Written Testimony

of

The Honorable Suzanne E. Spaulding
Under Secretary
National Protection and Programs Directorate
Department of Homeland Security

Dr. Ronald J. Clark
Deputy Under Secretary
National Protection and Programs Directorate
Department of Homeland Security

Dr. Phyllis A. Schneck
Deputy Under Secretary fo Cybersecurity and Communications
National Protection and Programs Directorate
Department of Homeland Security

Regarding

"Examining the Mission, Structure, and Reorganization Effort of the National Protection and Programs Directorate"

Before the
Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies
U.S. House of Representatives

October 7, 2015

Thank you, Chairman Ratcliffe, Ranking Member Richmond, and distinguished Members of the subcommittee. I appreciate the opportunity to appear before you today to discuss the Department's cyber and infrastructure protection mission and the proposed transformation of the National Protection and Programs Directorate (NPPD). The growing demand for NPPD services as a result of the evolving risks requires the organization to be prepared to address whatever challenges we face in the future. Therefore we are developing a plan that will strengthen our ability to carry out NPPD's mission.

NPPD's Cyber and Infrastructure Protection Mission

NPPD serves a critical role in homeland security by leading the national effort to secure and enhance the resilience of the Nation's infrastructure against cyber and physical risks. NPPD works with interagency partners as well as owners and operators of critical infrastructure in the private sector and state, local, tribal, and territorial government agencies to, collectively, maintain secure, functioning, and resilient infrastructure that is vital to public confidence and the Nation's safety, prosperity, and well-being.

I'd like to thank Members of this subcommittee for the continued recognition and support of this critical mission. In just the past year, the subcommittee demonstrated bi-partisan support for NPPD's mission by introducing legislation that enhanced authority for NPPD operations in the areas of cybersecurity and infrastructure protection, specifically chemical facility security. Through the leadership of this subcommittee, as well as Chairman McCaul and Ranking Member Thompson, these bills ultimately became law. Most recently, the subcommittee introduced legislation, which was passed by the House of Representatives to improve cybersecurity by encouraging voluntary information sharing between and amongst the private sector and NPPD's National Cybersecurity & Communications Integration Center (NCCIC). This important legislation would strengthen cybersecurity by enabling automated sharing of cyber threat indicators in a way that protects privacy and brings this important information together so that trends can be seen and malicious cyber activity can be better understood and detected. . I appreciate your continued support for our mission, and I am committed to continuing working with you to ensure we have the authority and tools necessary to succeed.

NPPD was initially created in 2007 as a headquarters component of the Department by combining several existing entities. Over the years, the mission has evolved and NPPD has taken on more operational responsibility; especially as threats have grown. Malicious cyber activity has become more sophisticated over time, requiring an equally sophisticated and agile response. Given the importance of the mission and the evolving risks to critical infrastructure, NPPD must transition to an operational focus that fully leverages the combined expertise, skills, information, and relationships throughout DHS.

Transforming NPPD

To accomplish this vision, DHS is proposing a transformation that will achieve three key priorities: 1) Greater unity of effort across the organization, particularly across cyber and physical threats, vulnerabilities, consequences, and mitigation; 2) Enhanced operational activity; and 3) Excellence in acquisition program management and other mission support functions. This transformation includes restructuring the organization; cultural, governance, and process

changes; further cementing the organization as an operational component within the Department, and changing our name to better reflect our mission.

DHS is proposing changes in the structure of the organization to enable enhancements in operations. In the new structure, operations would be carried out through three interconnected, operational directorates. This will allow for focused operations with the necessary coordination to ensure our operations mitigate risk in a holistic, comprehensive manner.

The first directorate, Infrastructure Security, will focus on activities to protect the Nation's infrastructure from cyber and physical risks by working with private and public sector owners and operators to build the capacity to assess and manage these risks. Through regionally-based field operations -- to include the Protective Security Advisors, Cyber Security Advisors, Regional Emergency Communications Coordinators, and the Chemical Security Inspectors -- Infrastructure Security will deliver training, technical assistance, and assessments directly to stakeholders to enable these owners and operators to increase security and resilience. This includes working with facilities that are often identified as soft targets because of their open access. The foundation of Infrastructure Security will include existing programs within the Office of Cybersecurity and Communications, including the Office of Emergency Communications, the Cyber Security Advisor program, and the Critical Infrastructure Cyber Community (C^3) Voluntary Program. In addition, Infrastructure Security will include programs currently within the Office of Infrastructure Protection, including the Protective Security Advisor program and the Chemical Facility Anti-Terrorism Standards program. It will also execute the Sector Specific Agency responsibilities for nine sectors and serve as the national coordinator for the remaining sectors.

The second operational directorate will focus on cyber-specific operations and DHS's responsibility to mitigate and respond to threats to information technology (IT) and communication assets, networks, and systems. Through an enhanced and elevated NCCIC, we would execute cyber-specific protection, prevention, mitigation, incident response and recovery operations for private and public sector partners, including protection of federal networks. The focus on this area of operational activity will ensure DHS is able to respond to malicious cyber activity at the speed demanded by the rapidly evolving threat, while closely aligning pre-incident prevention and protection with incident detection, response and recovery. The NCCIC will also collaborate with the other two operational directorates to ensure cyber operations and expertise support, and benefit from, the operational activity of those protecting federal facilities and building capacity with public and private-sector stakeholders.

The third operational directorate, the Federal Protective Service, will continue to focus on the direct protection of federal facilities, and those who work in and visit them, across the Nation, through integrated law enforcement and security operations. It will increase its focus on protecting cybersecurity aspects of federal facilities in coordination with the NCCIC. In addition, the Federal Protective Service will better integrate its field operations with field forces in Infrastructure Security to enable comprehensive security and resilience for our stakeholders, as well as co-locate incident management support with the combined watch functions of the NCCIC and the National Infrastructure Coordinating Center (NICC) to gain efficiencies and improve situational awareness.

To ensure coordinated execution of the mission and better integration among the three operational activities, we will combine existing elements to establish a mission support element for coordinated operations, joint operational planning, and integrated situational awareness. NPPD is currently piloting these enhancements to strengthen situational awareness and operational coordination using the National Infrastructure Coordinating Center as a foundation. We will use the results of the pilot to inform the establishment of permanent mechanisms for integrated situational awareness, coordinated operations, operational planning, and integrated continuity planning. The Office of Cyber and Infrastructure Analysis will support this important coordination function. In 2014, NPPD established the Office of Cyber and Infrastructure Analysis as a first step in integrating key risk-assessment activity, particularly with regard to understanding interdependencies and consequences across physical and cyber. This function will provide essential analysis to support coordinated operational planning and joint situational awareness. This integrated operations and watch function will serve as a critical element of the Department's counterterrorism mission in protecting critical infrastructure, including federal facilities and those who work in and visit them..

Enhanced operations will be supported through improved mission support functions. We will re-orient the roles of operational and mission support elements so operators are focused on operations and mission support elements are structured with appropriate authorities to effectively and efficiently support operations, consistent with the structure of other DHS Operating Components. We will change the way the organization executes and manages acquisition programs. DHS is proposing an Acquisition Program Management function to enable greater effectiveness and accountability in acquisition programs and ensure that operational programs have the tools required in a timely manner. These changes will also help us collaborate with the DHS Science and Technology Directorate to strengthen our ability to leverage innovation, research and development for DHS and national benefit. Aligning activities that provide oversight and accountability for these large acquisition programs will allow operational directorates to focus on executing daily operations with the confidence that their requirements are being met by a team of acquisitions professionals. In many instances, these acquisition professionals will continue to be co-located with the programs they support to ensure user requirements are well understood and being met.

We will also enable those carrying out day-to-day operations to focus on the mission by changing current business models for other management functions as well. Streamlining and centralizing management of business support functions will create efficiencies by reducing management layers and provide greater predictability and agility in meeting the needs of the workforce and of our operations. We will ensure the delivery of these services remains customer-focused by placing staff in the same location as the operators when their needs can best be met by in-person support. Centralizing management of these activities will support the goal of enabling operators to focus on operations while ensuring mission support elements are empowered to support the operators and effectively carry out our mission.

This proposed structure reflects the three priorities of the transition; but a critical part of the transformation to achieve these priorities includes an underlying support structure with updated processes and internal governance to ensure the organizational structure permits the necessary flexibility and integration of programs required to carry out NPPD's mission. In addition, the proposed structure will allow for enhanced operations and performance of its critical mission

with minimal requirements for new resources by identifying and implementing a series of efficiencies. In a time of growing mission demands and continued resource constraints, greater efficiencies are imperative and DHS is committed to ensuring that direct impacts to budget from the transformation are minimal. This approach can be achieved through the combination and co-location of similar functions, the establishment of a joint planning function that leverages existing planning resources in a coordinated manner, and a flattening of certain management functions.

Benefit to Stakeholders

Reducing risks to critical infrastructure is a joint effort between the private and public sectors. DHS is unable to carry out our mission without the support and participation of stakeholders within the public and private sectors, including critical infrastructure owners and operators, public safety and government officials at all levels of government, and our interagency partners. Therefore, this transformation is designed to directly benefit these stakeholders. Through the changes outlined above, DHS will be able to more effectively and efficiently leverage relationships to support operational activity by identifying, coordinating, managing, and countering physical and cyber risks to infrastructure.

DHS is committed to improving service delivery to customers by enhancing our staff presence outside D.C. and better integrating field activities. A more robust field force will directly engage with stakeholders located throughout the Nation and carry out operations at a local level. In order to create efficiencies, improve the delivery of services to public and private-sector customers in the field, and ensure DHS is addressing cybersecurity and infrastructure protection regional priorities, we will more fully integrate and support regional operations. To achieve the priorities of both enhancing operations and achieving a unity of effort across programs, we will use the results of an ongoing regional pilot project to inform a plan for aligning field forces into a more cohesive organization. By embracing a regionally-focused organizational framework, we can tailor the delivery of programs that reflect regional needs and that evolve as the capabilities of each region to mature and expand. This framework also will better position us to develop career path options for regional and headquarters-based employees.

In addition to our external stakeholders, this transformation will benefit the workforce. I am privileged to serve with the committed men and women of NPPD. Our workforce carries out the incredibly difficult and demanding mission of protecting our Nation's infrastructure, both cyber and physical. The hard work and dedication of our staff forms the backbone of our operations as we strive to meet evolving mission needs. Many of the ideas I have discussed above for this transformation came directly from our workforce, and our employees have served a critical role in this process by developing plans and recommendations. Our employees best know the requirements and demands of this mission; therefore, I value their input and feedback. Their efforts and continued role in this process will be all the more important as we move forward to strengthen our capabilities to carry out this challenging and evolving mission.

As we continue to develop NPPD's organizational structure and improve our governance processes to support are evolving mission, a new organizational name would support our efforts help create a more unified and strong sense of identity, enhance stakeholder outreach and reflect the operational activities NPPD employees carry out each day.

Next Steps

The plan for NPPD's transformation I have just outlined provides a clear path to further enhance and improve our ability to carry out the mission. However, our work is not yet complete. Senior executives are now working on action plans to further develop details for the proposed areas of change I named above. We are also working with our stakeholder community to ensure their feedback is incorporated into this organizational construct.

Several of the areas I have identified above will require Congressional action to amend existing law, seek approval of organizational changes, and enable the changes. I appreciate the opportunity to appear before you today to discuss our proposal and look forward to working with Members of Congress on the implementation of this plan. Your support to date has enabled NPPD to carry out our critical operations and make significant progress, in collaboration with our stakeholders, to protect the Nation's infrastructure. Together we can ensure DHS is best positioned to carry out the critical mission of cybersecurity and infrastructure protection now and in the future.

In closing, I would like to note that October is National Cybersecurity Awareness Month and next month, November, is Critical Infrastructure Security and Resilience Month. Every year we use these opportunities to raise awareness of the importance of the cybersecurity and infrastructure protection mission. This hearing is an important part of that dialogue and I thank you for the opportunity to testify before you today.

I look forward to your questions.