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
Subcommittee on Homeland Security
March 20, 2013

Introduction

Chairman Carter, Ranking Member Price, and distinguished Members of the Subcommittee, let me begin by thanking you for the strong support that you have provided the Department of Homeland Security (DHS) and the National Protection and Programs Directorate (NPPD). 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 discuss the importance of protecting and making more resilient the Nation's critical infrastructure and cyber networks.

Integrated Critical Infrastructure

Critical infrastructure, both physical and cyber, is a key element of our national security and economic prosperity, and it is at risk from a variety of hazards, including cyber attacks. When we discuss integrated physical and cyber critical infrastructure protection and resilience, we are talking about understanding cyber and physical needs and vulnerabilities, identifying both cyber and physical safeguards and solutions, and understanding the interplay between the two.

Physical and cyber infrastructure have become inextricably linked. We rely on cyber systems to run everything from power plants to pipelines and hospitals to highways. This linkage means that both cyber and physical security measures are required to guard against the full array of potential attacks. For example, physical security measures prevent unauthorized access to servers and other sensitive information technology equipment, protecting against insider threats, which leverage close physical proximity to networks, systems, or facilities in order to modify, gather, or deny access to information. Conversely, cybersecurity measures can prevent an attack that could result in physical consequences. A successful cyber attack on a control system, such as those used in water treatment plants and energy facilities, could have devastating impacts on the health and safety of human lives and cause serious damage to the environment and the economy. These attacks frequently steal data, sometimes disable systems, often disrupt business operations, and have the potential to destroy infrastructure. Individually, or in combination, these attacks could negatively affect the quality of life and well-being of ordinary Americans.

Presidential Policy Directive 21 and Cyber Executive Order

Critical infrastructure security and resilience requires a whole-of-community effort that involves partnerships among public, private, non-profit sectors, and others; as well as a clear understanding of the risks we face. The Federal Government's role in this effort is to share information and to encourage enhanced security and resilience, while also identifying gaps not filled by the marketplace. The enhanced information sharing programs supported by the recently released Executive Order (EO) 13636 for Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD) - 21 on Critical Infrastructure and Resilience help secure critical infrastructure and increase its resilience against cyber and physical attacks, as well as natural disasters and terrorist attacks.

To complement PPD-21, EO 13636 clears the way for more efficient sharing of cyber threat information with the private sector and directs the establishment of a Cybersecurity Framework to identify and implement better security practices among critical infrastructure sectors. Through partnerships between the government and private sector, the critical infrastructure cyber systems upon which much of our economic well-being, national security, and daily lives depend are being better protected.

By issuing EO 13636 and PPD-21, the Administration is taking an integrated approach that strengthens the security and resilience of critical infrastructure against all hazards, through an updated and overarching national framework that acknowledges the evolving risk environment and increased role of cybersecurity in securing physical assets. PPD-21 and the EO 13636 reinforce holistic thinking and action in the realms of security and risk management. The issuance of these important documents allows us to build upon and enhance our existing partnership model with our key private sector and state, local, tribal and territorial partners. Implementation of the EO 13636 and PPD-21 will also drive action toward system and network security and resilience. The Department is well positioned to make advances in the space defined by the cyber-physical security nexus that PPD-21 and EO 13636 address.

DHS has already formed a task force to coordinate implementation of PPD-21 and EO 13636 in order to:

- Lead DHS's implementation of PPD-21 and EO 13636, including coordination with the Department of Commerce, National Institute of Standards and Technology, on the Cybersecurity Framework;
- Serve as the focal point for collaboration with industry;
- Involve key stakeholders from all levels of government; and
- Prioritize tasks, plan implementation, and coordinate principal offices of responsibility.

NPPD Efforts to Secure Infrastructure, Increase Resiliency, and Identify and Evaluate Risk

Securing cyber networks and physical infrastructure

NPPD programs work to secure cyber networks and physical infrastructure. This includes programs that secure and provide diagnostics for Federal cyber networks and those that provide physical security to Federal facilities. Also included are regulatory programs designed to ensure facilities are securing dangerous chemicals.

Protecting Federal Networks

DHS has operational responsibilities for securing unclassified federal civilian government networks and working with owners and operators of critical infrastructure to secure their networks through cyber threat analysis, risk assessment, mitigation, and incident response capabilities. We also are responsible for coordinating the national response to significant cyber incidents and for creating and maintaining a common operational picture for cyberspace across the government.

DHS directly supports federal civilian departments and agencies in developing capabilities that will improve their cybersecurity posture. For example, NPPD is moving to provide Federal agencies with the capability to continuously diagnose and mitigate cyber vulnerabilities in their critical systems. An array of internal sensors provides data about an agency's cybersecurity posture in a near-real time dashboard so that agency security managers can move quickly to defeat common cyber threats. This capability will be a vast improvement over the current expensive and time-consuming process, which requires auditors to manually assess an information technology (IT) system and determine whether it meets static requirements under the Federal Information Security Management Act.

In fiscal year (FY) 2013 NPPD, in support of the Administration's Continuous Monitoring initiative, is supporting the procurement of monitoring equipment, diagnostic sensors and tools, and dashboards to provide situational awareness for agencies across the Federal Executive Branch. Thisprogram will eventually conduct 60 to 80 billion vulnerability and configuration-setting checks every one to three days across the .gov network which will help agencies repair their worst cybersecurity problems first.

The National Cybersecurity Protection System (NCPS), also referred to as EINSTEIN, is an integrated intrusion detection, analytics, information sharing, and intrusion-prevention system that uses hardware, software, and other components to support DHS's cybersecurity responsibilities. In FY 2013, the program will expand intrusion detection and cyber analytics capabilities at Federal agencies, improving NPPD's situational awareness and allowing a more agile response to threats to Federal networks and systems. Additionally, the NCPS intrusion prevention service, known as E^3A, will reach initial operating capability by providing signature-based intrusion prevention capabilities to secure Federal agency traffic. These efforts will ensure that Federal cybersecurity capabilities are efficiently keeping pace with cutting-edge technologies and adapting to emerging threats. NPPD is also growing its cyber mission information sharing environment to improve DHS's ability to respond to and mitigate cyber threats and securely share information across multiple stakeholders.

Integrated Cybersecurity Operations

DHS is also home to the National Cybersecurity & Communications Integration Center (NCCIC), a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement. Cybersecurity is a shared responsibility and operators from the United States Computer Emergency Readiness Team (US-CERT), the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and the National Coordinating Center for Telecommunications (NCC), along with representatives from the DHS

Office of Intelligence and Analysis, Federal law enforcement, the intelligence community, the Department of Defense, state and local governments, and the private sector come together at the NCCIC to support our response to significant cyber or physical incidents affecting critical infrastructure. In FY 2012, the NCCIC began providing a daily common operating picture for cyber incidents. This capability enhanced the situational awareness of cyber incidents detected via EINSTEIN and those reported to the NCCIC by Federal agencies, Federal law enforcement, the intelligence community, the Department of Defense, information sharing organizations, state and local governments, private sector entities, the general public, and international partners. Since 2009, the NCCIC has responded to nearly a half a million incident reports and released more than 26,000 actionable cybersecurity alerts to our public and private sector partners.

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 provides response support and defense against cyber attacks for the Federal Executive Branch (.gov) and information sharing, analytic collaboration, and response support to state, local, tribal and territorial (SLTT) governments, industry, and international partners. US-CERT interacts with Federal agencies, industry, the research community, SLTT governments, and other entities to disseminate actionable cybersecurity information to the public. In 2012, US-CERT resolved approximately 190,000 public and private sector cyber incident reports. This represents a 68 percent increase from 2011. In addition, US-CERT issued more than 7,455 actionable cyber-alerts in 2012 used by private sector and government agencies to protect their systems and had more than 6,400 partners subscribe to the US-CERT portal to engage in information sharing and receive cyber threat warning information. ICS-CERT responded to 177 incidents last year while completing 89 site assistance visits and deploying 15 teams with US-CERT to respond to significant private sector cyber incidents.

Historically, physical processes upon which critical infrastructures depend, such as opening and closing pipeline valves, switching railcars, turning on pumps in chemical facilities, adjusting buildings' HVAC and fire suppression systems, and calibrating implantable medical devices, were completed using human power or using machines with local control. Disasters often occurred when these processes were incorrectly applied, whether maliciously or otherwise. For example, on November 25, 1964, a recently replaced natural gas transmission pipeline exploded and burned in Saint Francisville, Louisiana, killing five workers and injuring at least 23 others. A backhoe was suspected as the cause of the pipeline's rupture. Today, our pipelines are just as vulnerable, but not only to such physical threats but also to those we cannot see. We must not only ensure the physical security of the control systems that govern complex systems such as pipeline systems, but we must also ensure their cybersecurity.

Increasingly sophisticated cyber attack tools can exploit vulnerabilities in commercial industrial control system components, telecommunication methods, and common operating systems found in modern industrial control systems. Many of these systems were designed for operability and reliability during an era when online security was not a priority for these systems.

ICS-CERT works closely with industrial control system vendors, researchers, security service providers, and other government agencies to analyze, identify, and responsibly share industrial control system vulnerabilities and mitigation strategies. ICS-CERT also works closely with critical infrastructure industry owners and operators since they are often best-positioned to

understand the consequences of a malicious, disruptive intrusion into one of their networks. ICS-CERT works with all of these stakeholders to secure control systems and provide incident response assistance.

Protecting Federal Facilities

Just as NPPD executes daily operations that secure and provide diagnostics for Federal cyber networks, we provide daily physical security to Federal facilities. The Federal Protective Service (FPS) protects the 1.1 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 13,000 contract Protective Security Officers (PSO), and security countermeasure services for more than 9,000 General Services Administration-owned, -leased or -operated facilities located in 11 regions across the country.

During the last fiscal year, FPS responded to 47,000 incidents, made 1,902 arrests, interdicted more than 886,000 weapons and prohibited items at Federal facility entrances during routine checks, conducted over 55,000 post inspections, disseminated 331 threat and intelligence-based products to stakeholders, and investigated and addressed more than 1,000 threats and assaults directed towards Federal facilities and their occupants.

Specific priorities in FY 2013 and continuing through FY 2014 for FPS include continued implementation of the Facility Security Assessment process, providing tailored recommendations for countermeasures, and enhancing its stakeholders' understanding of vulnerabilities and protective and mitigation strategies. In FY 2012, FPS deployed the Modified Infrastructure Survey Tool (MIST), which surveys the existing level of protection in a number of security disciplines (such as access control, perimeter control, security force management, security planning and others) and plots them against the baseline level of protection required for a particular facility in the Interagency Security Committee Standards. In addition, NPPD is executing a pilot joint assessment using physical and cybersecurity expertise from across the component. The outputs of this project include a cyber and physical facility assessment report for the General Services Administration; the development of a compendium of NPPD security tools, techniques, and processes (tool kit); development of requirements for an integrated assessment approach/methodology; and an analysis of recommendations and lessons learned for future joint assessments.

FPS also initiated an effort to define an activity-based cost structure, which will map costs to the activities that FPS performs. Through this effort, FPS stakeholders will have greater transparency into the costs of FPS activities and the level of services provided in law enforcement operations and risk-based security services at Federal facilities.

Securing Dangerous Chemicals

NPPD is responsible for implementing the Chemical Facility Anti-Terrorism Standards (CFATS) program, which has made our Nation more secure by identifying and regulating high-risk chemical facilities to ensure they have security measures in place to reduce the risks associated with these chemicals. The CFATS program has made significant progress, advancing programmatically while simultaneously addressing internal operational concerns. The

Department remains committed to working with stakeholders and with Congress on a path forward to ensure the CFATS program continues to build upon its successes to date.

NPPD is continually evaluating the program to identify areas for improvement and adjusting course when necessary to ensure proper implementation. Through the Infrastructure Security Compliance Division's (ISCD) comprehensive Action Plan, we have identified and acted decisively to address areas in which improvements were warranted. This has resulted in significant progress in the program over the last year.

As of March 5, 2013, CFATS covers 4,380 high-risk facilities nationwide; of these 4,380 facilities, 3,468 have received final high-risk determinations and are required to develop Site Security Plans (SSPs) or Alternative Security Programs (ASPs). Since the inception of CFATS, close to 3,000 chemical facilities have eliminated, reduced, or otherwise made modifications to their holdings of potentially dangerous chemicals and are now no longer considered high-risk. This significant reduction in the number of chemical facilities that represent attractive targets for terrorists is an important success of the CFATS program and is attributable both to the design of the program as enacted by the Congress and to the hard work of CFATS personnel who have consulted directly with thousands of chemical facilities.

Among the important items identified in the Action Plan and completed by ISCD was the need to streamline the process for reviewing SSPs. Using the new system, ISCD has completed its review of all Tier 1 SSPs and has begun reviewing Tier 2 SSPs. As of March 5, 2013, 83 of the Tier 1 SSPs have been authorized and 36 Tier 1 SSPs have been approved. ISCD is starting to make progress with Tier 2 as well. As of March 5, 2013, 172 Tier 2 SSPs have been authorized and four Tier 2 SSPs have been approved. ISCD anticipates that we will have completed the approval process for all Tier 1 security plans by October 2013 and for all Tier 2 security plans by May 2014. In addition, Alternative Security Programs (ASPs) are an important part of the CFATS program's continued progress. The ASP provides an option for regulated facilities to submit information required to document site security measures that address the risk-based performance standards through an alternative format. As of March 5, 2013, 397 ASPs have been submitted in lieu of SSPs. ISCD has been working with industry stakeholders regarding their options for the development and use of ASPs. Recently, the American Chemistry Council released a guidance document and template developed in consultation with DHS. Additionally, DHS has been in discussion with other industry stakeholders, including the Agricultural Retailers Association and the Society of Chemical Manufacturers Affiliates, about developing templates specific to their members. DHS has also been engaging industry partners on the development of "corporate" ASPs. For industry partners that own several regulated facilities, the corporation can develop a single ASP template, which can be easily leveraged by all of its facilities. ASPs submitted by facilities using an industry-developed or proprietary template would be reviewed under the same standards that ICSD currently reviews SSPs. The potential for these ASPs to serve as a force multiplier is tremendous as DHS continues to authorize and approve SSPs and ASPs.

Identifying and evaluating risk to cyber networks and physical infrastructure

NPPD maintains a number of projects to 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 to our national security, economic stability, public health and safety. NPPD conducts assessments to collect vulnerability, capability, and consequence information required to produce comprehensive analyses of asset and system risks. These analyses of dependencies, interdependencies, and cascading effects guide NPPD's risk mitigation efforts and security planning to strengthen critical infrastructure resilience.

NPPD's Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) is the Department's analytical infrastructure-intelligence fusion center. HITRAC creates actionable risk-informed consequence analysis for Federal, state, local, tribal, territorial, private sector, and international partners. An integrated understanding of cyber and physical critical infrastructure dependencies and interdependencies is crucial to our ability to prepare for, respond to, and recover from disruptions to the Nation's critical infrastructure. HITRAC is working to improve the Department's cyber and physical infrastructure analysis capabilities including through three proofs of concept projects that will identify dependencies and interdependencies between cyber and physical infrastructure and provide a more comprehensive picture of risk across infrastructure sectors. This integrated analysis capability will allow NPPD to provide more informed risk analysis to our partners and decision-makers on emerging threats, risks, and consequences.

Increasing the resiliency of cyber networks and physical infrastructure

NPPD programs work with public and private sector partners to increase the security and resilience of cyber networks and physical infrastructure. This includes programs to support critical infrastructure owners and operators in enhancing their facilities' physical and cyber security and resilience, coordinating critical infrastructure sectors, providing communications capabilities for national security and emergency preparedness (NS/EP) users responding to a disaster, and enhancing the communications capabilities of state and local first responders.

Infrastructure resilience is not only the responsibility of government, it is very much a whole-of-Nation activity, which starts with those who own and operate the infrastructure, both private and public sector, and those who make the decisions daily that protect and secure our most critical assets and systems. Information sharing is the core foundation of any truly effective public-private partnership. DHS plays a central role in protecting our Nation's critical infrastructure by working with critical infrastructure owners and operators to prepare for, prevent, mitigate, and respond to threats to their facilities. We work with owners and operators to develop and monitor approaches to reduce risk to our critical infrastructure and make it more secure and resilient.

NPPD/IP builds partnerships across the critical infrastructure domain, leads related preparedness activities, and serves as an information sharing conduit between private sector and public entities. IP's work spans the spectrum of security and resilience and allows us to promote

enhanced infrastructure reliability in an all-hazards environment. IP works jointly with government partners at the Federal, state, local, tribal, and territorial levels as well as stakeholders in the private sector to ensure that all impacted organizations are actively involved in building a resilient infrastructure.

Coordinating Critical Infrastructure Sectors
NPPD is responsible for coordinating the Nation's critical infrastructure security and protection efforts, including development and implementation of the National Infrastructure Protection Plan (NIPP). The NIPP 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. The NIPP is updated every four years to capture evolution in the critical infrastructure risk environment. In FY 2013, IP will begin updating the NIPP based on requirements set forth in PPD-21. NPPD will work with critical infrastructure stakeholders to focus the NIPP on better integration of cyber and physical risk management, requirements for increased resilience, and recognition for the need for enhanced information sharing and situational awareness.

NPPD also provides a unifying environment for information exchange, built primarily on DHS's Homeland Security Information Network for Critical Sectors (HSIN-CS), which brings together the 16 sectors[1], fusion centers from across the country, and Federal agencies that provide information relevant to the critical infrastructure sectors. In FY 2012, HSIN-CS supported more than 120 sector partnership councils and working groups. DHS, in coordination with the councils, delivered approximately 150 products, issue resolutions, and strategic plan reviews. In FY 2012, this project provided 40 online portals for Sectors, fusion centers, regional communities, and other organizations providing content to the critical infrastructure 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, including information from the NCCIC on cybersecurity. As part of this effort, the project supported 28 online seminars that reached more than 17,000 participants. NPPD also delivers 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.

Direct Engagement with Federal, State, Local, Private Sector, and International Entities
NPPD collaborates with critical infrastructure owners and operators to assess and mitigate risk to the Nation's 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. We also coordinate these efforts with international partners, when appropriate, to ensure the delivery of coordinated messaging to critical infrastructure. In order for us to inspire action and build greater resilience, we need to have the right people at the table who can make the investment decisions that allow critical infrastructure operators to close gaps, increase security, and upgrade technology.

[1] Previously there were 18 sectors, but through consolidation of sectors through PPD-21, the number was reduced to 16.

Executive engagement is crucial to maintaining a healthy partnership because the access to resources, strategic vision, and the multidisciplinary skills necessary to address big infrastructure protection and resilience issues often resides at the CEO level. Beginning in FY 2012, IP has been increasing its efforts in engaging more CEOs, including a briefing for approximately 75 electric and nuclear CEOs as well as engagements with local CEOs that bring a variety of DHS partners to the table.

Protective Security Advisors (PSAs) serve as the nexus of our infrastructure security and coordination efforts at the Federal, state, local, tribal, and territorial levels. PSAs 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 PSAs 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 2012, the Protective Security Advisors conducted more than 1,000 Enhanced Critical Infrastructure Protection security surveys, which capture facility security data and track improvements made by facilities to enhance security and resilience. In addition, approximately 50 percent of NPPD's cybersecurity site assessments administered by NPPD's Office of Cybersecurity and Communications were conducted in tandem with PSAs—an example of how we are working to better and more effectively integrate our physical and cyber security efforts across NPPD and the Department.

NPPD supports the Multi-State Information Sharing and Analysis Center (MS-ISAC), which provides cybersecurity services to SLTT members. MS-ISAC is represented at the NCCIC and plans to provide 150 onsite assessments of critical infrastructure to evaluate the cybersecurity posture and resilience of critical service providers in FY 2013. These assessments focus on both general network security and industrial control systems security, applying one of two methodologies—the Cyber Resiliency Review (CRR) and the Cyber Security Evaluation Tool (CSET). Using the CRR, NPPD also completed the first Nationwide Cybersecurity Review in 2012, which assessed cybersecurity maturity levels and risk awareness across 49 states, two U.S. territories, and more than 75 cities, counties, and municipalities. NPPD will conduct a second review in 2014. The CSET, used by ICS-CERT when conducting site assessments, also is freely available for asset owners and operators to download in support of self-assessments. Each year, CSET distribution reaches each of the CI sectors. In FY 2013, NPPD expects to distribute approximately 7,000 copies of the tool.

NPPD also supports the Regional Resiliency Assessment Program (RRAP), which examines the inherent connectivity of assets and systems within a specific geographic area or infrastructure function. The goal of the RRAP is to identify opportunities for regional homeland security officials and critical infrastructure partners to strengthen resilience to all hazards. This is achieved through a combination of vulnerability assessments, regional analysis, and research related to the RRAP focus area. The RRAP process identifies critical infrastructure dependencies, interdependencies, cascading effects, and capability gaps. IP has partnered with the critical infrastructure community to complete 27 RRAP projects over four years on a diverse

and dynamic set of critical infrastructure topics, touching nearly every major region and most sectors. Ten RRAPs were conducted in FY 2012, with another 10 scheduled in FY 2013.

The Office for Bombing Prevention builds capabilities within the general public and across the private and public sectors to prevent, protect against, respond to, and mitigate bombing incidents. In FY 2013, the Office for Bombing Prevention will conduct 125 capability assessments, including a new Bombing Prevention Index, which establishes a baseline score that enables measurement of progress toward improvised explosive device (IED)-related national resilience and preparedness goals and used the capability data to conduct 10 Multi-jurisdictional improvised explosive device security plans, 30 bomb-making materials assessment program events, and 75 IED awareness and risk mitigation training courses. The Technical Resource for Incident Prevention (TRIPwire) Information Sharing program provides law enforcement and first responders with unclassified IED information, with more than 15,514 registered TRIPwire users, including 2,500 users added in FY 2012. In addition, the Office for Bombing Prevention continues to lead DHS efforts in executing the national policy for Countering Improvised Explosive Devices.

Ensuring Adequate Communications Capabilities to Support Disaster Response Operations
NPPD provides a series of national security/emergency preparedness (NS/EP) and emergency communications capabilities in partnership with Federal, SLTT and private sector stakeholders. NPPD develops and maintains NS/EP communications priority services programs, which have supported the communication needs of over one million users across all levels of government and the private sector. The Government Emergency Telecommunications Service **(**GETS) program is a White House-directed emergency telecommunications service. GETS supports more than 274,000 Federal, state, local, tribal, and territorial government, industry, and non-governmental organization personnel in performing their NS/EP communications missions by providing a robust mechanism to complete calls during network congestion from anywhere in the United States. Wireless Priority Service (WPS) is the wireless complement to GETS, created due to the overwhelming success of GETS during 9/11. The program enhances the ability of 108,000 NS/EP subscribers to complete cellular phone calls through a degraded public switched telephone network during a crisis or emergency situation. In FY 2013, NPPD plans to continue the expansion and general availability of WPS across multiple carriers and plans to achieve at least a 90 percent call completion rate during emergency communication periods and National Special Security Events.

NPPD is also working to support the implementation of the *Middle Class Tax Relief and Job Creation Act of 2012*, which established the Nationwide Public Safety Broadband Network (NPSBN) for emergency responders at all levels of Government. A DHS priority is to ensure resilience measures are built into the network. DHS is currently working with industry and Federal stakeholders to develop a risk assessment of the network's physical and cybersecurity infrastructure and offer recommendations to ensure appropriate security measures are built in from the outset of the Network's deployment. The Act establishes a new entity with-in the National Telecommunications and Information Administration of the Department of Commerce to oversee planning, construction and operation of the network, known as the First Responder Network Authority, or FirstNet.

To advance FirstNet's deployment of a nationwide public safety broadband network, NPPD's Office of Emergency Communications (OEC) is leading a number of activities designed to assist state and local agencies with understanding their current and planned broadband communications needs. As FirstNet's deployment advances, OEC coordination with state and local public safety first responders will become more critical than ever with the adoption of broadband communications. To increase coordination of Federal efforts for broadband implementation, the Emergency Communications Preparedness Center (ECPC) is working to identify Federal broadband requirements by preparing a consolidated view of emergency communications assets, addressing associated legal and regulatory barriers, reviewing and analyzing Departmental positions on pending broadband regulatory matters and rulemakings, and establishing standardized grant guidance and processes. Concurrently, the OneDHS Emergency Communications Committee is providing consolidated Departmental input into Federal interagency efforts, as well as developing strategies for broadband technology migration from current land mobile radio technology to next generation wireless network technology.

Leveraging Integrated Capabilities: Hurricane Sandy Response and Recovery

Before, during, and after Hurricane Sandy, NPPD provided support through resources and personnel to the affected area. Through NPPD's existing partnerships with critical infrastructure partners, DHS was able to facilitate much-needed fuel deliveries to critical telecommunication sites in lower Manhattan in order to fuel generators and keep the facilities operational. After PSAs were notified of the fuel supply shortage, HITRAC provided analysis on the wide-spread impact if the telecommunications facility lost power, while the NCC worked with its public and private sector partners to identify a fuel supply and coordinate its delivery to the critical site.

PSAs closely monitored Hurricane Sandy in the lead up, during, and following the storm as part of their incident response mission area to protect the Nation's critical infrastructure. Thirty-four PSAs deployed to Regional Response Coordination Centers in Federal Emergency Management Agency Regions I, II, and III as well as state, county, and regional Emergency Operations Centers. The PSAs served as infrastructure liaisons and provided expert knowledge of impacted infrastructure; maintained communications with owners and operators of critical infrastructure; and prioritized and coordinated response, recovery, and restoration efforts. Throughout the entire course of the incident, the PSAs provided updates on the status of critical infrastructure.

HITRAC mobilized to provide actionable analysis for decision makers throughout the storm including impact analysis, high fidelity consequence modeling, and infrastructure protection prioritization priorities. It also developed timely, authoritative, and incident-specific preparedness and response activities, which included risk and threat analysis, predictive consequence modeling and prioritization analysis, and product development. HITRAC was able to provide critical information on fuel supply and infrastructure of concern. In addition, the NICC provided situational awareness to DHS leadership throughout the event as well as critical information collection and distribution for Critical Infrastructure Stakeholders in the Public and Private sector. These efforts helped share information regarding storm impacts and restoration priorities.

Throughout the preparation and response efforts, FPS coordinated with Federal tenants and the GSA to ensure that law enforcement and security needs related to Federal properties and assets brought in to help with power restoration were met. In addition to the more than 30 law enforcement officers originally on duty in the affected areas, FPS launched national deployments of its Crisis Response Team, which brought an additional 40 law enforcement officers to support tenant agencies and Federal facilities as well as 24 law enforcement officers to support FEMA. These officers played a key role in preventing vandalism, theft, and destruction of Federal property and were instrumental in ensuring that equipment and supplies from the U.S. Army Corps of Engineers leveraged as part of the Power Restoration Task Force were protected.

NPPD is currently supporting Hurricane Sandy recovery efforts. Eighty-eight FPS PSOs are assigned to 18 locations in New York and 38 FPS PSOs are assigned to a Joint Field Office in New Jersey. IP personnel are also deployed to the region supporting the New Jersey Joint Field Office and New York Joint Field Office. There are two senior representatives providing critical infrastructure analysis capabilities and support to FEMA's Infrastructure Systems Recovery Support Function as part of the National Disaster Recovery Framework in response to Hurricane Sandy. New York PSAs have continued to work closely with Federal, state and local responders, dividing efforts among the New York City Emergency Operations Center (EOC), the Nassau County EOC, and the Suffolk County EOC.

Conclusion

Protecting critical infrastructure – both physical and cyber – is a shared responsibility. Just as we all enjoy and rely on the benefits of critical infrastructure, we all must play a role in keeping it strong, secure, and resilient. NPPD is leveraging the full breadth and scope of expertise in the Directorate and all of our industry and government stakeholders to collaborate on the protection, resiliency, and risk identification and evaluation of physical and cyber infrastructure. Additionally, as NPPD mission operations have grown tremendously over the last five years, it is imperative that the Directorate have the appropriate resources to provide management, support, and oversight to ensure program performance and mission success.

We know that evolving threats– and the need to address them – do not diminish because of budget reductions. In the current fiscal climate, we do not have the luxury of making significant reductions to our capabilities without significant impacts. Sequester reductions will require us to scale back and delay the development and deployment of critical capabilities for the defense of Federal cyber networks.

Thank you, Chairman Carter, Vice Chairman Aderholt, Ranking Member Price, and distinguished Members of the Subcommittee for the opportunity to discuss NPPD's role in strengthening cybersecurity for the Nation's critical infrastructure. I look forward to any questions you may have.