Statement for the Record

The Honorable Rand Beers

Under Secretary
United States Department of Homeland Security

Before the
United States House of Representatives
Appropriations Committee

March 1, 2012

Introduction

Chairman Aderholt, Vice Chairman Culberson, Ranking Member Price, and distinguished Members of the Subcommittee, let me begin by saying thank you to this Committee for the strong support that you have provided. I look forward to continuing to work with you in the coming year to protect the homeland and the American people.

I am pleased to appear before the Committee today to present President Obama's Fiscal Year (FY) 2013 Budget for the Department of Homeland Security's National Protection and Programs Directorate (NPPD).

NPPD leads the efforts to protect and enhance the resiliency of the Nation's physical and cyber critical infrastructure from terrorist attacks, natural disasters, and other catastrophic incidents. This work requires ongoing collaboration and information sharing with NPPD's Federal, State, local, tribal, territorial, international, and private-sector partners as well as the American public.

The demands on NPPD continue to grow. Terrorist adversaries remain determined to strike us here at home, cybersecurity threats continue to evolve, the Nation faces the ongoing risk of natural disasters and other large-scale emergencies, and the vast network of critical infrastructure is increasingly interconnected and interdependent. The NPPD FY 2013 Budget allows us to continue to meet these evolving threats and challenges by prioritizing our essential operational requirements—while reflecting a commitment to fiscal discipline that maximizes the effectiveness of every security dollar that we receive.

FY 2013 Budget Request

The FY 2013 budget request for NPPD is $2.5 billion in gross discretionary funding and $1.2 billion in net discretionary funding. The Federal Protective Service (FPS) is funded through an estimated $1.3 billion in offsetting collections from other agencies.

The following are highlights of the NPPD FY 2013 Budget:

Organizational Realignments

- *Office of Risk Management and Analysis*: As directed by Congress in the FY 2012 appropriations bill, NPPD's Risk Management and Analysis program will be eliminated and its core function transferred to the DHS Office of Policy, subject to a Section 503 transfer. As such, NPPD is not requesting any funding for this activity in FY 2013.

United States Visitor and Immigrant Status Indicator Technology (US-VISIT): To better align US-VISIT's functions with the Department's operational components, the budget request proposes the transfer of US-VISIT functions from NPPD to Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE). Currently, CBP operates numerous

screening and targeting systems, supporting more than 70,000 users from over 20 Federal agencies that are responsible for a wide range of programs that rely on CBP information and systems to determine benefits, process travelers, inform investigations, support case management, and enhance intelligence capabilities. Although ICE will assume responsibility of the US-VISIT overstay analysis services, CBP and ICE will collaborate on system support for the overstay mission. Transition of the analysis and identification of the overstay population in ICE aligns with the ICE mission of administrative immigration enforcement. These transfers will enable NPPD to further tighten its mission focus on risk reduction to physical and cyber infrastructure.

NPPD supports the following Quadrennial Homeland Security Review missions:

- **Mission 1: Preventing Terrorism and Enhancing Security** – NPPD leads the coordinated efforts to protect and enhance the resilience of the Nation's critical infrastructure by integrating and disseminating critical infrastructure threat, consequence, and vulnerability information; developing risk mitigation strategies; overseeing the National Infrastructure Protection Plan (NIPP); 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 4: Safeguarding and Securing Cyberspace** – NPPD leads the 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 through the National Cyber Incident Response Plan to ensure that our computers, networks, and 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 incidents.

Preventing Terrorism and Enhancing Security

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 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 enhance 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;
- Forming voluntary partnerships to increase preparedness and resilience for facilities, systems, and surrounding communities; and
- Developing regulations for and monitoring the regulatory compliance of certain critical infrastructure owners and operators.

The NIPP establishes a partnership framework for coordination across 18 critical infrastructure sectors, through which DHS coordinates with critical infrastructure partners in Government and the private sector to implement the NIPP risk management framework. This framework establishes processes for combining consequence, vulnerability, and threat information to produce assessments of national or sector 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.

Identifying and analyzing risks

IP maintains 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 threats, vulnerabilities, and consequences. These projects provide an inventory of critical infrastructure and assets whose loss or compromise would pose the greatest risk. IP also conducts assessments to collect vulnerability, capability, and consequence information required to produce comprehensive analyses of asset and system risks. These analyses of interdependencies and cascading effects guide IP's risk mitigation efforts and security planning to strengthen critical infrastructure resilience and preparedness. The projects established to meet these goals include Bombing Prevention, Infrastructure Sector Analysis, and Vulnerability Assessments.

The FY 2013 budget request for these projects is $56.9 million, which includes $20.6 million for Vulnerability Assessments. These funds will support 10 Regional Resiliency Assessment Programs and 200 critical infrastructure assessments, including site assistance visits, Computer-Based Assessment Tool imagery capture, and new nuclear reactor security consultations. Bombing Prevention capabilities include continued support for the Regional Resiliency Assessment Program with Multi-Jurisdiction Improvised Explosive Device Security Planning and Improvised Explosive Device Risk Mitigation training; National Capabilities Analysis Database assessments; the Technical Resource for Incident Prevention (TRIPWire); and continued DHS leadership in executing the *National Strategy for Combating Terrorist Use of Explosives in the United States* and the Homeland Security Presidential Directive-19 Implementation Plan. The FY 2013 budget request also would support the establishment of sector-relative risk baselines for 50 percent of the Sector-Specific Agencies under the Sector-Specific Agency (SSA) Management Project.

Coordinating among State, local, and private-sector entities

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. These efforts include the NIPP, coordinating efforts of the 18 critical infrastructure 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 2011, IP developed and published the *Interim Facility Security Committees: an Interagency Security Committee Standard*, which established procedures for use by a Facility Security Committee when presented with security issues that affect the entire facility. Additionally, IP launched the IP Regional Initiative to jointly coordinate between IP and the State, Local, Tribal, and Territorial Government Coordinating Council to ensure that our State, local, and regional partners have the tools and information they need to implement the NIPP risk management framework effectively. The IP Regional Initiative enables IP to prioritize and resource regional and State requirements more effectively. IP also completed the Federal Triangle Project Phase I, led by the Interagency Steering Committee (ISC), Phase I of which has contributed to the validation process of the Physical Security Criteria/Design Basis Threat and provided a regional perspective and cost on physical security of Federal buildings in the Federal Triangle.

The FY 2013 budget request for the Sector Management and Governance projects is $67.1 million. Funding will support the ISC's creation of performance-based standards for checkpoint detection technologies for explosives and other threats; development of minimum standards for the use, training, and certification of unarmed security officers; and the development of minimum standards for certification of all Federal facility security supervisors. The funding will also support the expanded implementation and synchronization of the base elements of the Critical Infrastructure Risk Management Enhancement Initiative (CIRMEI), the National Annual Report (NAR), and the Critical Infrastructure Risk Management Plan; establish best practices in CIRMEI outcome statements and metrics reporting; increase the number of training completions by 15 percent or more annually to build core competencies; and support regional implementation of critical infrastructure risk reduction activities. The funding will also support IP's collaboration with the State, Local, Tribal, and Territorial Government Coordinating Council to develop a set of State/local/regional outcome statements that can be included in the NAR to show progress in information sharing, risk management, and incident management through the IP Regional Initiative.

Included in the Sector Management and Governance FY 2013 request is $24.2 million for the SSA Management Project, which ensures that IP-led sectors are more capable of preparing for, responding to, or recovering from a natural disaster, technological incident, or terrorist attack. The project has conducted 11 Active Shooter seminars and exercises, reaching hundreds of industry stakeholders and first responders, as well as six Chemical Sector Explosive Threat Awareness Training courses. The SSA Management Project provides free sector-specific risk self-assessment tools that can be used both by the private sector and State, local, tribal, and territorial officials to identify areas for improvement in security, resiliency, and preparedness. The specific tools developed by IP include the Dams Self-Assessment Tool; the Commercial Facilities Risk Self-Assessment Tool, with specific modules for stadiums and arenas, performing

arts centers, lodging, convention centers, racetracks, and theme parks; the Voluntary Chemical Assessment Tool; and the Emergency Services Self-Assessment Tool.

Forming partnerships

The FY 2013 budget request includes $56.5 million for the Regional Field Operations projects, which support IP's efforts to increase preparedness and resilience for facilities, systems, and surrounding communities. These efforts include building and sustaining a comprehensive network of stakeholder engagement structures and processes, consolidating significant primary and cascading impacts caused by critical infrastructure degradation resulting from an incident, and providing comprehensive critical infrastructure protection capacity through the deployment of Protective Security Advisors across the United States.

The Regional Field Operations FY 2013 request includes $28.3 million for 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's onsite critical infrastructure and vulnerability assessment specialists. They are a vital channel of communication for owners and operators of critical infrastructure assets seeking to communicate with DHS. As incidents or threats occur, the Protective Security Advisors living in communities across the country continue to provide the Department with a 24/7 capability to assist in developing the common operational picture for critical infrastructure. In FY 2011, the Protective Security Advisors conducted 600 Enhanced Critical Infrastructure Protection security surveys, which capture facility security data and track improvements made by facilities to enhance security and resilience. The Regional Field Operations FY 2013 request also includes $13.5 million for the National Infrastructure Coordinating Center (NICC), which provides steady-state monitoring and incident management planning for conditions and events that threaten the Nation's critical infrastructure assets.

The Regional Field Operations budget request also provides $14.7 million for the support for the public-private partnership and information sharing, which represent the foundation of voluntary critical infrastructure program through the Partnerships and Information Sharing project. This project provides the necessary unifying framework for the national Sector Partnership, and building and sustaining a network of regional stakeholder forums in partnership with State and local government partners. It also provides a unifying environment for information exchange, built primarily on DHS' Homeland Security Information Network for Critical Sectors (HSIN-CS) - that brought together the 18 sectors, fusion centers across the country, and Federal agencies, such as the U.S. Secret Service, that provide information relevant to the critical infrastructure sectors. In FY 2011, this project supported the operations of more than 40 councils consisting of more than 1,000 members, of which more than 200 were trade associations representing more than 4 million members. Jointly, they delivered approximately 150 products, issue resolutions, and strategic plan reviews. In FY 2011, this project provided 40 online portals for Sectors, Fusion Centers, regional communities, and other organizations providing content to the CI community. For these portals, the project documented communication and coordination Standard Operating Procedures that included incident response coordination, alerts and warnings, suspicious activity reporting, and best practices sharing for risk mitigation. In FY 2011, a new

registrant entered this information sharing environment every hour-and-a-half. The environment provides access to more than 12,000 products. As part of this effort, the project supported 28 online seminars that reached more than 17,000 participants. The project delivered a daily Open Source Infrastructure Report, available on www.dhs.gov, which has 35,000 subscribers and was accessed nearly 372,000 times over the year.

Developing regulations and monitoring regulatory compliance

The request includes $74.5 million to develop and implement mechanisms that assess high-risk chemical facilities and ensure that covered facilities meet risk-based performance standards. This funding will also support the development and implementation of mechanisms to regulate the sale and transfer of the Nation's supply of ammonium nitrate.

NPPD has done much work over the past few years to establish and implement this unprecedented regulatory program, but challenges remain. Accordingly, in mid-2011, I asked the new Director and Deputy Director of NPPD's Infrastructure Security Compliance Division (ISCD) to provide for my consideration their views on the successes and challenges of the CFATS program. In late November 2011, ISCD hand-delivered a detailed memorandum to me that included for my consideration a proposed action plan with detailed recommended steps for addressing the challenges of the CFATS program. NPPD has made progress in addressing many of the challenges identified in the memorandum.

For example, ISCD is using an interim Site Security Plan (SSP) review process that is allowing the Department to review Tier 1 facility SSPs in a more effective and timely manner. Using this interim approach, over the past few months, ISCD has been able to more than quadruple the number of authorized SSPs, and I am pleased to report that as of February 14, 2012, CFATS covers 4,464 high-risk facilities nationwide; of these 4,464 facilities, 3,693 are currently subject to final high-risk determinations and due dates for submission of an SSP or ASP. The remainder of the facilities are awaiting final tier determinations based on their SVA submissions. ISCD continues to issue final tier notifications to facilities across all four risk tiers as we make additional final tier determinations.

The Department and NPPD take our responsibilities for the CFATS program and the Nation's security seriously and are moving forward quickly and strategically to address the challenges before us. We believe that CFATS is making the Nation safer and are dedicated to its success. We will make the necessary course corrections to improve the program to better protect the Nation.

Federal Protective Service

FPS protects the 1.4 million daily tenants and visitors in the facilities, on the grounds, and on property owned, occupied, or secured by the Federal Government. FPS provides law enforcement and security management services, which include operations and oversight of approximately 14,000 contract Protective Security Officers (PSOs), and security countermeasure services for approximately 9,000 General Services Administration-owned, -leased or -operated facilities located in 11 regions across the country. To do so, FPS employs an integrated risk

management strategy to routinely provide a range of services including: ongoing review of facility countermeasures to ensure that they are functioning as designed; regular assistance to Facility Security Committees to implement or improve security practices to align them with Interagency Security Committee (ISC) Physical Security Criteria; assistance with emergency planning and exercises; response to criminal incidents and reports of suspicious activity, including explosive detector dog screening of facilities and clearing of unattended packages; patrol of facilities to deter and detect criminal activity; comprehensive assessment of threats and vulnerabilities using the ISC Design Basis Threat and Physical Security Criteria; security and duress alarm monitoring; awareness training to inform tenants how to prevent and react to events in the facility (e.g., active shooter awareness); and recurring assessment reports with immediate and long-term recommendations to improve facility risk mitigation.

During the last fiscal year, FPS conducted more than 1,800 high-visibility operations (called Operation Shield) and 150 Covert Test operations, ensuring the protection of Federal buildings and infrastructure; responded to 53,000 incidents; made 1,975 arrests; interdicted more than 680,000 weapons/prohibited items at Federal facility entrances during routine checks; and investigated and mitigated more than 1,300 threats and assaults directed towards Federal facilities and their occupants. In addition, FPS trained more than 900 law enforcement officers and agents in "Active Shooter Response Tactics," conducted more than 1,100 student hours of instruction, and conducted more than 200 hours of Active Shooter Tenant Awareness training.

For FY 2013, FPS projects the availability of $1,301.8 million in total collection authority. FPS's primary funding source, the basic security fee, will remain at $0.74 per square foot in FY 2013. NPPD is committed to maintaining 1,371 full-time positions in FY 2013, of which at least 1,007 will be law enforcement officers. FPS is taking a deliberate approach to invest in key areas and better equip our personnel with technology to operate effectively in the risk management environment. FPS will balance the priorities listed below against the statutorily required 1,371 positions.

Specific priorities in FY 2012 and continuing through FY 2013 include development of a follow-on risk assessment methodology that will standardize how facility security assessments are performed, ensuring consistent results, providing tailored recommendations for countermeasures, and enhancing the stakeholders' understanding of vulnerabilities and protective and mitigation strategies. The methodology and process will also ensure that security measures are determined in accordance with standards and criteria established by the ISC. FPS also will undertake an effort to define an activity-based cost structure, which will map costs to the activities that FPS performs. Through this effort, FPS will identify the fees necessary to provide law enforcement operations and risk-based security services at Federal facilities. FPS stakeholders then will have greater transparency into the costs of FPS activities and the level of services provided.

Additionally, FPS will collaborate effectively with stakeholders such as the ISC and industry to develop and implement an informed approach to contract PSO oversight using feedback and best practices. FPS also will explore the means of leveraging technology to ensure effective oversight of PSOs and establish post inspection requirements by security level and frequency requirements for administrative audits. FPS also will improve oversight and management of the PSO force through acquisition strategies and intensive monitoring and coaching.

Safeguarding and Securing Cyberspace

Cybersecurity

DHS works collaboratively with public, private, and international entities to secure cyberspace and America's cyber assets. Working through the National Cyber Security Division (NCSD) within NPPD's Office of Cybersecurity and Communications, DHS works to integrate information about cyber activity and coordinate cyber incident response; enable Federal agencies to secure their systems and networks; provide cyber intrusion detection, prevention, and information sharing capabilities; facilitate education and training for cybersecurity professionals; and mitigate risk to cyber critical infrastructure.

We have improved the ability of Federal agencies to defend their systems and provide expertise and technology that detects, mitigates, and prevents malicious activity on the networks. NCSD's Federal Network Security (FNS) branch manages activities designed to enable agencies to secure their systems and networks. FNS provides a single, accountable focal point for achieving cyber infrastructure security and compliance throughout the Federal enterprise. In FY 2013, $236.0 million is requested for FNS. This includes an increase of $202.0 million to support Federal Executive Branch civilian departments and agencies in implementing capabilities that will improve their cybersecurity posture in accordance with the Federal Information Security Management Act and enable improved continuous monitoring at Departments and Agencies. Aligned with the National Cybersecurity Protection System (NCPS), these resources will support a robust cyber security posture across the Federal Government to thwart advanced persistent threats in a dynamic threat environment.

The request also includes $345.0 million for Network Security Deployment (NSD). NSD manages the NCPS, operationally known as EINSTEIN. NCPS is an integrated intrusion detection, analytics, information sharing, and intrusion-prevention system that uses hardware, software, and other components to support DHS's responsibilities within the Comprehensive National Cybersecurity Initiative mission. In FY 2013, the program will improve its common operating picture to respond in a more agile way to threats to Federal networks and systems by expanding intrusion detection and cyber analytics capabilities and maintaining its capacity to provide intrusion-prevention coverage for Federal network traffic through advanced intrusion-prevention units and supporting infrastructure. Additionally, the program will evolve its service offerings by migrating to a Managed Security Service (MSS) approach for intrusion-prevention services. The evolution of this service will be based on the convergence of a number of existing and near-term intrusion-prevention-services-related initiatives that include EINSTEIN 3 and the Joint Cybersecurity Services Pilot (previously known as the DIB pilot). These efforts will ensure that Federal cybersecurity capabilities are efficiently keeping pace with cutting-edge technologies and adapting to emerging threats. Under the MSS solution, each internet service provider will provide its own intrusion-prevention services that will conform to certain security, assurance, and communication requirements provided by DHS. NSD also will begin planning and developing a cyber mission information sharing environment to improve DHS's ability to respond to and mitigate cyber threats and securely share information across multiple stakeholders.

To keep pace with the expanded NCPS capabilities, the budget includes $93.0 million for United States Computer Emergency Readiness Team (US-CERT) Operations, an increase of $13.9 million. As the operational arm of NCSD, US-CERT leads and coordinates efforts to improve the Nation's cybersecurity posture, promote cyber information sharing, and manage cyber risks to the Nation. US-CERT encompasses the activities that provide immediate customer support and incident response, including 24-hour support in the National Cybersecurity and Communications Integration Center. In FY 2011, US-CERT processed more than 106,000 incident reports from Federal agencies, critical infrastructure, and international partners and released more than 5,200 actionable cybersecurity alerts and information products. As more Federal network traffic is covered by NCPS, additional US-CERT analysts are required to ensure that cyber threats are detected and that the Federal response is effective.

We also collaborate with critical infrastructure owners and operators to assess and mitigate risk to the Nation's cyber critical infrastructure; promote cybersecurity awareness among and within the general public and key communities; maintain relationships with governmental cybersecurity professionals to share information about cybersecurity initiatives; and develop partnerships to promote collaboration on cybersecurity issues. The FY 2013 request includes $62.8 million for the Critical Infrastructure Cyber Protection and Awareness (CICPA) branch. This includes $6.5 million to expand the Multi-State Information Sharing and Analysis Center to 30 States. The CICPA funding will also enable DHS to conduct 75 onsite assessments of critical infrastructure to evaluate the resilience of critical services.

The FY 2013 request also includes $22.0 million for the Global Cyber Security Management (GCSM) branch. GCSM works to develop and promulgate sound practices for software developers, information technology professionals, and other critical infrastructure owners and works to address the need to build a skilled cybersecurity workforce. This amount includes $12.9 million for cybersecurity education. These funds will promote high-quality, cost-effective cybersecurity education and training programs to develop and grow a robust cybersecurity workforce that is able to protect against and respond to national cybersecurity threats and hazards. This funding also will enable DHS to continue to lead and advance the goals of the National Initiative for Cybersecurity Education.

Ensuring Resilience to Disasters

Communications

NPPD supports Mission 5 of the Quadrennial Homeland Security Review, Ensuring Resilience to Disasters, by seeking to improve the security and reliability of America's telecommunications assets by coordinating a provision of telecommunications services to meet national security and emergency preparedness communications requirements during natural disasters or terrorist attacks. NPPD also works to promote interoperable emergency communications capabilities for Federal, State, local, and tribal governments.

The FY 2013 request includes $103.9 million for the National Communications System (NCS) to sustain and advance emergency telecommunications capabilities for national security and emergency preparedness users. These funds also will support technical studies and analyses of

public communications infrastructures and assessments of new communications technologies vulnerabilities, and will work with the international communications industry consensus standards organizations to ensure that evolving communications commercial standards address national security and emergency preparedness communications technical requirements. NPPD also is working to ensure that these emergency telecommunications capabilities continue to operate as telecommunications carriers transition to new technologies through the Next Generation Networks Priority Services program, which will maintain and migrate legacy priority voice telecommunications features to new technologies.

In FY 2011, NCS provided support through the National Coordinating Center for Communications and Telecommunications Service Priority program office during the Japan earthquake/tsunami; flooding in the Mississippi Valley; winter storms in the Midwest and Northeast; the Joplin, Missouri, tornado; tornadoes in the Southeast; Missouri flooding during Spring 2011; flooding in the Northeast and Upper Midwest; and the 2011 National Level Exercise. NCS also supports the Federal Emergency Management Agency (FEMA) and the National Response Framework by serving as the Primary Coordinating Agency for Emergency Support Function #2 (Communications). The Priority Telecommunications Service, which includes the Government Emergency Telecommunications Service (GETS), Wireless Priority Service (WPS), and Special Routing Arrangement Service, serves approximately 400,000 users. In FY 2011, more than 97 percent of GETS users' calls were completed during emergency periods. NCS is also making improvements to the WPS program to address the significant increase in the use of mobile networks.

The FY 2013 request also includes $38.7 million for the Office of Emergency Communications (OEC) to advance Federal, State, local, tribal, and territorial government emergency communications capabilities. OEC continues to partner with stakeholders to implement the National Emergency Communications Plan. In FY 2011, OEC engaged in a comprehensive, nationwide assessment of emergency communications capabilities as a part of plan implementation. OEC is currently working with States to submit and review results. When complete, this assessment will provide a detailed view of capabilities at the county level in all 56 States and territories. This detailed look at emergency communications—the first of its kind—will generate valuable data that DHS and the States can use to focus future resources and improvement activities more effectively and efficiently.

In addition to continued work improving traditional Land Mobile Radio communications, OEC is playing a leading role in nationwide efforts to set the broad policy framework for a public safety broadband network and has coordinated with its State and local partners to ensure that the public safety community's requirements are represented fully in network broadband planning and implementation efforts. OEC regularly engages with the early adopters of public safety wireless broadband communications through the Operator Advisory Committee—a stakeholder group comprising all 21 jurisdictions that have been granted Federal Communication Commission waivers for early adoption of broadband operations in the 700 MHz band. OEC is providing technical assistance to these jurisdictions and developed policy guidance to educate stakeholders on wireless broadband planning and education efforts.

In FY 2011, OEC provided 138 individual technical assistance engagements to 54 States and territories to support the implementation of Statewide Communication Interoperability Plans, including a new wireless broadband technical assistance offering for broadband planning support. OEC also worked through the Emergency Communications Preparedness Center to develop and publish recommendations for common Federal grant guidance to synchronize emergency communications spending across more than 40 grant programs. The Emergency Communications Preparedness Center has also identified the development of broadband standards and research and development as one of its strategic priorities for the coming year and established a focus group to identify Federal broadband requirements. In FY 2011, OEC finalized placement of a Regional Coordinator in each FEMA Region to support the efforts of Federal, State, local, tribal, and territorial agencies to build and improve emergency communications capabilities. The Regional Coordinators strengthen collaboration and knowledge sharing with stakeholders and also provide operational support during federally declared disasters. In August 2011, four of OEC's Regional Coordinators were deployed to support the response to Hurricane Irene. The Regional Coordinators supported many tasks throughout the hurricane response, but their most valuable role was leveraging their strong intergovernmental relationships and localized knowledge base of the regions in which they work. Because the Regional Coordinators work with stakeholders every day, they have an in-depth understanding of the needs of different communities across their regions.

Conclusion

The FY 2013 budget proposal reflects this Administration's strong commitment to protecting the homeland and the American people through the effective and efficient use of limited resources. As outlined in my testimony today, the Department and NPPD will continue to strengthen, secure, and ensure the capacity and reliability of the Nation's critical infrastructure, both cyber and physical.

Thank you for inviting me to appear before you today. I look forward to answering your questions and to working with you on the FY 2013 Budget Request and other homeland security issues.