. Employing the concept of independent and integrated testing and evaluation in support of acquisition decision events and other program reviews, this process leverages data from multiple developmental and operational testing sources, accredited vendor data, modeling and simulation, and other special analyses (as required), in accordance with testing and evaluation and systems engineering principles and best practices, to streamline testing and evaluation requirements while still providing a credible and comprehensive evaluation product.

The deployment team has been increased and structured into a regional paradigm with specialized knowledge of each respective region and the attendant airport requirements for permitting and other deployment logistics. Deployment Planning and Execution is organized across three regional areas (East, Central, and West). The deployment process makes use of the integrated product team (IPT) approach to develop strategies, monitor overall performance and achieve deployment program goals.

Question 7a. On June 2, 2009, committee staff received an announcement from TSA indicating that TSA is "currently denying air service by Delta to Nairobi and Monrovia until security standards are met or security threat assessments change." What steps did TSA take to reach this decision?

Did you engage Delta throughout your decisionmaking process?

Question 7b. When was Delta informed of your decision to deny air service to Nairobi and Monrovia?

Answer. The Transportation Security Administration Representative (TSAR) for Africa and a team of TSA inspectors completed a comprehensive security assessment of Roberts International Airport (ROB) in Monrovia, Liberia and Jomo Kenyatta International Airport (NBO) in Nairobi, Kenya. TSA also conducted a Man Portable Air Defense Systems (MANPADS) Assistance Visit of NBO and worked with the U.S. intelligence community to develop a full understanding of the terrorist threat to civil aviation in Africa.

Upon completion of these initial airport assessments of NBO and ROB, the TSA Office of Global Strategies (OGS) led a TSA Integrated Product Team (IPT) that included representatives from TSA's Offices of Intelligence (OI), Law Enforcement/Federal Air Marshal Service (OLE/FAMS), Transportation Sector Network Management (TSNM), and Chief Counsel (OCC), to ensure that a thorough evaluation of security conditions was performed, training and assistance provided, and additional security measures implemented, as appropriate.

TSA is continuing to work with the Liberian Civil Aviation Authority to assist it in achieving compliance with international security standards, and with the Kenyan Civil Aviation Authority to address identified security vulnerabilities and implement mitigating measures. TSA will reassess the situation at ROB and NBO as appropriate measures are implemented.

TSA actively engaged Delta Air Lines representatives throughout the decision-making process. TSA OGS senior leadership met with Delta Air Lines corporate senior security officers on several occasions at TSA Headquarters, including on December 11, 2008, January 6, 2009, April 2, 2009, and April 30, 2009.

TSA's decision to deny Delta's proposed air service to NBO and ROB was communicated to Delta Air Lines on June 1, 2009, based on TSA's determination that security was not yet adequate to allow these airports to be served. On April 2, TSA briefed Delta Air Lines on the observations made by the security inspectors at ROB, and on April 30, a similar briefing was provided to Delta regarding the observations made by the security inspectors at NBO. During each of these meetings, TSA advised Delta Corporate Security officers that while a final decision would be made by TSA's Acting Assistant Secretary, in consultation with Secretary Napolitano, the TSA IPT was recommending that Delta not initiate service to ROB or NBO due to identified security deficiencies and/or assessed security concerns.

Question 8. DHS, and specifically TSA, has had significant challenges in its acquisition process, notably in the Secure Flight Implementation, Business Operation (IBO) program, and the Information Technology Infrastructure Program (ITIP). What steps have you taken to ensure that TSA is progressing and improving its acquisition process to ensure that procurements are done efficiently and competitively, and that there is integrity in the process?

Answer. The Transportation Security Administration (TSA) has confronted many acquisition challenges since its founding only 7 years ago. However, TSA takes competition and the integrity of its procurements very seriously. The Secure Flight Implementation and the Business Operation (IBO) and Information Technology Infrastructure Program (ITIP) are competitively awarded procurements. They represent a significant advancement and evolution in acquisition strategy. For example, the ITIP effort evolved into a performance-based service acquisition, in which the scope of the predecessor contract was separated into multiple fixed-priced acquisitions instead of a time and materials contract. While difficult and challenging, this strategy provides for better performance measurement, and the ability to incorporate best industry practices.

TSA has made significant strides to establish processes and procedures to ensure consistent, efficient, and effective acquisitions. TSA exceeded the competition goal established by the Department of Homeland Security Chief Procurement Officer by awarding 71 percent of all contract dollars on a competitive basis. In fiscal year 2008, TSA awarded 1,100 contracts and only 12 protests were submitted to the Government Accountability Office. Also, TSA awarded over 20 percent of all contract dollars to small businesses. All of Tier 1 and 2 (TSA's largest programs) have certified Program Managers and Contracting Officer's Technical Representatives. TSA has pursued several initiatives to improve the acquisition process including: (1) Implemented several initiatives to ensure the TSA acquisition workforce has the appropriate skills; (2) completed an exhaustive lean six sigma effort to identify, document, and improve the efficiency and effectiveness of acquisition processes; (3) instituted a phased review program, in which procurements are reviewed prior to solicitation and award and after execution; and implemented an aggressive small business program which has produced marked improvement in awarding contracts to small business.

(TSA) AVIATION

Question 9a. Earlier in the Congress, the House unanimously passed H.R. 559, FAST Redress Act of 2009. The legislation required the Department of Homeland Security to develop a "comprehensive cleared list" which will enhance the overall efficiency and effectiveness of the DHS Traveler Redress Program. The President's budget has requested $1.3 million and 1 FTE for the management of the program.

How will the additional funding and staffing allocation improve the overall effectiveness of the program?

Question 9b. Additionally, the President's budget discusses the "centralization of the DHS TRIP processing system"; could you please expand on what this "centralization" entails and how it will work with Secure Flight in the future?

Answer. The Department of Homeland Security (DHS) Travel Redress Inquiry Program (DHS TRIP) serves as the centralized U.S. Government customer service office for traveler-related redress concerns. While the program office has made substantial progress in establishing a robust redress process, it can enhance performance further through centrally automating key process functions—such as inquiry intake, routing, vetting, tracking, reporting, and response. The objective is to gain operational efficiencies and to reduce the overall time required to process traveler requests. The fiscal year 2010 budget will accomplish this objective through investing in DHS TRIP technology and staffing capabilities.

DHS plans to direct over half of the requested funding toward Information Technology (IT) improvements for DHS TRIP through an enhanced case management system. This case management system will leverage lessons learned since the launch of DHS TRIP in February 2007 to centralize and improve inquiry intake, routing, tracking, reporting, and response functions. DHS plans to direct the remaining funding and its staffing allocation to develop and implement additional enhancements (i.e., call center support and an improved vetting process) that will strengthen customer service. These investments will also allow DHS to expand redress support to non-travel related watchlist vetting programs in the Department, supporting DHS's objective of reusing redress results across vetting programs.

These IT improvements will allow programs such as Secure Flight to use the results of the redress process more effectively to reduce occurrences of misidentifications during vetting. DHS TRIP currently provides a listing of cleared individuals to the airlines and to Secure Flight to assist in the watch list matching process. This cleared list contains individuals for whom the redress process has determined are not on the watch list but may be prone to misidentification due to the similarity of their names and biographic information to records in the watch list. Once the new DHS TRIP IT system is implemented, Secure Flight (as well as other DHS vetting programs) will benefit by receiving automated inquiry updates of cleared individuals on a more frequent basis and in a more efficient format. As a result, DHS can better prevent future inconveniences to misidentified travelers.

Question 10a. Throughout meetings between committee staff and TSOs, a number of concerns have been raised on TSA's ability to provide adequate training for all TSOs who may need recurrent training on certain technologies at checkpoints. Additionally, TSOs indicated that very few of them were cross-trained to serve in more than one position at an airport checkpoint.

How is TSA able to verify that appropriate recurrent training is made available to TSOs who need it at any given time?

Question 10b. Additionally, does TSA cross-train TSOs to be able to serve multiple positions at checkpoint? If so, what percentage of TSOs is trained to serve multiple locations at a checkpoint?

Answer. The Transportation Security Administration (TSA) has established an annual National Training Plan. Specific recurrent security training courses are loaded into the learning plans of all Transportation Security Officers (TSO) on the On-Line Learning Center (OLC). TSOs are required to complete this training to ensure they maintain proficiency of skills learned during basic training. Additionally, the recurrent courses are designed to keep the workforce up-to-date with procedural changes; build upon existing skills and abilities, new technologies introduced into the screening operations; equipment used by the TSOs in the performance of their duties; and, new threat items. Recurrent training is available via web-based training on the OLC, through instructor-led classes, and hands-on training at the checkpoint. Additional training can be assigned to TSOs by the field training staff to target TSOs' individual training needs (e.g. X-Ray Image Interpretation).

All TSOs must participate in an Annual Proficiency Review to ensure that they meet the qualifications and performance standards required to perform their duties as set forth under the Aviation and Transportation Security Act (ATSA). TSOs are certified annually based on their overall annual performance as defined by the Performance Accountability and Standards System (PASS). One of the components of PASS is that TSOs must complete all assigned training. Training is recorded and tracked through the OLC.

TSOs are trained to perform checkpoint screening functions, checked baggage functions or both. TSA does not have multiple positions at the checkpoint, but multiple functions. TSOs rotate and perform the various functions. Upon successful completion of Basic Screener Training and On-the-Job Training, as well as achievement of passing scores on all tests associated with this training, 100 percent of the TSOs certified to perform checkpoint screening functions can perform each of those functions, therefore, no cross-training is required.

The TSO workforce is comprised of 16,980 TSOs who can perform all checkpoint screening functions; 5,626 TSOs who can perform checked baggage screening functions, and 23,753 TSOs who can perform both checkpoint and checked baggage functions.

Question 11. Last year, Assistant Secretary Hawley discussed Checkpoint Evolution as TSA's new way of modernizing checkpoints across airports. This initiative was started at the end of the previous administration. Outside of BWI, it does not appear that many of the elements have been implemented at other airports. What is the status of Checkpoint Evolution, has it been implemented across all airports? What components in Checkpoint Evolution provide TSA with metrics in which to measure enhanced security at airports?

Answer. Response was not received at the time of publication.

Question 12. So much of the aviation security budget is geared towards passenger checkpoint and baggage screening. Please provide us with an explanation as to how the agency will balance the need to quickly roll out new technologies against the realistic budgetary constraints that force TSA to prioritize how new checkpoint and baggage screening equipment is allocated at airports.

Answer. The Transportation Security Administration's (TSA) Passenger Screening Program (PSP) has been aggressively engaged in the national deployment of new technologies at the screening checkpoint. The defined strategy of deploying to high-risk, high-volume airports is used to prioritize and determine when each airport will receive the new technology. PSP has gained and implemented a host of best practices from the recent deployments of Advanced Technologies (ATs) and passenger imaging technologies. The preparations for the accelerated deployments have been predicated upon these best practices. The deployment team has been increased and structured into a regional approach with specialized knowledge of their region and the various airport requirements for permitting and other deployment logistics. There has been dedicated space identified at the Technology System Integration Facility for the swift and massive undertaking to provide daily monitoring and teaming of the upcoming deployments. Site designs are already in the process of being drawn up in anticipation of the accelerated deployments thereby shortening the time required to plan and install. Finally, there is a streamlining of the contract vehicle for deployments with the single systems integrator contract currently under competition.

Question 13. In fiscal year 2010, for Explosives Detection Systems (EDS) purchase and installation there is $250 million in mandatory spending from the 9/11 Act, $856 million for discretionary spending in the fiscal year 2010 budget request, and also $700 million in Recovery Act funding. Can you please give the committee a perspective on how this money will be allocated and prioritized in deploying these systems at airports Nation-wide?

Answer. The additional funding from the American Recovery and Reinvestment Act and fiscal year 2010 budget request will enable the Transportation Security Administration (TSA) to accelerate its implementation of the Electronic Baggage Screening Program (EBSP). As stated in the American Recovery and Reinvestment Act (ARRA) expenditure plan, the additional $700 million will shorten the timeline of full optimal system deployment by up to 2 years. The initial ARRA spend plan included 16 EDS aiport projects to receive the first infusion of ARRA funds. Per congressional direction, quarterly updates addressing ARRA spend plan changes and fiscal year 2009 appropriation changes will also be submitted to Congress.

Funding considerations for the EBSP include: Program Operations and Management (O&M), previously committed multi-year agreements for facility modifications, purchase and install of explosives detection systems equipment, new terminals, compliance, fulfilling existing agreements, equipment for new projects, new funding for facility modifications, and technology/engineering initiatives. In developing the spend plan, TSA first considers the funding needed to keep the organization operating—the Program O&M costs. Next, TSA identifies the funding required for previously committed multi-year agreements. Then funding is identified for the purchase and installation of this equipment to fulfill existing agreements, equip new terminals, address compliance issues, and include new projects not requiring facility modifications. TSA tries to accommodate all of these projects since they are required for 100 percent compliance of the requirement to screen all checked baggage for explosives, fulfilling previous agreements, equipment-only requests, and new terminal operations. With any remaining funds, TSA will prioritize facility modification requests and balance those with technology and engineering initiatives for system improvements and cost management opportunities.

Question 14. The overall number of Transportation Security Officer FTEs remains about the same in the fiscal year 2010 budget request as in previous years with just under 46,000 personnel. At the same time, more of these FTEs are performing specialized functions such as Behavioral Detection and Travel Document Checking. Please explain how you determine what the right amount of passenger and baggage screeners is for the current volume of passenger traffic, and how shifting more personnel into other specialized security roles impacts traditional passenger and baggage screening.

Answer. The Transportation Security Administration (TSA) utilizes a discrete event simulation commonly known as the Staffing Allocation Model to determine base staffing requirements for baggage and passenger screening activities. The inputs for this model includes multiple variables such as an airport's physical configuration, flight schedules, passenger volumes, and type and number of screening equipment on hand. This level of detail ensures staffing allocations are molded to the demand and are sufficient to cover all operations. Furthermore, field engineers and workforce utilization experts conduct routine analyses to verify that the model inputs remain accurate throughout each year. Shifting personnel into specialized security roles has no adverse effect on the traditional passenger and baggage screening, and improves our overall security posture. TSA has become more efficient in its utilization of resources and technology. The shifting of resources was not done at the expense of passenger and baggage screening, but rather as a result of increased efficiencies identified through the use of advanced technologies along with improved resource utilization.

Question 15. The fiscal year 2010 budget contains a modest increase over last year's enacted amount for Transportation Security Officer training programs. Please highlight where TSA intends to focus with respect to allocating training resources. Can you say that TSOs have access to appropriate facilities at work to participate in training? Have you heard any complaints from the TSO workforce about training issues, and if so, have there been any corrections or improvements made in this area?

Answer. With the rapid pace of change and implementation of new concepts, demographic challenges, and enabling technologies, the Transportation Security Administration (TSA) constantly seeks to improve ways to help the security workforce be successful on the job with the right knowledge and skills. Therefore, acquiring and using emerging technologies and innovative ways to deliver training is critical to the success of the mission.

We recognize that training space constraints continue to be a challenge, and we continue to provide off-site space to address space restrictions at many airports. Although Transportation Security Officers (TSOs) may not have immediate access to training at the checkpoints, appropriate facilities are available at every airport for TSOs to complete training.

Question 16. There is a modest increase in the fiscal year 2010 budget request for Aviation Regulation that includes the inspection programs for international programs, repair stations, and the canine training program. Given the upcoming cargo-screening mandate, can you say that the regulatory programs are adequately resourced?

Answer. The fiscal year 2010 budget request by the Transportation Security Administration (TSA) provides adequate regulatory oversight resources to screen 100 percent of passenger cargo originating at U.S. airports.

Question 17. The budget very briefly states in the Tort Claims section that TSA screens over 50 million bags per month and reimburses passengers that have experienced baggage loss or damage due to TSA negligence. Please describe how this process is working in terms of outstanding and adjudicated claims.

Answer. In fiscal year 2008, the Transportation Security Administration (TSA) received and adjudicated approximately 17,600 claims, 19 percent of which resulted in payments to the claimant. In fiscal year 2009, through June, TSA has received just over 10,000 claims. Fiscal year 2009 payment percentages remain consistent with fiscal year 2008. TSA is processing claims within the 6-month deadline established by the Federal Tort Claims Act, with the exception of certain special cases, such as claims that are in litigation. As of the end of June 2009, TSA had 2,666 claims under adjudication (i.e., outstanding). Of these claims, over 80 percent have been received since May 1, 2009.

(TSA) SURFACE TRANSPORTATION

Question 18. Please explain the reasoning behind the allocation of surface transportation security resources toward the VIPR program, including whether any Federal entities (such as GAO or the DHS Inspector General) or non-Federal stakeholders were consulted about surface transportation security priorities, and whether any new surface-focused components are envisioned for VIPR teams devoted to surface activities.

Answer. The requested additional funding will specifically address the inherent vulnerabilities of our Nation's surface transportation systems and better position the Transportation Security Administration (TSA) to more readily and proactively perform its surface security mission as outlined in the 9/11 Act.

Through Visible Intermodal Prevention and Response (VIPR), TSA teams State and local agencies with additional Federal Air Marshals (FAMs), Transportations Security Inspectors—Surface, Behavior Detection Officers, and Bomb Appraisal Officers. Each element brings expertise to the surface modes of transportation in a collaborative effort to deter, disrupt, and defeat possible terrorist or criminal actions towards the Nation's transportation system. Utilization of these assets has been proven effective through the collaborative deployment of over 1,600 VIPR operations in the surface modes using existing resources not specifically dedicated to VIPR operations. Dedication of these assets will create an even greater deterrence and public awareness to the surface transportation domain, especially given the enhanced level of coordination and communication that now exists between TSA and its VIPR partner agencies.

For example, all of TSA's operational components collaborate on plans to deploy VIPR resources in the surface transportation domain and TSA's Office of Transportation Sector Network Management meets regularly with its stakeholder/partners, collaborating on best practices to secure the transportation domain. TSA's transportation stakeholder/partners provide necessary and regular feedback and input into the plans TSA proposes for future VIPR operational deployments and this relationship has strengthened considerably since the Government Accountability Office and the Department of Homeland Security Office of Inspector General audits. Moving forward, TSA expects these working relationships to continue to improve at a national level, particularly if additional resources are made available to support the VIPR program as requested in the President's budget.

Question 19. Please explain why only 18 additional canine teams are supported by the budget request for surface transportation, and why some of those teams are targeted for the ferry sector rather than rail and transit activities.

Answer. The Transportation Security Administration's (TSA's) funding of an additional 18 canine teams for surface transportation security represents an appropriate allocation of resources within the TSA budget. These teams will be under the control of local law enforcement responsible for surface transportation security in their respective jurisdictions. This is in addition to 82 canine teams in the National Explosive Detection Canine Team Program (NEDCTP) that are already dedicated to surface transportation security. The NEDCTP will continue to monitor its budget during fiscal year 2010 to determine if additional surface canine teams can and should be funded.

With respect to ferry teams, NEDCTP worked with other offices within TSA to identify surface transportation security requirements, which included ferry systems. The NEDCTP based its decisions for team locations on system-wide surface transportation security needs, deployment requirements, and overall concept of operations. Ferry systems were chosen based on passenger ridership and U.S. Coast Guard risk management data.

Question 20. Please clarify what is happening to the First Observer program. This program is supported by the Trucking Security Grant Program, which is targeted for termination; yet, the budget justification for TSA's request with regard to surface transportation security states that the Highway Information Sharing and Analysis Center (ISAC) will be continued through fiscal year 2010. The ISAC is part of the First Observer Program, which, as noted, is supported by the trucking grants. How is this program going to continue if the source of its funding is being eliminated?

Answer. The First Observer program was funded for $15.5 million by the fiscal year 2008 Trucking Security Program (TSP) grant, which has a 36-month period of performance. The HMS Company was awarded the fiscal year 2008 TSP grant for the First Observer program, and it developed its budget, which includes funding for the Information Sharing and Analysis Center (ISAC) for 41 months from the date of award. The grant award date was July 15, 2008 and the period of performance is August 1, 2008 through December 31, 2011. Therefore, the Information Sharing and Analysis Center will continue to operate through December, 2011, funded by the fiscal year 2008 TSP grant.

Question 21. Does the "inter-modal security training and exercise program" referenced in your written testimony and the budget justification include the outstanding training regulations for transit, rail, and bus workers required under the 9/11 Act? Where is it housed within TSA? And for the purposes of this program, does "inter-modal" include aviation? Please explain how this budget request reflects the importance of supporting TSA's regulatory functions to address the long delays in issuing these critical security regulations.

Answer. Three sections of the *Implementing Recommendations of the 9/11 Commission Act of 2007* (9/11 Act) require the establishment of a program for conducting security exercises for public transportation agencies, railroad carriers, and over-the-road buses. The Transportation Security Administration (TSA) has developed the Intermodal Security and Training Exercise Program (I–STEP) under the auspices of the TSA Office of Transportation Sector Network management (TSNM) to provide these exercises. The intermodal programs under the I–STEP do not include aviation.

The I–STEP Program does not address the development of regulations calling for security training for frontline employees in certain modes, as required by the 9/11 Act. TSA is actively developing regulations to fulfill these requirements. Once these regulations are issued as final rules, I–STEP will reinforce the training standards during exercises. The funds needed for continued regulatory development are included in the fiscal year 2010 budget request.

Question 22. In your written testimony you reference the International Working Group on Land Transport Security and state that TSA is engaged with that organization to promote best practices, capacity building, and information sharing. Please describe all of TSA's activities with respect to the International Working Group, and elaborate on how this budget reflects the significance of those activities.

Answer. The United States proposed the creation of an international land transport security working group at the Japanese Ministerial Conference on International Transport Security in January 2006. The purpose was to create a forum within which the international transportation security community could improve land transport security by sharing best practices, enhancing cooperation between government authorities and industry, and sharing technology information. Three years after its inception, members now include: Australia, Canada, China, the European Commission, France, Germany, India, Indonesia, Israel, Italy, Japan, Malaysia, Netherlands, Philippines, Republic of Korea (South), Russia, Spain, United Kingdom, and the United States.

The Transportation Security Administration (TSA), hosted the 4th and 5th International Working Group on Land Transport Security (IWGLTS) sessions on behalf of the United States. During the 4th session in November 2008, the following priorities for IWGLTS were agreed upon by the participating States: (1) Information sharing as an overarching theme and the No. 1 priority; (2) creating a compendium of smart practices; further developing the secure web board for IWGLTS efforts; (3) conducting inter-sessional work; and (4) reaching out to other organizations (e.g., International Union of Railways—UIC) to maximize efforts; and conducting a survey of members' current and planned technologies in land transport security.

Identifying specific deliverables within the previously agreed-upon priorities (Mitigation Activities, Risk Assessment, Technology, Public Awareness and Stakeholder Partnerships), prioritizing and deciding which deliverables will be pursued before the 6th Session, and identifying leads/co-leads for each deliverable for work to begin during inter-session periods were accomplished at the 5th session in May 2009. IWGLTS members not only identified, prioritized, and committed to several deliverables, but also began establishing timelines and planning inter-session efforts for the following activities: (1) Conduct a survey of members' mitigation security measures for land transportation modes—U.S. lead; (2) conduct a survey of members' current/future land transport security technologies—Australia lead; (3) develop a risk assessment matrix of land transport modes—France lead; and (4) develop presentations and discussion on Public Awareness campaigns (India, Indonesia, and United States will present at the next IWGLTS meeting)—U.S. to coordinate during inter-session periods.

SMALL BUSINESS

Question 23. As of June 22, 2008, TSA was no longer exempt from complying with the Federal Acquisition Regulation. How has this change impacted minority-owned, woman-owned, and veteran-owned businesses?

Answer. Although mandated to comply with the Federal Acquisition Regulation since only June 2008, the Transportation Security Administration (TSA) has been a strong advocate for small business since its inception and has developed a strong and robust small business program. Prior to 2007, TSA developed internal management directives and processes based upon acquisition best practices to ensure small business participation. In 2007, TSA was required to comply with the Small Business Act. In fiscal year 2008, TSA awarded over 20 percent of contract dollars to small businesses, an increase of 5.3 percent from fiscal year 2003. In addition, TSA awarded 6.7 percent of contract dollars to small disadvantaged business, exceeding the goal of 5 percent. TSA also awarded 2.6 percent of contract dollars to small businesses owned by disabled veterans.

Question 24. In order to receive grant funding from TSA, do State and local governments that plan to utilize funds in a competitive manner have to comply with any Federal rules/regulations on minority business or disadvantaged business utilization?

Answer. The Transit Security Grant Program (TSGP) Grant Guidance and Application Kit that is published for each grant cycle includes language on Disadvantaged Business Requirements. Both the fiscal year 2009 TSGP Guidance (page 49) and the fiscal year 2009 American Recovery and Reinvestment Act TSGP Guidance (page 53) state “Applicants are advised that, to the extent that recipients of a grant use contractors or subcontractors, such recipients shall use small, minority, women-owned or disadvantaged business concerns and contractors or subcontractors to the extent practicable.”

○