Statement for the Record

Jeanette Manfra
Assistant Secretary
Office of Cybersecurity and Communications
National Protection and Programs Directorate
U.S. Department of Homeland Security

FOR A HEARING ON

Interagency Cyber Cooperation:
Roles, Responsibilities and Authorities of the Department of Defense and Department of Homeland Security

BEFORE THE
SUBCOMMITTEE ON CYBERSECURITY
AND INFRASTRUCTURE PROTECTION OF THE HOUSE HOMELAND SECURITY COMMITTEE

&

THE SUBCOMMITTEE ON EMERGING THREATS OF THE HOUSE ARMED SERVICES COMMITTEE

Wednesday, November 14, 2018
Washington, DC

UNCLASSIFIED

Chairman Ratcliffe, Chairman Stefanik, Ranking Member Richmond, Ranking Member Langevin, and members of the Committees, thank you for today's opportunity to testify regarding the Department of Homeland Security's (DHS) ongoing and collaborative efforts to strengthen the cybersecurity of our Nation's critical infrastructure. Safeguarding and securing cyberspace is a core homeland security mission, and DHS's National Protection and Programs Directorate (NPPD) leads the Nation's efforts to ensure the security and resilience of our cyber and physical infrastructure.

NPPD is responsible for assisting agencies with the protection of civilian Federal Government networks and coordinating with other Federal agencies, as well as state, local, tribal, and territorial governments, and the private sector to defend our Nation's critical infrastructure from malicious cyber activity. We work to enhance cyber threat information sharing across the globe in order to help critical infrastructure entities and government agencies protect their cyber systems and quickly recover should such an attack occur. By bringing together all levels of government, the private sector, international partners, and the public, DHS protects against cybersecurity risks, improves our whole-of-government incident response capabilities, enhances information sharing of best practices and cyber threats, and strengthens resilience of our Nation's critical infrastructure.

Threat Assessment

Cybersecurity threats remain one of the most significant strategic risks for the United States, threatening our national security, economic prosperity, and public health and safety. We have seen advanced persistent threat actors, including cyber criminals, nation states and their proxies, increase the frequency and sophistication of malicious cyber activity. Our adversaries have been developing and using advanced cyber capabilities in attempts to undermine critical infrastructure, target our livelihoods and innovation, steal our national security secrets, and threaten our democracy.

Global cyber incidents, such as the "WannaCry" ransomware incident attributed to North Korea and the "NotPetya" malware incident attributed to the Russian military in May and June 2017, respectively, are examples of malicious actors leveraging cyberspace to create disruptive effects and cause economic loss. These incidents exploited known vulnerabilities in software commonly used across the globe. Prior to these events, DHS had already taken actions to help protect networks from similar types of attacks. NPPD's National Cybersecurity and Communications Integration Center (NCCIC) publishes a list of known software vulnerabilities and pushes this information out to stakeholders on a routine basis. Additionally, through requested vulnerability scanning, we helped stakeholders identify vulnerabilities on their networks so they could be patched before incidents and attacks occurred. Recognizing that not all users are able to install patches immediately, we shared additional mitigation guidance to assist network defenders. As the incidents unfolded, we led the Federal Government's asset response efforts, working with our interagency partners, in providing situational awareness, information sharing, malware analysis, and technical assistance to affected government and critical infrastructure entities.

In a series of incidents since at least May of last year, working with U.S. and international partners, DHS and the Federal Bureau of Investigation (FBI) have identified Russian government actors targeting government entities and businesses in the energy, nuclear, water, aviation, and critical manufacturing sectors. Consistent with Presidential Policy Directive 41 and the National Cyber Incident Response Plan, DHS, FBI, and ODNI led coordination of the Federal Government's incident response. Support was also provided by the Department of Energy (DOE) and the Department of Defense (DOD), certain elements of the Intelligence Community, and the Nuclear Regulatory Commission.

DHS assesses that this campaign ultimately collected information pertaining to industrial control systems (ICS) with the intent to gain access to ICS environments, and in minimal instances did develop access to the ICS environments. The intrusions have been comprised of two distinct categories of victims: (1) staging and (2) intended targets. Through the Department's incident response actions, we identified activities by Russian government actors to target certain entities that then become pivot points, leveraging existing relationships between the initial victim and the intended targets to hide their activity, as part of a multi-stage intrusion campaign to gain access to networks of our Nation's critical infrastructure. Based on our analysis and observed indicators of compromise, DHS has confidence that this campaign is still ongoing, and threat actors are actively pursuing their ultimate long-term campaign objectives. DHS and FBI continue to conduct incident response related to this activity and have published a joint technical alert and hosted public webinars to enable network defenders to identify and take action to reduce exposure to this malicious activity.

As another example of specific threats, the U.S. Government has received information from multiple sources—including public and private sector cybersecurity research organizations and allies—that cyber actors are exploiting large numbers of network infrastructure devices (e.g., routers, switches, firewall, and network-based intrusion detection system devices) worldwide since 2015. Earlier this year, DHS, FBI, and the United Kingdom's National Cyber Security Centre published a publicly-available joint technical alert attributing this activity to Russian state-sponsored actors. Targets are primarily government and private-sector organizations, critical infrastructure providers, and Internet service providers supporting these sectors. Several days after publication of the alert, an industry partner notified DHS and FBI of related malicious cyber activity in which the actors redirected certain queries to their own infrastructure and obtained sensitive information, which included the configuration files of networked devices. Russian state-sponsored actors are using compromised routers to conduct man-in-the-middle attacks to support espionage, extract intellectual property, maintain persistent access to victim networks, and potentially lay a foundation for future offensive operations.

Joint DOD and DHS Cybersecurity Efforts

The challenge of effectively coordinating homeland security and homeland defense missions is not new, but it is amplified and complicated by the global, borderless, interconnected nature of cyberspace where strategic threats can manifest in the homeland without advanced warning. DHS and DOD recently finalized an agreement which reflects the commitment of both Departments in collaborating to improve the protection and defense of the U.S. homeland from strategic cyber threats. This agreement clarifies roles and responsibilities between DOD and

DHS to enhance U.S. government readiness to respond to cyber threats and establish coordinated lines of efforts to secure, protect, and defend the homeland.

The roles and responsibilities of DOD and DHS are complementary but different. DOD must maintain the US military's ability to fight and win wars and project power in a contested environment or while under attack in any domain, including cyberspace. As the government lead for national risk management, DHS is responsible for leading overall government efforts to protect critical infrastructure and civilian federal government informational system. As a part of these missions, DHS is working with a range of partners to identify national critical functions and ensure their integrity and resilience by leading government efforts to integrate and coordinate cybersecurity risk management and assistance with state, local, tribal, and territorial, and private sector critical infrastructure partners. DHS is a focal point for sharing cyber threat indicators and information and is responsible for providing tools, services, and programs to reduce and mitigate the risk of catastrophic consequences stemming from cyber-attacks.

DHS and DOD are both committed to improving the protection and defense of the homeland from strategic cyber threats. Specifically, DHS and DOD are working to improve intelligence, indications, and warning of malicious cyber activity; strengthen the resilience of the highest priority national critical infrastructure; improve joint operations planning and coordination; improve joint incident response to significant cyber incidents; expand cooperation with State, local, tribal and territorial authorities; and improve joint defense of Federal networks.

DHS and DOD will achieve these objectives through three primary lines of effort. First, DOD and DHS are adopting a threat-informed, risk-based approach that ensures the resilient delivery of national critical functions and services, and denies strategic adversaries the ability to prevent delivery of such functions and services. DOD and DHS will jointly prioritize a set of high priority national critical functions and non-DOD owned mission critical infrastructure that is most critical to the military's ability to fight and win wars and project power. Second, DOD and DHS in coordination with the FBI and the intelligence community are collaborating to build a common understanding of strategic cyber threats that can empower private sector network defenders, critical infrastructure owners and operators, and government actors to improve resilience and integrity of national critical functions. Timely access to threat information related to adversary capabilities and intent is critical to understand and counter the risk facing our nation's critical infrastructure effectively. Third, DoD and DHS are coordinating to inform and mutually support respective planning and operational activities as appropriate for each Department's unique authorities. DHS's knowledge of the domestic risk landscape, its work with the private sector, can inform DOD's efforts to preempt, defeat, or deter malicious cyber activity targeting U.S. critical infrastructure. And, DOD's "defend forward" operations can inform and guide DHS efforts to anticipate adversary action and understand potential risks to critical infrastructure.

Cybersecurity Priorities

DHS, our government partners, and the private sector are committed to a more strategic and unified approach as we work to improve our Nation's overall defensive posture against

malicious cyber activity. In February 2013, Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, recognized that only a more integrated approach to managing risk would enable the Nation to counter malicious cyber activity targeting our critical infrastructure. In May of this year, DHS published a Department-wide Cybersecurity Strategy, providing DHS with a strategic framework to execute our cybersecurity responsibilities during the next five years.

This Administration has leaned forward even further, prioritizing the protection and defense of our people and economy from the range of threats that exist today, including those emanating from cyberspace. In September the President released the National Cyber Strategy which recognizes that cyberspace has become foundational to our American way of life. Last year, the President signed Executive Order (EO) 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. This Executive Order set in motion a series of assessments and deliverables to enable the improvement of our defenses and lower our risk to cyber threats.

EO 13800 requires continued examination of how the Federal Government and industry work together to protect our Nation's critical infrastructure, prioritizing deeper, more collaborative public-private partnerships in threat assessment, detection, protection, and mitigation. In collaboration with civilian, defense, and intelligence agencies, we have worked to identify authorities and capabilities that agencies could employ, soliciting input from the private sector, and developed recommendations to support the cybersecurity efforts of those critical infrastructure entities at greatest risk of attacks that could result in catastrophic impacts. It is only through this collective defense model that we will be successful against this threat.

Additionally, under EO 13800, DHS and DOE, in consultation with ODNI, and state and local governments, assessed the potential scope and duration of a prolonged power outage associated with a significant cyber incident and the readiness to manage its consequences. DOE and DHS are focused on closing identified gaps in order to build on the already robust collaboration between government and industry on electricity sector cybersecurity. Continuing to enhance these partnerships is critical to enhancing cybersecurity preparedness and response capabilities, limiting the potential scope and duration of a significant cyber incident, and reducing impacts to the critical national economy, defense, and lifeline functions which the electric grid supports.

Department of Homeland Security's Cybersecurity Responsibilities

In accordance with the *Homeland Security Act of 2002*, as amended, the *National Cybersecurity Protection Act of 2014*, the *Federal Information Security Modernization Act of 2014*, the *Cybersecurity Act of 2015*, and Presidential Policy Directives 21 and 41, among other authorities and directives, DHS leads the Federal Government's efforts to enhance the cybersecurity and resilience of our Nation's critical infrastructure. As the next legislative step, we must ensure that NPPD is appropriately organized to address cybersecurity threats both now and in the future. Therefore, we urge the House to bring the Cybersecurity and Infrastructure Security Agency Act to the floor for final passage. This legislation would establish a cybersecurity agency at DHS, and realign NPPD to ensure it is focused on the core mission.

NPPD's NCCIC operates at the intersection of the private sector, state and local governments, federal departments and agencies, international partners, law enforcement, and intelligence and defense communities. The *Cybersecurity Information Sharing Act of 2015* established DHS as the Federal Government's central hub for the automated sharing of cyber threat indicators and defensive measures. The NCCIC's automated indicator sharing (AIS) capability allows the Federal Government and the private sector network defenders to share technical information at machine speed. The NCCIC also provides entities with information, technical assistance and guidance they can use to secure their networks, systems, assets, and information by reducing vulnerabilities and ensuring resilience to cyber incidents. DHS does this in a way that protects privacy and civil liberties.

NPPD's NCCIC provides a broad range of capabilities to assist private sector entities across all 16 sectors of critical infrastructure. In addition to information sharing and incident response, these capabilities include assessments and technical services that include recommended remediation and mitigation techniques that improve the cybersecurity posture of our Nation's critical infrastructure. Among other services, these include vulnerability scanning and testing, penetration testing, phishing assessments, and red teaming on operational technology that includes the industrial control systems that operate our Nation's critical infrastructure.

While DHS makes available to our Nation's critical infrastructure owners and operators unclassified and classified cyber threat information as well as a full range of technical assistance capabilities, DHS also closely coordinates with our federal partners, including Sector-Specific Agencies. For instance, the DOE is the Sector Specific Agency for the energy sector. DHS and DOE cooperate on a range of cybersecurity matters, particularly regarding information sharing, incident response, and research and development. NPPD's NCCIC works closely with DOE and the Energy Sector's Electricity Information Sharing and Analysis Center and Oil and Natural Gas Information Sharing and Analysis Center to share actionable information. We work closely with DOE to ensure we do not duplicate resources in areas such as incident response or information sharing, but also to ensure we leverage DOE's unique relationships and capabilities in the sector.

NPPD also funds work at the Idaho National Lab to enhance the cybersecurity of our Nation's industrial control systems that operate critical infrastructure, such as the electricity grid. This work includes a biannual conference with experts from across the industrial control systems cybersecurity community to ensure information and experience is shared across this community. In addition to assessments and sharing of technical cyber threat information, through Idaho National Lab, NPPD provides extensive hands-on training to the critical infrastructure owners and operators on protecting and securing industrial control systems from cyber-attacks and includes a red team/blue team exercise conducted within an actual control systems environment.

National Risk Management

We face an urgent, evolving crisis in cyberspace. Our adversaries' capabilities online are outpacing our stove-piped defenses. Working together with the private sector and our government partners, we are addressing this problem and taking collective action against

malicious cyber actors. Specifically, there is a need to enhance and promote the Department's cross-sector, cross-government coordination on critical infrastructure security and resilience.

We must improve our focus on examining the critical functions that drive our economy and facilitate national security. In other words, we need to continually advance our ability to organize and collaborate on risk strategies, planning, and solutions. For many years, DHS has worked closely with the private sector, but it has become clear that it must be a focal point for turning threat intelligence into joint action.

At the Department's first National Cybersecurity Summit this summer, in response to a clear demand signal and after extensive consultation with industry and government partners, Secretary Nielsen announced the rebranding of the Office of Cyber and Infrastructure Analysis as the National Risk Management Center (NRMC). Housed within DHS, the NRMC is the logical evolution of the ongoing improvements made over the last several years in information sharing and partnership building between the government and industry. The NRMC draws on existing resources and functions from across NPPD, the Department and our Federal and international partners to bring our risk management efforts to the next level of effectiveness.

The NRMC's mission is to enable analysts and planners, from both public and private sector, to jointly assess our country's cyber risks, plan to combat those risks and—most importantly—enable implementation of tailored solutions to protect our networks. The full expertise of the Federal Government should be brought to bear on these challenges.

Perhaps most importantly, the NRMC's core mission focuses on the systems or functions that cut across sectors. Ultimately, the NRMC will facilitate a partnership among and across government and industry that can provide a unified, collective approach to the defense that the nation needs to achieve superiority over our adversaries.

The NCCIC and National Infrastructure Coordination Center (NICC) will continue to carry out current operations, and the NRMC will enhance their efforts. The NRMC will support NCCIC and NICC operations by helping with prioritization and other needs, while also looking ahead to plan more strategically, and leveraging feedback from operations and other partners.

Conclusion

In the face of increasingly sophisticated threats, DHS employees lead efforts to defend our Nation's critical infrastructure from cyber threats. Our infrastructure environment today is complex and dynamic with interdependencies that add to the challenge of securing and making it more resilient. Clearly, we cannot do this unless we work together with our interagency partners, and use all available capabilities, people, and information. DHS remains committed to leading this effort while working hand in hand with our interagency partners to leverage every tool we have available. Further, as new threats emerge, we redouble our efforts. Expertise in cyber-physical risk assessments and cross-sector critical infrastructure interdependency evaluation is where NPPD brings unique experience and capabilities.

Thank you for the opportunity to appear before the Committee today, and I look forward to your questions.