Testimony of

Suzanne Spaulding
Under Secretary
National Protection and Programs Directorate

and

Phyllis Schneck
Deputy Under Secretary for Cybersecurity and Communications
National Protection and Programs Directorate

United States Department of Homeland Security
Before the
United States House of Representatives
Appropriations Committee
Subcommittee on Homeland Security

April 29, 2014

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). We look forward to continuing to work with you in the coming year to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards.

We are pleased to appear before the Committee today to discuss NPPD's efforts to strengthen the Nation's physical and cyber critical infrastructure security and resilience against terrorist threats, cyber events, natural disasters, and other catastrophic incidents. The President's Fiscal Year (FY) 2015 Budget Request for NPPD is $2.9 billion, offset by $1.3 billion in collections for the Federal Protective Service (FPS). This request is a $44 million, or 1.6%, increase over the FY 2014 Omnibus and provides targeted investments that integrate and execute cybersecurity and physical security capabilities.

The National Infrastructure Protection Plan (NIPP) was released in December 2013, establishing the strategic direction for integrating the Nation's various critical infrastructure protection and resilience initiatives into a coordinated effort. NPPD is committed to ensuring that its cybersecurity, infrastructure protection, and identity management functions are adequately resourced to help protect the Nation's critical infrastructure and other critical government functions. At the same time, this budget request emphasizes that we must think about physical security and cybersecurity holistically; both to better understand how they relate and integrate and how best to mitigate the consequences of attacks that can cascade across all.

On April 16, 2013, the Pacific Gas and Electric (PG&E) Metcalf substation, that controls the energy supply for much of San Jose, California, was attacked by an unknown individual or individuals who fired multiple shots at various components within the substation. This incident is still under investigation. This was not a cyber attack, rather, the attack on this infrastructure likely occurred with an unknown tool that severed a group of fiber optic cables running between a critical electric substation and a remote communications facility. This attack also degraded the hardline telephone service for Santa Clara County and surrounding localities, and broke key connections from a remote facility that communicated with the substation, threatening Silicon Valley with a potentially cascading power failure. This incident is a poignant reminder that disruptions to the Nation's critical infrastructure, whether via cyber or physical attack, can have far reaching consequences that cascade beyond the initial attack and that permeate the physical and cyber domains.

Leveraging Integrated Capabilities: Implementing PPD-21 and EO 13636

On February 12, 2013, the President signed Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity* and Presidential Policy Directive (PPD) 21, *Critical Infrastructure Security and Resilience*, which set out steps to strengthen the security and resilience of the Nation's critical infrastructure, and reflect the increasing importance of integrating cybersecurity efforts with traditional critical infrastructure protection. To implement both EO 13636 and PPD-21, the Department established an Integrated Task Force to lead DHS implementation and coordinate interagency, public and private sector efforts, and to ensure effective integration and synchronization of implementation across the homeland security enterprise.

The FY 2015 budget request reflects targeted enhancements to continue implementation of the EO and PPD. Enhancements of $17million, including 58 positions, is requested for the Critical Infrastructure Cyber Community (C³, or "C-Cubed") Voluntary Program; Enhanced Cybersecurity Services (ECS); Regional Resiliency Assessment Program; National Coordinating Center (Communications) (NCC) 24x7 communications infrastructure response readiness; and Infrastructure Design and Recovery Support (IDRS). NPPD has partially offset these enhancements with $9 million in reductions to realign resources to support these key EO and PPD initiatives.

C³ Voluntary Program

The C^3 Voluntary Program is a public-private partnership aligning business enterprises as well as Federal, State, local, tribal, and territorial (SLTT) governments to existing resources that will assist their efforts to use the National Institute of Standards and Technology Cybersecurity Framework to manage their cyber risks as part of an all-hazards approach to enterprise risk management. The program emphasizes three elements: converging CI community resources and driving innovation and markets to support cybersecurity risk management and resilience through use of the Cybersecurity Framework; connecting CI stakeholders to the national resilience effort through cybersecurity resilience advocacy, engagement and awareness; and coordinating CI cross-sector efforts to maximize national cybersecurity resilience. The $6 million enhancement, including 10 positions, is requested to manage and support this program and increase the number of evaluations completed.

Enhanced Cybersecurity Services
The ECS capability enables owners and operators of critical infrastructure to enhance the protection of their networks from unauthorized access, exfiltration, and exploitation by cyber threat actors. The requested enhancement of 24 positions and $3 million allows ECS to execute the operational processes and security oversight required to share sensitive and classified cyber threat information with qualified Commercial Service Providers that will enable them to better protect their customers who are critical infrastructure entities.

Regional Resiliency Assessment Program (RRAP)
The $5 million, including 11 positions, is requested to complete five additional cyber-centric RRAPs. Through these RRAPs, NPPD will identify cross-sector physical and cyber dependencies and interdependencies and better understand the consequences and cascading impacts of disruptions to lifeline sectors. We anticipate that the findings will provide valuable data about the energy, water, and transportation sectors and their reliance on cyber and communications infrastructure.

National Coordinating Center for Communications Operations
The proposed increase of three positions and $1 million in funding to the NCC will maintain 24x7 communications infrastructure response readiness and requirements coordination between FSLTT and industry responders. Due to the loss of staff previously provided to DHS from the Department of Defense on a non-reimbursable basis, the NCC will no longer be able to provide 24x7 readiness without these additional resources.

Infrastructure Design and Recovery Support
To support its role in PPD-21 and assignment in the National Disaster Recovery Framework, an increase of $3 million, including 10 positions, is requested to establish an IDRS function. This function will support the efforts of owners and operators to incorporate appropriate resilience measures into their critical infrastructure at all stages of that infrastructure's lifecycle, including the recovery phase following an event. Interacting with stakeholders throughout government and the critical infrastructure sectors, this function will set the stage for an informed national discussion on how to implement infrastructure resilience enhancements to combat high-priority challenges, including terrorist incidents, extreme weather, and aging and failing infrastructure.

Integrated Cybersecurity Operations

Increased connectivity has led to significant transformations and advances across our country and around the world. It has also increased complexity and exposed us to new vulnerabilities that can only be addressed by timely action and shared responsibility. Successful responses to dynamic cyber intrusions require coordination among DHS, the Departments of Justice (DOJ), State (DOS) and Defense (DOD), the Intelligence Community, the specialized expertise of Sector Specific Agencies such as the Department of the Treasury, private sector partners – who are critical to these efforts – and SLTT, as well as international partners, each of which has a unique role to play.

DHS is home to the National Cybersecurity and Communications Integration Center (NCCIC), a national nexus of cyber and communications integration. A 24x7 cyber situational awareness, incident response, and management center, NCCIC partners with all Federal departments and agencies, SLTT governments, private sector and, critical infrastructure owners and operators, and international entities. The NCCIC disseminates cyber threat and vulnerability analysis information and assists in initiating, coordinating, restoring, and reconstituting national security/emergency preparedness (NS/EP) telecommunications services and operates under all conditions, crises, or emergencies, including executing Emergency Support Function #2 - Communications Annex responsibilities under the National Response Framework.

The NCCIC also provides strategic cyber-threat analysis, through its United States Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) in conjunction with the National Infrastructure Coordinating Center (NICC), to reduce malicious actors exploiting vulnerabilities. Threat management decisions must incorporate cyber threats based on technological as well as non-technological factors, and consider the varying levels of security required by different activities. Since its inception in 2009, the NCCIC has responded to nearly a half million incident reports and released more than 37,000 actionable cybersecurity alerts to our public and private sector partners. In FY 2013, NCCIC received 228,244 public and private sector cyber incident reports, a 41 percent increase from 2012, and deployed 23 response teams to provide onsite forensic analysis and mitigation techniques to its partners. NCCIC issued more than 14,000 actionable cyberalerts in 2013, used by private sector and government agencies to protect their systems, and had more than 7,000 partners subscribe to the NCCIC/US-CERT portal to engage in information sharing and receive cyber threat warning information. .

Further demonstrating NPPD's commitment to greater unity of effort in strengthening and maintaining secure and resilient critical infrastructure against both physical and cyber threats, the NICC has moved its watch operations center to collocate with the NCCIC. The NICC is the information and coordination hub of a national network dedicated to protecting critical infrastructure essential to the nation's security, health and safety, and economic vitality. In accordance with and supporting the physical-cyber integration directives of PPD-21, this new integration will enhance effective information exchange, and improve the alacrity of protection with real-time indicator sharing. Concurrently, the NCCIC will refine and clarify the NICC-NCCIC relationship to advance national unity of effort within NPPD and the Federal Government.

Protecting Federal Networks

DHS directly supports federal civilian departments and agencies in developing capabilities that will improve their own cybersecurity posture. Through the Continuous Diagnostics and Mitigation (CDM) program, led by the NPPD Federal Network Resilience Branch, DHS enables Federal agencies to more readily identify network security issues, including unauthorized and unmanaged hardware and software; known vulnerabilities; weak configuration settings; and potential insider attacks. Agencies can then prioritize mitigation of these issues based upon potential consequences or likelihood of exploitation by adversaries.

Available to all Federal civilian agencies, the CDM program provides diagnostic sensors, tools, and dashboards that provide situational awareness to individual agencies and at a summary federal level. This allows agencies to target their cybersecurity resources toward the most significant problems, and enables comparison of relative cybersecurity posture between agencies based upon common and standardized information. The CDM contract can also be accessed by defense and intelligence agencies, as well as by State, local, tribal, and territorial (SLTT) governments. 108 departments and agencies are currently covered by Memoranda of Agreement with the CDM program, encompassing over 97 percent of all federal civilian personnel. In FY 2014, DHS issued the first delivery order for CDM sensors and awarded a contract for the CDM dashboard. The $143 million and 15 staff requested in FY 2015 will support deployment of the federal dashboard and capabilities to federal agencies.

In addition, the National Cybersecurity Protection System (NCPS), a key component of which is referred to as EINSTEIN, is an integrated intrusion detection, analytics, information sharing, and intrusion-prevention system utilizing hardware, software, and other components to support DHS responsibilities for protecting Federal civilian agency networks. In FY 2015, the program will expand intrusion prevention, information sharing, and cyber analytic capabilities at Federal agencies, marking a critical shift from a passive to an active role in cyber defense and the delivery of enterprise cybersecurity services to decision-makers across cybersecurity communities.

In July 2013, EINSTEIN 3 Accelerated (E^3A) became operational and provided services to the first Federal Agency. In FY 2014, we reached the initial milestone of deploying Intrusion Prevention capabilities at one Internet Service Provider to cover one Federal Executive Branch civilian network's traffic. As of February 2014, Domain Name System and/or email protection services are being provided to a total of seven departments and agencies. Full Operational Capability is planned for FY 2016. With the adoption of E^3A, DHS will assume an active role in defending .gov network traffic and significantly reduce the threat vectors available to malicious actors seeking to harm Federal networks. In FY 2015, $378 million is requested for NCPS. We will continue working with the Internet Service Providers to deploy intrusion prevention capabilities, allowing DHS to provide active, in-line defense for all federal network traffic protocols.

It is important to note that the Department has strong privacy, civil rights, and civil liberties standards implemented across its cybersecurity programs. DHS integrates privacy protections throughout its cybersecurity programs to ensure public trust and confidence. DHS is fully responsible and transparent in the way it collects, maintains, and uses personally identifiable information.

Data Security Breaches

On December 19, 2013, a major retailer publicly announced it had experienced unauthorized access to payment card data from the retailer's U.S. stores. The information involved in this incident included customer names, credit and debit card numbers, and the cards' expiration dates and card verification-value security codes. Another retailer also reported a malware incident

involving its point of sale system on January 11, 2014, that resulted in the apparent compromise of credit card and payment information. A direct connection between these two incidents has not been established.

During both incidents, NPPD's NCCIC utilized its unique cybersecurity, information sharing and mitigation capabilities to help retailers across the country secure their systems to prevent similar attacks while simultaneously providing timely analysis to the United States Secret Service (USSS). DHS's ability to provide a cross-component response during this incident underscores the importance of leveraging complementary missions at the Department, and highlights the interplay between the criminal aspects of malicious cyber activity and NPPD's increased focus on not just responding to incidents but also reducing vulnerabilities, protecting against future attacks, and mitigating consequences.

In response to this incident, NCCIC/US-CERT analyzed the malware identified by the USSS as well as other relevant technical data and used those findings, in part, to create two information sharing products. The first product, which is publicly available and can be found on US-CERT's website, provides a non-technical overview of risks to point of sale systems, along with recommendations for how businesses and individuals can better protect themselves and mitigate their losses in the event an incident has already occurred. The second product provides more detailed technical analysis and mitigation recommendations, and has been securely shared with industry partners to enable their protection efforts. NCCIC's goal is always to share information as broadly as possible, including by producing actionable products tailored to specific audiences.

While the criminal investigation into the these activities is on-going, NPPD, through the NCCIC and other organizations, continues to build shared situational awareness of similar threats among our private sector and government partners and the American public at large. At every opportunity, the NCCIC and our private sector outreach program publish technical and non-technical products on best practices for protecting businesses and customers against cyber threats and provide the information sharing and technical assistance necessary to address cyber threats as quickly as possible. DHS remains committed to ensuring cyberspace is supported by a secure and resilient infrastructure that enables open communication, innovation, and prosperity while protecting privacy, confidentiality, and civil rights and civil liberties by design.

Understanding Cyber and Physical Critical Infrastructure Interdependencies

One of NPPD's top priorities is providing our government and private sector partners with the information, analysis, and tools they need to protect our Nation's critical infrastructure in the face of physical and cyber risks. Key to this effort is understanding the consequences of potential disruptions to critical infrastructure, including interdependencies and cascading impacts, from all hazards to better equip and prepare our partners and stakeholders. Understanding consequences helps identify potential mitigation measures and prioritize the allocation of limited resources for both government and private sector.

NPPD has already demonstrated the impact of this enhanced coordination over the last year. For example, prior to the establishment of OCIA, the Homeland Security Infrastructure Threat and Risk Analysis Center (HITRAC) established the Integrated Analysis Cell to serve as the

intersection of NPPD's two operational centers: the National Infrastructure Coordinating Center (NICC) and National Cybersecurity and Communications Integration Center (NCCIC). The Integrated Analysis Cell has already made great strides integrating support within both the NICC and NCCIC. The ability to provide near-real time information to the NICC and the NCCIC is essential for our operational capabilities going forward and enhancing this capability will continue to be a key priority for NPPD. Similarly the work that has been done to implement Section 9 of EO 13636 through the Cyber-Dependent Infrastructure Identification Working Group exemplifies how the skills that have been developed in HITRAC over the years can now be applied to the new mission analyzing cyber infrastructure.

Integrating Cyber and Physical Analytic Capabilities

To advance this objective, NPPD established the Office of Cyber and Infrastructure and Analysis (OCIA) in February 2014. OCIA has an important role in DHS's efforts to implement PPD-21, which calls for integrated analysis of critical infrastructure, and EO 13636, identifying critical infrastructure where cyber incidents could have catastrophic impacts to public health and safety, the economy, and national security.

OCIA grew out of a pilot effort, the Integrated Analysis Task Force (IATF), which assessed the best approach for integrating analytic support for all CI sectors using an all hazards approach. To understand the potential physical consequences from a cyber-attack, IATF collaborated with the State of New Jersey at four Water and Wastewater Sector facilities to assess the facilities' systems and identify site-specific options to mitigate potential physical consequences that could stem from exploited cyber vulnerabilities within those systems. The resulting analyses were used to enhance security and resilience at a local level for these facilities, and provides a model for addressing similar issues in other regions and sectors. By integrating site-specific vulnerability information and related cyber-physical consequence analysis, OCIA is developing new and unique analyses that can serve a broad spectrum of critical infrastructure protection community partners and stakeholders.

Similarly, the IATF brought together experts from across Government, including the General Services Administration (GSA) and the location's new federal tenants, to evaluate the cyber-physical security and critical infrastructure resilience of a federal building in Southwest D.C. The joint assessment expanded awareness of existing data, capabilities, and assessment tools and fostered an integrated perspective for protecting federally owned or leased infrastructure from cyber, physical, and human threats. As a result of the joint assessment, NPPD has become more able to recognize and account for interconnections and dependencies of physical countermeasure equipment on IT and communication systems. Assessment participants investigated the ways in which various systems within the building interacted, and how each could be affected by an accidental or malicious cyber or other event. This exercise was of crucial importance given recent transitions to technologically sophisticated building control systems (i.e., Smart Buildings), which open the door to previously unconsidered vulnerabilities. Through this collaborative process, NPPD is generating new techniques and sharing lessons learned to ensure that cyber and physical considerations are addressed in a comprehensive, integrated manner.

In addition to these recent efforts which demonstrated NPPD's ability to integrate cyber and physical infrastructure analysis, OCIA will incorporate and build upon the established analytic

expertise of both Homeland Infrastructure Threat and Risk Analysis Center and the National Infrastructure Simulation and Analysis Center. $33 million is requested in FY 2015 to support these efforts.

Partnering Across the Homeland Security Enterprise

California Power Substation Attack and Subsequent Outreach Campaign
In response to the April 16, 2013 attack on a PG&E Company grid control center (Metcalf substation), NPPD initiated a campaign intended to raise security awareness across the Electricity Subsector. The campaign was conducted in close collaboration and coordination with the Department of Energy (DOE), Federal Bureau of Investigation, North American Electric Reliability Corporation, Federal Energy Regulatory Commission, and multiple industry partners. This campaign is taking place in ten U.S. and three Canadian cities, serving to raise awareness of the evolving risk environment and promoting increased collaboration on risk mitigation strategies, protective measures, and industry best practices. Information concerning this awareness campaign was posted to the Homeland Security Information Network, DHS's Web-based information sharing platform, which brings together homeland security partners across the spectrum.

NPPD also took part in a national drill involving more than 10,000 electrical engineers and cybersecurity specialists, among others, in November 2013 to exercise a response to approximately 40 simulated cyber attacks.

In addition to the extensive interagency efforts described above, IP has been conducting security assessments of electrical power and telecommunications facilities to provide stakeholders with best practices in access control, closed-circuit television usage, and intrusion detection systems and protective measures. This effort assists power companies by recommending security practices and protective measures, which are captured in the *Infrastructure Protection Report Series* that is broadly shared with critical infrastructure stakeholders.

NPPD, along with the DOE – which as the sector-specific agency for energy, works to protect against and mitigate threats to energy infrastructure – continues to coordinate national efforts to raise awareness about evolving threats and promote measures to reduce risks to systems such as the electric grid and system components such as electric substations. This effort is part of ongoing collaboration with industry to understand and reduce other physical and cyber risks to the energy sector and critical infrastructure.

Engaging with Federal, SLTT, and Private Sector Entities
NPPD is committed to engaging with Federal, SLTT, and private sector stakeholders. More than 1,100 participants were involved in the development of NIPP 2013, providing thousands of comments reflecting our partners' input and expertise. Through the Critical Infrastructure Partnership Advisory Council, IP plans to conduct more than 500 classified and unclassified meetings with critical infrastructure partners to share actionable information and recommend preventive measures about evolving threats, best practices, and requirements for risk mitigation capacity development in FY 2014. Protective Security Advisors (PSAs) proactively engage with SLTT government mission partners and members of the private sector stakeholder community to

protect the Nation's critical infrastructure, serving as DHS's onsite critical infrastructure and vulnerability assessment specialists. In FY 2015, PSAs will conduct more than 600 Enhanced Critical Infrastructure security surveys, which capture facility security data and track improvements made by facilities to enhance security and resilience. Finally, NPPD has become increasingly focused on engaging stakeholders at the executive level, and working with the DOE, will implement a sustained outreach strategy to energy sector Chief Executive Officers to elevate risk management of evolving physical and cyber threats to the enterprise level. NPPD will also explore similar efforts across the critical infrastructure community.

NPPD serves as a principal coordination point for stakeholder engagement for Cybersecurity through the Cyber Security Evaluation Program (CSEP). CSEP which provides voluntary evaluations intended to enhance cybersecurity capacities and capabilities across all 16 Critical Infrastructure Owner/Operators, as well as SLTT governments through its Cyber Resilience Review (CRR) process. The goal of the CRR is to develop an understanding and measurement of key cybersecurity capabilities and provide meaningful maturity indicators to an organization's operational resilience and ability to manage risk to its critical services during normal operations and times of operational stress and crisis.

The Office for Bombing Prevention (OBP), within NPPD's Office of Infrastructure Protection, 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 2014, OBP will conduct 250 capability assessments measuring progress toward Improvised Explosive Device (IED)-related national resilience and preparedness goals and used the capability data to conduct 10 Multi-Jurisdiction IED Security Planning sessions, 30 bomb-making materials assessment program events, and 250 IED awareness and risk mitigation training courses. The Technical Resource for Incident Prevention (TRIP*wire*) is an online information sharing resource on IED incidents, tactics, techniques, and procedures, as well as corresponding IED prevention and protective measures. TRIPwire provides law enforcement and first responders with unclassified IED information. There are more than 16,700 registered TRIPwire users, including 1,200 users added in FY 2013. In addition, OBP continues to lead DHS efforts in executing the national policy for Countering IEDs. In FY 2015, $8 million is requested for OBP, and the program is focused on moving towards more cost-effective, online and train-the-trainer courses to ensure IED awareness and risk mitigation.

Enhancing communications

The FY 2015 President's Budget includes $180 million for communications capabilities within NPPD.

NPPD provides a series of NS/EP and emergency communications capabilities required by National Security Presidential Directive-51/Homeland Security Presidential Directive-20, National Continuity Policy, and the 21st Century Emergency Communications Act of 2006 that support SLTT and private sector stakeholders. NPPD develops and maintains NS/EP communications priority services programs, which ensure commercial communications are available during a crisis to over 300,000 NS/EP users across all levels of government and first responders, even during heavy telecommunications usage/congestion.

EO13618, *Assignment of National Security and Emergency Preparedness Functions*, assigned DHS responsibility for ensuring priority communications requirements using commercial, government, and privately-owned communications resources. The Next Generation Networks-Priority Services (NGN-PS) program was established to ensure priority services will be available to NS/EP users as commercial telecommunications carriers transition from circuit-switched to Internet Protocol-based infrastructures. Over the long term, NGN-PS will deliver priority voice, video, and data communication services.

The FY 2015 President's Budget Request includes an enhancement of $48 million for NGN-PS, bringing total funding for the program to $70 million. This funding enables priority services to maintain the same degree of coverage across the United States regardless of the underlying technology. In FY 2015, NGN-PS services will be expanded to three long distance carriers' core networks. In addition to continuing the deployment into the carrier's core network, the budget request supports the transition of the Wireless Priority Services (WPS) infrastructure to Internet-based technologies through implementation of Phase 1, Increment 2 of the NGN-PS program.

The Government Emergency Telecommunications Service **(**GETS) program supports more than 310,675 FSLTT government, industry, and non-governmental organization personnel in performing their NS/EP communications missions by providing a mechanism to complete calls during network congestion from anywhere in the United States. WPS, which is the wireless complement to GETS, enhances the ability of 118,390 NS/EP subscribers to complete cellular phone calls through a congested wireless network during a crisis or emergency situation. In FY 2013, NPPD expanded the availability of WPS across multiple carriers and achieved a 97 percent call-completion rate during emergency situations.

NPPD is also supporting the implementation of the *Middle Class Tax Relief and Job Creation Act of 2012 (*Public Law 112-96), which established the Nationwide Public Safety Broadband Network for emergency responders at all levels of government. A DHS priority is to ensure resilience measures are built into the network as part of the design. DHS worked closely with industry and Federal stakeholders to develop a risk assessment of the network's physical and cybersecurity infrastructure and offered recommendations to ensure appropriate security measures are built in from the outset of the Network's deployment. In 2013, this risk assessment was provided to the First Responder Network Authority, or FirstNet, and the FirstNet Board on which the Secretary of DHS serves as one of three permanent members alongside the Attorney General of the United States, and the Director of the Office of Management and Budget.

DHS continues to aid in the advancement of FirstNet's deployment of a nationwide public safety broadband network through NPPD's Office of Emergency Communications (OEC) which leads 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 is working to identify Federal broadband requirements, preparing a consolidated view of emergency communications assets for potential use by FirstNet, and establishing standardized

grant guidance and processes to align with FirstNet's technical architecture. 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.

Securing High-Risk Chemical Facilities

NPPD secures America's high-risk chemical facilities through the systematic regulation, inspection, and enforcement under the authority of the Chemical Facility Anti-Terrorism Standards (CFATS). The CFATS rule establishes enforceable risk-based performance standards for the security of our Nation's highest risk chemical facilities. High-risk facilities have the flexibility to develop appropriate site-specific security measures that will effectively address risk by meeting these standards through Site Security Plans (SSPs) or, if the facility so chooses, through Alternative Security Programs (ASPs). In FY 2015, $87 million is requested for the Infrastructure Security Compliance Division (ISCD). ISCD will invest in enhancements to its internal information sharing platform and will improve its data analytic capabilities to better enable comparison between agency, State, and local lists of chemicals. Specifically, ISCD will run comparisons on the EPA Risk Management Program and the Superfund Amendments and Reauthorization Act Title III data from all 50 individual state data sets on an annual basis to identify facilities that are potentially non-compliant with the CFATS regulation. Each discrepancy between the data sets will then be investigated and resolved to ensure reporting facilities adhere to all regulatory obligations. In addition, ISCD will coordinate and work with each of the 50 State Emergency Response Commissions and the 3,000 (+) Local Emergency Planning Committees to ensure communities can meet their responsibilities in regard to potential chemical emergencies. Lastly, ISCD will coordinate inspections with EPA and Occupational Safety and Health Administration and participate in cross-training activities to integrate and improve the outreach of Federal regulatory programs.

NPPD continually evaluates the CFATS program to pinpoint areas for improvement and fine-tunes its processes when necessary to ensure efficient and effective implementation, resulting in continued forward progress for the program. The Department remains committed to working with Congress and stakeholders to build upon its successes.

As of April 1, 2014, CFATS covered 4,172 high-risk facilities nationwide; of these, 3,316 have received final high-risk determinations and are required to develop Site Security Plans (SSPs) or ASPs. Using a new, streamlined process, the ISCD has completed its initial review of all Tier 1, Tier 2, and Tier 3 SSPs; the Division has recently begun reviewing Tier 4 SSPs for authorization and approval. As of April 1, 2014, SSPs have been authorized for 107 of the 110 final Tier 1 facilities and 100 of those Tier 1 SSPs have been approved. ISCD is nearing completion of the Tier 2 SSPs as well. As of April 1, 2014, SSPs have been authorized for 263 of the 336 Tier 2 facilities, with 211 Tier 2 SSPs having been approved.

ASPs are also 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 April 1, 2014, approximately 450 ASPs have been submitted in lieu of SSPs. In addition to progress related to SSP and ASP approvals, ISCD began conducting compliance inspections in FY 2014. As of April 1, 2014, 19 compliance inspections have been conducted at Tier 1 facilities and three compliance inspections have been conducted at Tier 2 facilities.

In addition to carrying out the CFATS program, ISCD also is working to implement the Ammonium Nitrate Security Program. The Department is continuing to adjudicate comments received on the Ammonium Nitrate Security Program Notice of Proposed Rulemaking issued in August 2011 and is developing a final rule. The authorizing statute provides the Department with the authority to require individuals engaging in the purchase, sale, or transfer of ammonium nitrate to register with the Department and submit to vetting against the Terrorist Screening Database, and requires facilities transferring or selling ammonium nitrate to maintain records on such sales and transfers and report any identified thefts or losses of ammonium nitrate to appropriate authorities.

DHS/NPPD, along with the Environmental Protection Agency (EPA) and the Department of Labor, are the tri-chairs for the working group responsible for implementing EO 13650, *Improving Chemical Facility Safety and Security*, structured to identify ways to improve operational coordination with State and local partners; enhance Federal agency coordination and information sharing; modernize policies, regulations, and standards in order to enhance safety and security in chemical facilities; and work with stakeholders to identify best practices to reduce safety and security risks in the production and storage of potentially harmful chemicals.

Office of Biometric Identity Management

OBIM is the lead entity within DHS responsible for biometric identity management services. OBIM, through the Automated Biometric Identification System (IDENT) system, stores biometric identities and conduct recurrent matching against derogatory information, and analysts provide other biometric expertise and services to deliver accurate information to decision makers. By matching, storing, sharing, and analyzing biometric data, OBIM provides partners on the front lines of homeland security with rapid, accurate, and secure identification.

OBIM's current services consist of the biometric identity management and analysis capabilities that directly support agencies within DHS, as well as the Department of Justice; the Department of State; the DOD; the Intelligence Community; state, local, and tribal law enforcement, and foreign governments. OBIM also leads biometric standards development efforts and improves data sharing and interoperability between DHS and its partners. OBIM provides its customers with timely, accurate, and uninterrupted access to information on individuals to facilitate decisions on enforcing immigration laws, adjudicating immigration benefit requests, providing credentialing-related benefits or services, and granting or denying facility access rights. The services that OBIM provides broaden the scope of information available to OBIM users and leads to identifying tens of thousands of known or suspected terrorist (KST) and watch list matches every year in support of efforts to protect critical infrastructure and other DHS operations. In FY 2013, OBIM processed nearly 81 million total transactions with over two million watch list identifications, including 26,770 KST matches. Additionally, OBIM completed more than 4.6 million latent fingerprint comparisons with more than 1,200 identifications.

OBIM's total budget request for FY 2015 is $252 million. Of this total, $188 million is provided for the operations and maintenance (O&M) of IDENT, systems engineering, and other IT expenses. The request includes an enhancement of $28 million for implementation of IDENT system improvements. The increase will be used to leverage the existing DHS platform to simplify and integrate the server, network, and storage requirements associated with the system. Moreover, operational data storage will automate access to mission critical data extracted from external storage to meet OBIM stakeholder and customer requirements for data queries and reports.

Protecting Federal Facilities

FPS protects more than 9,000 GSA-owned, -leased, or -operated facilities, serving more than 1.1 million occupants, and receiving 1.4 million visitors per year. In this capacity, FPS conducts protective law enforcement and security services and leverages the intelligence and information resources of FPS' network of Federal, State, and local partners. FPS conducted almost 1,700 Facility Security Assessments in FY 2013 and continuously recommends appropriate countermeasures, ensures stakeholder threat awareness training, and oversees approximately 13,000 Protective Security Officers (PSO). FPS also responds to more than 40,000 calls for service annually, investigates a wide range of crimes related to Federal property and Federal employees, protects Federal facilities during national and local security special events, and provides protection services for disaster and emergency response.

During the last fiscal year, FPS responded to more than 45,700 incidents, made over 1,700 arrests, interdicted more than 781,000 weapons and prohibited items at Federal facility entrances during routine checks, conducted more than 50,400 post inspections, disseminated more than 300 threat and intelligence-based products to stakeholders, and investigated and addressed more than 900 threats and assaults directed towards Federal facilities and their occupants. Also in FY 2013, FPS delivered the first phase of a working cost model, which aligned costs to the activities performed by FPS for its customers. Through this effort, FPS stakeholders 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.

Additional priorities for FY 2014 and continuing through FY 2015 include: continued implementation of the Facility Security Assessment process; enhancing stakeholders' understanding of vulnerabilities and protective and mitigation strategies; and the institution of enhanced professional development training for law enforcement, management, and mission support personnel across DHS. FPS will continue to provide tailored recommendations for countermeasures and expand its countermeasure program to include closed-circuit television, Intrusion Detection Systems, and other technical countermeasures to standardize and create acquisition efficiencies.

FPS continues to enhance its facility assessment capability to integrate threats, vulnerabilities, and consequences to support risk-based facility protection decisions. Additionally, FPS is collaborating with the DHS Science and Technology Directorate on two efforts. The first involves the enhancement of explosives and weapons detection at checkpoints, to include the formation of partnerships with outside agencies. The second is to prototype a post tracking

system, automating the now manual process of ensuring that the contracted PSOs are working at a post, as scheduled, and that they possess the required training and certifications.

Conclusion

Infrastructure is the backbone of our nation's economy, security and health. We know it as the power we use in our homes, the water we drink, the transportation that moves us, and the communication systems we rely on for business and everyday life. We have an extremely dedicated and talented workforce engaged in activities that advance our mission and their innovation will continue to propel NPPD and DHS forward in FY 2015 and beyond. Each employee is dedicated to a safe, secure, and resilient infrastructure that enables our way of life to thrive.

Thank you, Chairman Carter, Ranking Member Price, and distinguished Members of the Subcommittee for the opportunity to discuss the FY 2015 President's Budget Request for NPPD. We look forward to any questions you may have.

Suzanne E. Spaulding

Under Secretary
National Protection and Programs Directorate
Department of Homeland Security

Suzanne E. Spaulding serves as Under Secretary for the National Protection and Programs Directorate at the Department of Homeland Security. As Under Secretary, she oversees the coordinated operational and policy functions of the Directorate's subcomponents: Offices of Cybersecurity and Communications, Infrastructure Protection, Biometric Identity Management, Cyber and Infrastructure Analysis, and the Federal Protective Service, with a mission to reduce the risk to -- and enhance the resiliency of -- critical infrastructure, secure Federal facilities, and advance identity management and verification.

Ms. Spaulding has spent nearly 25 years working on national security issues for both Republican and Democratic Administrations and on both sides of the aisle of Congress. She was most recently a principal in the Bingham Consulting Group and Counsel for Bingham McCutchen LLP in Washington, D.C. Prior to joining the private sector, she served as the minority staff director for the U.S. House of Representatives Permanent Select Committee on Intelligence for Ranking Member Jane Harman (D-CA), and as general counsel for the Senate Select Committee on Intelligence. She also spent six years at the Central Intelligence Agency (CIA) and served as senior counsel and legislative director for U.S. Senator Arlen Specter (PA).

In 2002, she was appointed by Virginia Governor Mark Warner to the Secure Commonwealth Panel, established after the attacks of September 11, 2001, to advise the governor and the legislature on preparedness issues in the Commonwealth of Virginia. Since then, Ms. Spaulding has worked with key critical infrastructure sectors including the nuclear power, electricity, and chemical sectors, and served as Security Counsel for the Business Roundtable

In addition, Ms. Spaulding served as the executive director of two congressionally mandated commissions: the National Commission on Terrorism, chaired by Amb. L. Paul Bremer III, and the Commission to Assess the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass Destruction, chaired by former CIA Director John Deutch. She was assistant general counsel at CIA, including a position as legal adviser to the Nonproliferation Center, and also spent several years in private practice.

In addition to running national commissions on terrorism and weapons of mass destruction, she has served on commissions on cybersecurity and homeland security, convened and participated in numerous academic and professional advisory panels, and is a frequent commentator in publications, media, and before Congress.

Ms. Spaulding was a Senior Fellow at George Washington University's Homeland Security Policy Institute. She is the former Chair of the American Bar Association's Standing Committee on Law and National Security, and founder of the Cybersecurity Legal Task Force.

Ms. Spaulding earned both her law degree and undergraduate degree at the University of Virginia.

Dr. Phyllis A. Schneck

Deputy Under Secretary for Cybersecurity and Communications
National Protection and Programs Directorate
Department of Homeland Security

Dr. Phyllis Schneck serves as the Deputy Under Secretary for Cybersecurity and Communications for the National Protection and Programs Directorate within the Department of Homeland Security (DHS). Dr. Schneck is the chief cybersecurity official for DHS and supports its mission of strengthening the security and resilience of the nation's critical infrastructure.

Dr. Schneck came to DHS from McAfee, Inc., where she was Chief Technology Officer for Global Public Sector. She was responsible for the technical vision for products and service for public sector as well as global threat intelligence, industrial control system security and telecom strategy.

Dr. Schneck has had a long and distinguished presence in the security and infrastructure protection community, serving as a Working Group Chair for the CSIS Commission on Cybersecurity for the 44th Presidency. Dr. Schneck was the Chairman of the Board of Directors for the National Cyber Forensics and Training Alliance, a partnership between corporations, government and law enforcement for cyber analysis to combat international cybercrime. She was also Vice Chairman of the NIST Information Security and Privacy Advisory Board and was recently named the Loyola University Maryland David D. Lattanze Center 2012 Executive of the Year. Dr. Schneck served eight years as chairman of the National Board of Directors of the FBI's InfraGard program and founding president of InfraGard Atlanta, growing the program from 2,000 members to more than 30,000 nationwide.

Named one of Information Security Magazine's Top 25 Women Leaders in Information Security, she holds seven information security patents and has six research publications in the areas of information security, real-time systems, telecom and software engineering.

Before joining McAfee, Dr. Schneck was Vice President of Research Integration for Secure Computing, where she conceived and built the early intelligence practice into a full Beta program for data as a service. She also worked as the Vice President of Enterprise Services for eCommSecurity; served as Vice President of Corporate Strategy for SecureWorks, Inc.; and, was Founder and Chief Executive Officer of Avalon Communications, a provider of real-time security technology that has since been acquired by SecureWorks, Inc.

Dr. Schneck earned her Ph.D. in Computer Science from Georgia Tech, and pioneered the field of information security and security-based high-performance computing at Georgia Tech. She previously held a seat on the Advisory Board of the Johns Hopkins University Department of Computer Science, served on the Steering Committee for the Sam Nunn Information Security Forum as well as a term on the Georgia Tech Advisory Board, and cofounded the Georgia Tech Information Security Center and the Georgia Electronic Commerce Association's Working Group on Information Security.

Last Updated: 12/3/13