

**Statement for the Record
of
Rand Beers
Under Secretary
and
Philip Reitinger
Deputy Under Secretary
National Protection and Programs Directorate
Department of Homeland Security**

**Before the
United States House of Representatives
Committee on Appropriations
Subcommittee on Homeland Security
Washington, DC**

March 31, 2011

Introduction

Chairman Aderholt, Vice Chairman Culberson, Ranking Member Price, and distinguished Members of the Subcommittee, it is our pleasure to appear before you today to present President Obama's Fiscal Year (FY) 2012 Budget Request for the Department of Homeland Security National Protection and Programs Directorate (NPPD).

The demands on NPPD have never been greater as we lead efforts to enhance the security of the Nation in partnership with the private sector and all levels of government. The services we rely on for daily life are heavily dependent on critical infrastructure. Threats and vulnerabilities put the availability and protection and resilience of these services, such as water distribution and treatment, electricity generation and transmission, healthcare, transportation, and financial transactions, at risk. The NPPD FY 2012 budget request allows us to continue to meet these evolving threats and challenges by prioritizing funding and personnel to our essential operational requirements—while demonstrating a commitment to fiscal discipline that maximizes the effectiveness of every dollar we receive.

FY 2012 Budget Request

The FY 2012 budget request for NPPD is \$2.6 billion in gross discretionary funding, and \$1.3 billion in net discretionary funding. The Federal Protective Service is funded through an estimated \$1.3 billion in offsetting collections from other agencies. NPPD supports the following Quadrennial Homeland Security Review (QHSR) missions:

- **Mission 1: Preventing Terrorism and Enhancing Security** – NPPD leads the coordinated efforts to reduce risk and improve resilience of the nation's critical infrastructure and key resources (CIKR) by integrating and disseminating CIKR threat, consequence, and vulnerability information; developing risk mitigation strategies; overseeing the National Infrastructure Protection Plan; and carrying out Chemical

Facility Anti-Terrorism Standards (CFATS) regulations. NPPD also secures federal facilities and protects 1.4 million occupants and visitors daily.

- **Mission 2: Securing and Managing our Borders and Mission 3: Enforcing and Administering Our Immigration Laws** – NPPD provides identity and document verification capabilities for border management and immigration agencies so that they can accurately determine if the people they encounter are who they say they are and whether those people pose a risk to the United States.
- **Mission 4: Safeguarding and Securing Cyberspace** – NPPD leads efforts to secure the Federal Executive Branch civilian government computer systems and critical infrastructure by working with the private sector, all levels of government, military, and intelligence stakeholders. NPPD analyzes and reduces cyber threats and vulnerabilities; distributes threat warnings; and coordinates the response to cyber incidents to ensure that our computers, networks, and cyber systems remain safe and secure.
- **Mission 5: Ensuring Resilience to Disasters** – NPPD protects and strengthens the reliability, durability, and interoperability of the nation’s communications infrastructure and capabilities, and also provides priority telecommunications service during an incident.

Cybersecurity and Communications

The Office of Cybersecurity and Communications (CS&C) is responsible for securing Federal Executive Branch civilian government networks, providing technical expertise, analysis, and warnings to the private sector and critical infrastructure owners and operators, raising cybersecurity awareness among the general public, coordinating the national response to cyber emergencies, and planning for and providing national security and emergency preparedness communications to the federal government and other stakeholders. To facilitate this effort, we work collaboratively with the private sector, all levels of government, military, law enforcement, and intelligence stakeholders to conduct risk assessments and mitigate vulnerabilities and threats to information technology assets and activities affecting the operation of civilian government and private sector critical infrastructures. The functions and mission of the National Cyber Security Center are supported within CS&C and include coordinating operations among the six largest federal cyber centers. The total FY 2012 budget request for CS&C is \$614.2 million.

Cybersecurity

In the protection of Federal Executive Branch civilian networks, we must collaborate with departments and agencies that own and operate widely varying networks. DHS improves the ability of departments and agencies to defend their systems and provides expertise and technology that detects, mitigates and prevents malicious activity on the networks.

As part of the Comprehensive National Cybersecurity Initiative (CNCI), DHS works with the Office of Management and Budget (OMB) to reduce and consolidate the number of external connections that federal agencies have to the Internet through the Trusted Internet Connection (TIC) initiative. This initiative reduces the number of potential vulnerabilities to government networks and allows DHS’ National Cyber Security Division (NCSA) to focus monitoring efforts and security capabilities on limited and known avenues for Internet traffic. NCSA conducts onsite evaluations of agencies’ progress toward implementing TIC goals.

In conjunction with the TIC initiative, the EINSTEIN system is designed to provide the U.S. government with an early warning system for intrusions to Federal Executive Branch civilian networks, near real-time identification of malicious activity, and automated disruption of that malicious activity. The second phase of EINSTEIN, developed in 2008 as part of the CNCI, incorporates intrusion detection capabilities into the original EINSTEIN system. DHS is currently deploying EINSTEIN 2 to Federal Executive Branch civilian agency TIC locations and Network Managed Trusted Internet Protocol Services (MTIPS) providers, which are private internet service providers that serve federal agencies, to assist them with protecting their computers, networks and information. EINSTEIN 2 has now been deployed at 15 of the 19 large departments and agencies that maintain their own TIC locations. Also, the four MTIPS providers currently provide service to seven additional federal agencies. In 2010, EINSTEIN 2 sensors registered 5.4 million “hits,” an average of more than 450,000 hits per month or nearly 15,000 hits per day. A hit is an alert triggered by a predetermined intrusion detection signature that is associated with a known or suspected threat. Each hit represents potential malicious activity for further assessment by the United States Computer Emergency Readiness Team (US-CERT).

The FY 2012 budget request allows NCSD to expedite the deployment of the third phase of the EINSTEIN system—an intrusion prevention capability that will provide DHS with the ability to automatically detect and disrupt malicious activity before harm is done to critical networks and systems. In advance of this development, DHS, in coordination with the National Security Agency (NSA), conducted the CNCI Initiative 3 Exercise, which advanced the potential capabilities of the EINSTEIN system by demonstrating defensive technology, sharing near real-time threat information with the Department of Defense (DoD) for enhanced situational awareness, and providing a platform upon which an oversight and compliance process can be implemented for the evolving set of EINSTEIN capabilities. The Department’s Privacy Office and its Office for Civil Rights and Civil Liberties carefully reviewed the exercise concept of operations, and the Privacy Office worked with US-CERT to publicly release a detailed Privacy Impact Assessment evaluating the exercise.

Beyond the TIC initiative and the EINSTEIN system, DHS, OMB, and the National Institute for Standards and Technology work cooperatively with agencies across the federal government to coordinate the protection of agency information systems through compliance with the Federal Information Security Management Act of 2002 (FISMA). US-CERT monitors EINSTEIN 2 sensors for intrusion activity and receives self-reported incident information from federal agencies. This information is reported to OMB for use in its FISMA oversight capacity. In 2010, NCSD also began to administer the CyberScope system, which was developed by the Department of Justice. This system collects agency information regarding FISMA compliance and—as NCSD, OMB and their agency partners move toward automated reporting—will enable real-time assessments of baseline security postures across individual agencies and the federal enterprise as a whole. This activity complements the development of reference architectures that NCSD designs for federal agencies that are interested in implementing security solutions based on standards and best practices. NCSD also works with the General Services Administration to create Blanket Purchase Agreements that provide security solutions for federal agencies.

The FY 2012 budget request provides significant funding for the protection of federal civilian networks through initiatives such as:

- US-CERT Operations: Provides remote and onsite response support and defense against malicious cyber activity for the Federal Executive Branch civilian networks. The FY 2012 budget request for US-CERT Operations is \$80.9 million. This funding enables US-CERT to expand its capabilities in the areas of cyber analytics, cybersecurity indications and warnings, collaboration and coordination, and cyber incident response to enhance its 24-hour operational capabilities.
- Federal Network Security: Focuses on achieving cybersecurity throughout the Federal enterprise through continuous monitoring and compliance assessments for TIC; promoting cybersecurity directives, statutes, and strategies; and supporting the Federal Executive Civilian Branch departments and agencies in achieving compliance with FISMA. The FY 2012 request for these activities totals \$40.9 million. This request increases the Department's efforts to strengthen Federal Network Security of large and small agencies and will enable NPPD identify and prioritize actions required to mitigate risks and improve cybersecurity posture across the Federal Executive Branch.
- Network Security Deployment: \$233.6 million is requested in FY 2012 to expedite the deployment of EINSTEIN 3 to prevent and detect intrusions on computer systems and to upgrade the National Cyber Security Protection System, building an intrusion detection capability and analysis capabilities to protect federal networks.
- Cybersecurity Coordination: \$5 million is requested in FY 2012 to provide ongoing coordinating operations among the six largest federal cyber centers.

The President's Cyberspace Policy Review called for "a comprehensive framework to facilitate coordinated responses by government, the private sector, and allies to a significant cyber incident." DHS coordinated the interagency, state and local government, and private sector working group that developed the National Cyber Incident Response Plan. The plan provides a framework for effective incident response capabilities and coordination among federal agencies, state and local governments, the private sector, and international partners during significant cyber incidents. It is designed to be flexible and adaptable to allow synchronization of response activities across jurisdictional lines. In September 2010, NCSA hosted Cyber Storm III, a response exercise in which members of the domestic and international cyber incident response community addressed the scenario of a coordinated cyber event. During the exercise, the National Cyber Incident Response Plan was activated and its incident response framework was tested. Based on observations from the exercise, the plan is in its final stages of revision prior to publication.

Cyber Storm III also tested the National Cybersecurity and Communications Integration Center (NCCIC)—DHS' 24-hour cyber and communications watch and warning center—and the federal government's full suite of cybersecurity response capabilities. The NCCIC works closely with government at all levels and with the private sector to coordinate the integrated and unified response to cyber and communications incidents impacting homeland security.

Numerous DHS components, including US-CERT, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the Office of Intelligence and Analysis, and the

National Coordinating Center for Telecommunications (NCC), are collocated at the NCCIC. Also present in the NCCIC are other federal partners, such as DoD and members of the law enforcement and intelligence communities. The NCCIC also physically collocates federal staff with private sector and non-governmental partners. Currently, representatives from the Information Technology and Communications sectors are located at the NCCIC. We are also finalizing steps to add representatives from the Banking and Finance sector, as well as the Multi-State Information Sharing and Analysis Center.

By leveraging the integrated operational capabilities of its member organizations, the NCCIC serves as an “always on” cyber incident response and management center, providing indications and warning of imminent incidents, and maintaining a national cyber “common operating picture.” This facilitates situational awareness among all partner organizations, and also creates a repository of all vulnerability, intrusion, incident, and mitigation activities. The NCCIC also serves as a national point of integration for cyber expertise and collaboration, particularly when developing guidance to mitigate risks and resolve incidents. Finally, the unique and integrated nature of the NCCIC allows for coordination with all interagency and private sector staff during steady-state operations to effectively incorporate partners as needed during incidents.

The FY 2012 request includes \$1.3 million to provide 15 DHS cyber analysts to enable DHS to coordinate national cyber security operations and interface with DoD’s National Security Agency (NSA) at Fort Meade, Maryland. This funding will support the landmark memorandum of agreement signed by Secretary Napolitano and Secretary of Defense Robert Gates that aligns and enhances the nation’s capabilities to protect against threats to critical civilian and military computer systems and networks.

As NCSD continues to make progress on initiatives such as TIC and EINSTEIN, the Department is also mindful that the nation’s cybersecurity challenge will not be solved by a single technology solution. Multiple innovative technical tools are necessary and, indeed, technology alone is insufficient. The mission requires a larger cybersecurity professional workforce, governance structures for enhanced partnerships, more robust information sharing and identity protection, and increased cybersecurity awareness among the general public. Responsibility for these solutions is, and will remain, distributed across public and private sector partners.

NCSD is focused on building a world-class cybersecurity team by hiring a diverse group of cybersecurity professionals—computer engineers, scientists, and analysts—to secure the nation’s digital assets and protect against cyber threats to our CIKR. NCSD continues to hire cybersecurity and information technology professionals, nearly tripling its cybersecurity workforce in FY 2009 and nearly doubling that number again in FY 2010. NCSD currently has more than 230 cybersecurity professionals on board, with dozens more in the hiring pipeline.

Several initiatives are designed to build the nation’s workforce of highly qualified cybersecurity professionals. NCSD and NSA co-sponsor the Centers of Academic Excellence in Information Assurance Education and Research programs, the goal of which is to produce a growing number of professionals with information assurance expertise in various disciplines. DHS and the Department of State co-host Operation Cyber Threat, a series of government-wide experiential and interactive cybersecurity training pilots designed to apply learning concepts and share best

practices in a secure, simulated environment to build capacity within the federal workforce. In December 2010, the Institute of Electrical and Electronics Engineers Computer Society, the world's leading organization of computing professionals, formally recognized the Master of Software Assurance (MSwA) Reference Curriculum, which DHS sponsored through its Software Assurance Curriculum Project. The MSwA program is the first curriculum of its kind to focus on assuring the functionality, dependability, and security of software and systems. Finally, NCSD co-sponsored the annual Colloquium for Information Systems Security Education and the Scholarship for Services (SFS) Job Fair/Symposium, which brought together 55 federal agencies and more than 200 SFS students.

The National Initiative for Cybersecurity Education (NICE) has the dual goals of a cyber-savvy citizenry and a cyber-capable workforce. Working with the National Institute of Standards and Technology (NIST), which is the overall interagency lead, NCSD heads the NICE awareness elements and co-leads the training and professional development components with DoD and the Office of the Director of National Intelligence.

The FY 2012 budget request includes \$24.5 million to provide high-quality, cost-effective virtual cybersecurity education and training to develop and grow a robust cybersecurity workforce that is able to protect against and respond to national cybersecurity threats and hazards.

DHS leverages its significant cybersecurity capabilities as we work collaboratively with our private sector partners to protect the nation's CIKR. US-CERT engages with the private sector on a voluntary basis and provides remote and onsite incident detection, analysis, mitigation, and response support, as well as assistance in assessing threats and vulnerabilities. This outreach is conducted in coordination with other appropriate federal entities with cybersecurity responsibilities, including the Federal Bureau of Investigation and NSA, leveraging the full capabilities of the federal government, as well as the Department's trusted relationships with private sector partners.

NCSD provides onsite support to owners and operators of critical infrastructure for protection against and response to cyber threats including incident response, forensic analysis, and site assessments in collaboration with the Office of Infrastructure Protection's Vulnerability Assessment program. In addition, NCSD provides a tool that enables owners and operators to conduct assessments on their own. ICS-CERT has also trained more than 14,000 stakeholders on ways to counter threats to industrial control systems. In this area, NCSD works closely with the Department of Energy's Idaho National Laboratory through an Interagency Agreement to augment our capabilities.

NPPD is committed to developing innovative ways to enhance the general public's awareness about the importance of safeguarding the nation's computer systems and networks from attacks. Every October, DHS and its public and private sector partners promote efforts to educate citizens about guarding against cyber threats as part of National Cybersecurity Awareness Month. Working with the private sector and the general public, DHS developed the *Stop. Think. Connect.* campaign as an ongoing national public education effort designed to increase public understanding of cyber threats and how individual citizens can develop safer cyber habits that will help make networks more secure.

The FY 2012 budget request includes \$61.4 million to support the collaboration with the public and private sectors to assess and mitigate risk to the nation's cyber CIKR and to promote cybersecurity awareness among and within the general public and key communities.

Communications

The FY 2012 request includes \$106.9 million for the National Communications System (NCS) to sustain, as well as advance, the telecommunications capabilities of the national security and emergency preparedness (NS/EP) user community. To this end, NPPD conducts analysis of the nation's communications infrastructure through the President's National Security Telecommunications Advisory Committee (NSTAC). Through the NCS, NPPD participates in international standards bodies to ensure evolving communications commercial standards address NS/EP communications technical requirements.

The NCS serves as the Communications Sector-Specific Agency fulfilling the role assigned by HSPD-7 and the NIPP to DHS to serve as the federal department responsible for protection activities in the communications sectors. The NCS conducts steady-state planning to identify and mitigate vulnerabilities to the nation's communications infrastructure and leads Emergency Support Function 2 (Communications) coordination between the federal government and state, local and private sector emergency management entities. NPPD is also advancing telecommunications capabilities through the Next Generations Networks Priority Service, a technology service designed to maintain and migrate legacy priority voice telecommunications features and apply priority to data applications as the public switched network evolves to Next Generation Networks.

Last year, the NCS grew Government Emergency Telecommunications Service (GETS), Wireless Priority Services (WPS) and Telecommunications Service Priority (TSP) subscribership among NS/EP users by 6 percent and exceeded a targeted 90 percent call completion rate for GETS and for NS/EP users during disasters. The NCS also delivered 24-hour operational support and coordination to preserve the health of the nation's communications infrastructure during the BP Deepwater Horizon oil spill; flooding in the upper Midwest, Central Plains, New England, Tennessee, and Alabama; and earthquakes in Maryland, Nevada, California, and Haiti.

The FY 2012 request includes \$43.5 million for the Office of Emergency Communications (OEC) to advance federal, state, local, and tribal government interoperable emergency communications capabilities by facilitating the identification of capability needs, the adoptions of solutions, and the verification (through realistic exercises) that capabilities effectively address the needs. Last year, OEC provided technical assistance to all 56 states and U.S. territories to support the implementation of Statewide Communication Interoperability Plans and the alignment of Statewide Communication Interoperability Plans to the National Emergency Communications Plan. Additionally, the Emergency Communications Preparedness Center was formally established to coordinate emergency communications policy across the federal interagency community.

OEC is involved in coordinating inter-agency public safety broadband communications efforts. This includes helping to set the broad policy framework for public safety broadband networks and ensuring that it aligns with existing emergency communications policy. OEC is offering

technical assistance to jurisdictions that received Federal Communications Commission waivers for early deployment of interoperable public safety broadband networks and other early adopters of broadband solutions to ensure that their activities remain aligned with the vision of a nationally interoperable network. OEC is also coordinating federal broadband efforts to develop requirements and influence standards associated with potential federal user participation in the National Public Safety Broadband Network. OEC will conduct key analysis, coordination and stakeholder outreach activities crucial to the effective management, deployment, and long-term operations and maintenance of the network, in collaboration with Emergency Response Interoperability Center.

Infrastructure Protection

The Office of Infrastructure Protection (IP) leads the coordinated national effort to mitigate risk to, strengthen the protection of, and enhance the resilience of the nation's critical infrastructure assets, systems, functions, and networks. IP oversees the implementation of the National Infrastructure Protection Plan (NIPP), which establishes the framework for integrating the nation's various critical infrastructure protection and resilience initiatives into a coordinated effort. The NIPP provides the structure through which DHS, in partnership with government and industry, implements programs and activities to protect critical infrastructure, promote national preparedness, and strengthen incident response.

Protecting the nation's critical infrastructure is a complex mission. The vast majority of critical infrastructure in the United States is privately owned and operated, making public-private partnerships essential to protect and boost the resilience of critical infrastructure and respond to events. IP manages mission complexity by:

- Identifying and analyzing risks.
- Coordinating among state, local and private sector entities that share information and resources.
- Mitigating risk and effects (encompassing both readiness and incident response).

IP's roles are guided by the NIPP and a robust set of programs and activities to support critical infrastructure partners in the field. The NIPP establishes a partnership structure for coordination across 18 critical infrastructure sectors and owners and operators, and a risk management framework to identify assets, systems, and networks whose loss or compromise pose the greatest risk. IP is building on this foundation through expanded mission collaboration with partners, to strengthen not only the protection of critical infrastructure, but also its resilience. Additionally, the FY 2012 budget request includes funds to allow IP to deploy more capabilities and personnel out into the field to further the collaboration with partners.

Identify and analyze vulnerabilities

IP has a number of projects that support the identification, prioritization, and protection of the nation's critical infrastructure, as well as the assessment of critical infrastructure vulnerabilities, consequences and risk. These projects provide an inventory of the nation's most critical infrastructure. IP also conducts and collects vulnerability assessments and consequence information required to produce comprehensive asset and system risk assessments, and these CIKR protection assessments enable the analysis of interdependencies and cascading effects.

The projects established to meet these goals include Vulnerability Assessments, Critical Infrastructure Technology and Architecture, and Infrastructure Sector Analysis.

The FY 2012 budget request for these projects is \$83.9 million, which includes \$22.3 million for Vulnerability Assessments. This will support a minimum of 275 assessments and an additional six Regional Resiliency Assessments. The FY 2012 budget request also supports reaching full operating capability for the Protected Critical Infrastructure Information (PCII) Management System, which will enable increased information sharing of PCII protected information among federal, state, and local partners.

Coordinate nationally and locally through partnerships

IP has several projects dedicated to increasing the ability of our state, local and private sector partners to assess risks, coordinate programs and processes, and execute risk mitigation programs and activities. This includes the NIPP, coordinating efforts of the 18 sectors to implement and execute their Sector-Specific Plans, cross-sector and sector-specific education and training, and activities to facilitate the development of critical infrastructure partner governance and coordination structures and foster information sharing and coordination with these groups.

In FY 2010, IP implemented the Secretary's Sports League Outreach Initiative, working with the owners and operators of 338 major sporting and entertainment venues across the country. Additionally, IP provided coverage and major incident information to critical infrastructure owners and operators through the National Infrastructure Coordinating Center for major incidents including the Deepwater Horizon oil spill, 2010 Midwest Floods, Haitian Earthquake, H1N1 Response, Chilean Earthquake, California Wildfires, Peshawar Attacks, Jakarta Attacks, Kabul Coordinated Attacks, Super Bowl XLIV, and the 2010 Hurricane Season. IP also provided incident-specific web postings via the Homeland Security Information Network – Critical Sectors portals for these and many other incidents impacting critical infrastructure, enabling owners and operators to prepare and respond to incidents. Additionally, IP provides information to federal, state, local, tribal and territorial law enforcement personnel and private sector security management personnel on current and emerging terrorist explosives tactics, techniques, and procedures through the Technical Resource for Incident Prevention (TRIPwire) information sharing portal. This information includes rapid reports on real-world incidents, including the failed attacks on Northwest Flight 253 and Times Square, and the Najibullah Zazi terrorism investigation.

The FY 2012 budget request for these projects is \$48.4 million. Funding will support the development and implementation of the Critical Infrastructure Risk Management Enhancement Initiative and Critical Infrastructure Risk Management Plan, which will identify goals, objectives, milestones and timelines for addressing specific risk-reduction activities and outcomes for Level 1 and Level 2 critical infrastructure, along with sector, state and local assets whose progress has been reported on by the National CIKR Protection Annual Report. IP will also continue to provide operational support to the NIPP public-private partnership councils, including the 18 critical infrastructure sectors, cross-sector, state and local, and regional government councils, currently containing 700 participant organizations and 80 working groups, which engage in more than 600 meetings annually.

Mitigate risk and effects

The FY 2012 budget request includes \$190 million to support IP efforts to mitigate risk and effects include voluntary and regulatory projects and activities, which enable NIPP partners to: identify and mitigate vulnerabilities; implement protective measures and report on risk mitigation activities; and increase preparedness and resilience for facilities, systems, and surrounding communities. They support public awareness efforts, facilitate the sharing of CIKR protection-related best practices and lessons learned, and enable infrastructure protection planning, readiness, and incident. The projects established to meet these goals include the National Infrastructure Coordinating Center, infrastructure security compliance, Protective Security Advisors, IP sector-specific responsibilities, bombing prevention, and incident planning and exercises.

IP has regulatory authority for security at high-risk chemical facilities. As of March 2011, CFATS covers 4,744 facilities—4,126 finally tiered facilities and 618 preliminarily tiered facilities. Once facilities receive a final tier notice, they are required to complete a Site Security Plan (SSP) or Alternate Security Plan (ASP) within 120 days. To date, IP has received and is in the process of reviewing just over 4,100 SSPs/ASPs. Additionally, our chemical inspectors are supporting facilities through Pre-Authorization Inspections (PAIs) in preparing their SSPs. As of February 2011, more than 150 PAIs have been completed. To date, DHS has also issued 66 Administrative Orders to facilities that failed to submit their SSPs within the prescribed deadline, and all 66 facilities complied with the Administrative Orders. DHS conducted its first Authorization Inspection (AI) of a chemical facility in summer of 2010, and a total of four AIs have been completed to date.

IP is also working closely with the U.S. Coast Guard to better harmonize CFATS and Maritime Transportation Security Act regulatory programs. Additionally, IP is determining the best approach for treatment of agricultural production facilities under CFATS and evaluating the current Chemicals of Interest list and the underlying CFATS regulations for potential updates. The FY 2012 budget request of \$99.3 million supports inspection activities, the full implementation of the Personnel Surety Program to identify individuals with potential terrorist ties at covered facilities, and refining the suite of Chemical Security Assessment Tools that support the program. This funding also supports the development and implementation of regulations governing the sale and transfer of the nation's supply of ammonium nitrate pursuant to the authority granted the Department in the Secure Handling of Ammonium Nitrate Act.

IP carries out its field efforts largely through the Protective Security Advisors, who serve as our infrastructure security representation and coordination at the federal, state, local, tribal and territorial levels across all 50 States and Puerto Rico. Protective Security Advisors provide a local perspective to the national risk picture and serve as DHS' on-site critical infrastructure and vulnerability assessment specialists. In FY 2010 the Protective Security Advisors conducted 674 Enhanced Critical Infrastructure Protection (ECIP) security surveys, which capture facility security data and track improvements made by facilities to enhance security and resilience. The FY 2012 request of \$27.5 million includes \$2.3 million to place 15 Infrastructure Security Specialists in State and Local Fusion Centers to develop State and regional critical infrastructure risk management and resiliency plans and work with Fusion Center personnel to support national-level critical infrastructure strategic analysis and decision-making.

The Sector-Specific Agency Management Project executes Sector-Specific Agency functions for 6 of the 18 CIKR sectors: Chemical; Commercial Facilities; Critical Manufacturing; Dams; Emergency Services; and Nuclear Reactors, Materials, and Waste (Nuclear). Last summer, IP held the 2010 Chemical Sector Security Summit, in coordination with the Chemical Sector Coordinating Council, which drew more than 400 participants. The two-day event provided a forum for officials and the private sector to share information on CFATS; threats to the Chemical Sector; local security resources; transportation risk; personnel surety; research and development; and cybersecurity. In addition, the Sector-Specific Agency Management Project serves as the Program Management Office for the Interagency Security Committee (ISC), a federal body created to enhance the security of non-military federal facilities. The ISC has been designated by Executive Order as the body responsible for setting federal building security policy and standards and IP serves as Chair of the ISC. The FY 2012 budget request includes \$24.7 million for these responsibilities, of which \$3.0 million is requested to support the ISC's leadership of senior executives from federal agencies and departments in the long-term development of comprehensive security standards to protect and secure all non-military government infrastructure. This funding will enable the ISC to finalize and issue standards for the Physical Security Criteria, Facility Security Councils, and Contract Guards for federal facilities.

Federal Protective Service

The Federal Protective Service (FPS) protects the 1.4 million daily tenants and visitors in the facilities, on the grounds, and property owned, occupied, or secured by the federal government. FPS provides law enforcement, security countermeasure service, and administers 14,000 contract Protective Security Officers (PSOs) to carry out this responsibility.

Last fiscal year, FPS protected 9,587 General Services Administration (GSA) facilities, conducted 738 facility security assessments, made 1,644 arrests on federal property, prevented more than 700,000 prohibited and potentially dangerous items from being brought into federal buildings, and responded to 2 million alarm activations. FPS also incorporated canines (K9s) capable of detecting explosives that could be carried into a federally protected facility, increasing the number of K9 teams by 38 percent to meet the protective mission of securing federal facilities, employees, and visitors.

The FY 2012 budget request for FPS is \$1,261.5 million. FPS is funded by offsetting collections from other government agencies, and a Basic Security Fee increase of \$0.08, from \$0.66 to \$0.74 per square foot, is requested to recover the costs for an additional 146 law enforcement officers and support personnel to ensure that the occupants of federal facilities are safe. The additional staff will focus on monitoring and oversight of guard performance.

US-VISIT

The United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program provides biometric identification through the collection, maintenance, and sharing of biometric and selected biographic data to authorized DHS, federal, state, tribal, and local law enforcement agencies, and internationally through data-sharing agreements with strategic foreign partners in support of the DHS mission. Through the use of biometrics, US-VISIT collects, stores and shares digital fingerscans and digital photographs for subsequent verification. The biometric

information is paired with biographic information and used to establish and verify an individual's identity, as well as to match that identity against criminal and immigration violator watchlists. US-VISIT also analyzes the biographic entry and exit records of aliens to identify individuals who may have violated U.S. immigration laws by overstaying the terms of their admission in the United States.

The US-VISIT Biometric Support Center (BSC), which began operations in 2004, achieved a major milestone in FY 2010 by making its 500th latent-fingerprint identification. The BSC performs approximately 120,000 latent-print comparisons a week, making it one of the largest latent-fingerprint operations in the world, and hits have included those associated with homicides, terrorism incidents, narcotics distributors, and smugglers. In FY 2010, US-VISIT provided ICE with more than 14,000 credible leads on in-country visa overstays and created 14,269 out-of-country overstay lookouts for officials at U.S. Customs and Border Protection, U.S. Citizenship and Immigration Services, and the Department of State.

US-VISIT increased strategic coalitions with international partners to build consensus on developing and deploying biometric identity-management capabilities across borders.

The FY 2012 budget request for US-VISIT is \$302.3 million including funding for:

- Identity Management and Screening Services: \$32.6 million is requested to enable US-VISIT to screen all new incoming overstay records. Coupled with the request to repurpose \$24.4 million of the current funding (see Biometric Air Exit bullet below), this will allow US-VISIT to clear all currently existing unvetted records and screen 100 percent of new records.
- System Operations and Maintenance: \$128.1 million is requested to operate and maintain two major automated identification systems—the Automated Biometric Identification System (IDENT) for biometric data and the Arrival and Departure Information System (ADIS) for biographic data—to support the significant annual increases in transaction volume and gallery sizes while still enabling timely data searching and response critical to the mission success of US-VISIT customers.
- Unique Identity: \$28.7 million is requested to achieve additional interoperability capabilities between IDENT and the biometric databases of the Departments of Justice and Defense, as well as development of enhancements of a multimodal biometric capability and automated data sharing with international partners, which will provide more data with which to verify an individual's identity.
- US-VISIT 1.0: \$4.9 million is requested to address current system performance limitations and rising operations and maintenance costs by analyzing multiple approaches to re-architecting the system to optimize performance and gain efficiencies. US-VISIT is concerned that the current approach for system maintenance and growth accommodation is insufficient to support the continuously growing demand for US-VISIT's biometric and biographic data services.
- Biometric Air Exit: The FY 2012 budget included a cancellation of \$25.6 million in prior-year funds for biometric air exit to fund immediate operational needs. As mentioned above, the request realigns the remaining \$24.4 million to eliminate the existing 1.5 million unvetted overstay records. The proposed changes in funding

represent a highly effective use of resources, allowing US-VISIT to work the unvetted records.

Risk Management and Analysis

The Office of Risk Management and Analysis (RMA) leads NPPD's effort to build an integrated approach for managing risk that supports the collective efforts and shared responsibilities of the entire homeland security enterprise. RMA provides strategic risk analysis for the Department, enhances risk management capabilities of DHS and enterprise-wide partners, and integrates risk management approaches through the coordinated development of guidance and governance.

RMA recently completed the Risk Assessment Process for Informed Decision-making (RAPID). RAPID is the Department's first quantitative multi-hazard assessment of risk, and provides an initial evaluation of the role that DHS programs play in managing that risk. RMA also collected information on and assigned relative risk level to more than 8,000 Special Events submitted to DHS in order to support federal, state, and local law enforcement efforts; and developed a Special Events geospatial information tool for operations centers, which was deployed in the National Operations Center.

The FY 2012 budget request for RMA is \$9.522 million to continue execution of the RAPID decision support tool, provide technical assistance to DHS and enterprise-wide partners, develop requirements for a Risk Knowledge Management System, and continue to build the Department's integrated Risk Management Framework through development of policy, guidance, processes, and training.

Conclusion

The FY 2012 NPPD budget proposal reflects our strong commitment to protecting the homeland and the American people. As outlined in our testimony today, the budget request allows DHS to continue to mature and strengthen the nation's cybersecurity and infrastructure protection posture while also being effective and efficient stewards of taxpayer dollars.

Thank you for inviting us to appear before you today. We look forward to answering your questions and to working with you on the FY 2012 Budget Request and other homeland security issues.