

Statement for the Record

**Philip Reitinger
Deputy Under Secretary
National Protection and Programs Directorate
United States Department of Homeland Security**

**Before the
United States House of Representatives
Committee on Homeland Security
Transportation Security and Infrastructure Protection Subcommittee**

June 10, 2009

Good afternoon, 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 (FY) 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 FY 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 FY 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 FY 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 FY 2009 positions. We are projecting bringing on board another 200 by the end of FY 2009. The FY 2010 budget request includes 350 additional Federal staff across the entire Directorate offset by funding decreases in contractor support funding. The FY 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 FY 2010.

I would now like to highlight some NPPD accomplishments as well as review the FY 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

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.

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 FY 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 FY 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 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 online 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 - 1612; and Tier 4 - 3940. 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 FY 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 FY 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 FY 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 6 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 FY 2010 budget request for RMA is \$9.9 million and includes 25 Federal staff. Major programs planned in FY 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 FY 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 FY 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 (NCS) assessed over 4,000 current external internet connections in the .gov domain and identified approximately 80 of those as consolidated internet access points.
- NCS 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 Statewide Communications Interoperability Plans.

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

- The FY 2010 request for the NCS is \$400.7 million.
 - This request includes an increase of \$75 million from FY 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 word national cyber security threats and apply effective analysis and risk mitigation strategies to detect and deter threats. NCS will support the ongoing reduction and consolidation efforts of external Federal access points, enabling more effective monitoring and alerting on suspicious activities occurring across the Federal enterprise.
 - The NCS request also includes an additional \$15 million to enhance outreach and coordination across all levels of government and the private sector. The FY

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 FY 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. NCS 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 FY2010 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 FY 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 Statewide Communication Interoperability Plan workshops.

OFFICE OF THE UNDER SECRETARY

The FY 2010 budget request includes \$34.7 million and 104 Federal positions for Directorate Administration and the Office of the Under Secretary. Priorities for FY 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 FY 2010 and look forward to answering any questions you may have.