Statement for the Record

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

Before the
United States Senate
Committee on Homeland Security and Government Affairs

Regarding

Mitigating America's Cybersecurity Risk

April 24, 2018

Chairman Johnson, Ranking Member McCaskill, and members of the Committee, thank you for the opportunity to testify before you today. The Department of Homeland Security (DHS) serves a critical role in safeguarding and securing cyberspace, a core homeland security mission. The National Protection and Programs Directorate (NPPD) at DHS leads the Nation's efforts to ensure the security and resilience of our cyber and physical infrastructure. Last month, this Committee reported favorably on H.R. 2825, the *Department of Homeland Security Authorization Act* (as amended). This bill includes the language from H.R. 3359, the *Cybersecurity and Infrastructure Security Agency Act of 2017*. If enacted, this language would mature and streamline NPPD and rename our organization to reflect clearly our essential mission and our role in securing cyberspace. The Administration strongly supports establishing the Cybersecurity and Infrastructure Security Agency within DHS, and we will continue working with this Committee and the rest of the Senate to get the necessary legislation enacted.

NPPD is responsible for protecting civilian Federal government networks and collaborating with other Federal agencies, as well as State, local, tribal, and territorial governments, and the private sector to defend against cyber threats. We endeavor to enhance cyber threat information-sharing across the globe to stop cyber incidents before they start and help businesses and government agencies to 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, we are taking action to protect against cybersecurity risks, improve our whole-of-government incident response capabilities, enhance information sharing of best practices and cyber threats, and to strengthen resilience.

Threats

Cyber threats remain one of the most significant strategic risks for the United States, threatening our national security, economic prosperity, and public health and safety. Malicious cyber activity causes impacts to infrastructure across both the virtual and physical domains. We have recently experienced a turning point in the cyber domain, at least in the public consciousness. We have long been confronted with myriad attacks against our digital networks. Americans have seen advanced persistent threat actors, including hackers, cyber criminals, and nation states, increase the frequency and sophistication of these attacks. Our adversaries have been developing and using advanced cyber capabilities 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 and the "NotPetya" malware incident 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, NPPD had already taken actions to help protect networks from similar types of attacks. Through requested vulnerability scanning, NPPD helped stakeholders identify vulnerabilities on their networks so they could be patched before incidents and attacks occur. Recognizing that not all users are able to install patches immediately, NPPD shared additional mitigation guidance to assist network defenders. As the incidents unfolded, NPPD led the Federal government's incident response efforts, working with our interagency partners, including

providing situational awareness, information sharing, malware analysis, and technical assistance to affected entities.

In a series of incidents since at least May of last year, working with U.S. and international partners, DHS and FBI have identified Russian government actors targeting government entities and businesses in the energy, nuclear, water, aviation, and critical manufacturing sectors. DHS assesses that this campaign ultimately collected information pertaining to industrial control systems with the intent to gain access to industrial control systems environments. The intrusions have targeted two distinct categories of victims: staging and intended targets. In other words, through the Department's incident response actions, we have observed this advanced persistent threat actor 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 major, high-value assets that operate components 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 the FBI continue to conduct incident response related to this activity and have published a joint technical alert to enable network defenders to identify and take action to reduce exposure to this malicious activity.

Cybersecurity Priorities

This Administration has prioritized protecting and defending our public and economic safety from the range of threats that exist today, including those emanating from cyberspace. Last year, the President signed Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. This Executive Order set in motion a series of assessments and deliverables to understand how to improve our defenses and lower our risk to cyber threats. This order also emphasized the importance of accountability–clarifying that department and agency heads are responsible and will be held accountable for the security of their networks and systems. NPPD plays an important role in providing capabilities, services, and direction to Federal agencies.

Across the Federal Government, agencies have been implementing action plans to use the industry-standard National Institute of Standards and Technology (NIST) Cybersecurity Framework. Agencies are reporting to DHS and the Office of Management and Budget (OMB) on their cybersecurity risk mitigation and acceptance choices. In coordination with OMB, DHS is evaluating the totality of these Agency reports in order to comprehensively assess the adequacy of the Federal Government's overall cybersecurity risk management posture.

Although Federal agencies have primary responsibility for their own cybersecurity, DHS provides a common set of security tools that helps agencies manage their cyber risk. NPPD's assistance to Federal agencies includes (1) providing tools to safeguard civilian executive branch networks through the National Cybersecurity Protection System (NCPS), which includes "EINSTEIN" and Continuous Diagnostics and Mitigation (CDM) programs, (2) measuring and motivating agencies to implement policies, directives, standards, and guidelines, (3) serving as a hub for information sharing and incident reporting, and (4) providing operational and technical

assistance, including threat information dissemination and risk and vulnerability assessments, as well as incident response services. NPPD's National Cybersecurity and Communications Integration Center (NCCIC) is the civilian government's hub for cybersecurity information sharing, asset incident response, and coordination for both critical infrastructure and the Federal government.

EINSTEIN refers to the Federal Government's suite of signature-based intrusion detection and prevention capabilities that protects agencies' unclassified networks at the perimeter of each agency. EINSTEIN provides situational awareness of civilian executive branch network traffic, so threats detected at one agency are shared with all others providing agencies with information and capabilities to more effectively manage their cyber risk. The Federal Government could not achieve such situational awareness through individual agency efforts alone.

Moving forward, leveraging existing investments, our non-signature based pilot efforts to move beyond current reliance on signatures are yielding positive results in the discovery of previously unidentified malicious activity. DHS is demonstrating the ability to capture data that can be rapidly analyzed for anomalous activity using technologies from commercial, government, and open sources. The pilot efforts are also defining the future operational needs for tactics, techniques, and procedures as well as the skill sets and personnel required to operationalize the non-signature based approach to cybersecurity.

State, local, tribal, and territorial governments are able to access intrusion detection and analysis services through the Multi-State Information Sharing and Analysis Center (MS-ISAC). MS-ISAC's service, called "Albert," closely resembles some EINSTEIN capabilities. While the current version of Albert cannot actively block known cyber threats, it does alert cybersecurity officials to an issue for further investigation. DHS worked closely with MS-ISAC to develop the program and considers MS-ISAC to be a principal conduit for sharing cybersecurity information with state and local governments.

EINSTEIN, the Federal Government's tool to address perimeter security, will not block every threat; therefore, it must be complemented with systems and tools working inside agency networks—as effective cybersecurity risk management requires a defense-in-depth strategy that cannot be achieved through only one type of tool. CDM program provides cybersecurity tools and integration services to all participating agencies to enable them to improve their respective security postures by reducing the attack surface of their networks as well as providing DHS with enterprise-wide visibility through a common federal dashboard.

CDM is helping us achieve two major advances for federal cybersecurity. First, agencies are gaining visibility, often for the first time, into the extent of cybersecurity risks across their entire network. With enhanced visibility, they can prioritize the mitigation of identified issues based upon their relative importance. Second, with the summary-level agency-to-federal dashboard feeds, the NCCIC will be able to identify systemic risks across the civilian executive branch more effectively and closer to real-time. For example, the NCCIC currently tracks government-wide progress in implementing critical patches via agency self-reporting and manual data calls. CDM will transform this, enabling the NCCIC to immediately view the prevalence of

a given software product or vulnerability across the federal government so that the NCCIC can provide agencies with timely guidance on their risk exposure and recommended mitigation steps. Effective cybersecurity requires a robust measurement regime, and robust measurement requires valid and timely data. CDM will provide this baseline of cybersecurity risk data to drive improvement across the civilian executive branch.

DHS conducts a number of activities to measure agencies' cybersecurity practices and works with agencies to improve risk management practices. The Federal Information Security Modernization Act of 2014 (FISMA) provided the Secretary of Homeland Security with the authority to develop and oversee implementation of Binding Operational Directives (BOD) to agencies. In 2016, the Secretary issued a BOD on securing High Value Assets, or those assets, federal information systems, information, and data for which unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to U.S. national security interests, foreign relations, the economy, or to the public confidence, civil liberties, or public health and safety of the American people. NPPD works with interagency partners to prioritize High Value Assets for assessment and remediation activities across the federal government. For instance, NPPD conducts security architecture reviews on these High Value Assets to help agencies assess their network architecture and configurations.

As part of the effort to secure High Value Assets, DHS conducts in-depth vulnerability assessments of prioritized agency assets to determine how an adversary could penetrate a system, move around an agency's network to access sensitive data, and exfiltrate such data without being detected. These assessments include services such as penetration testing, wireless security analysis, and "phishing" evaluations in which DHS hackers send emails to agency personnel and test whether recipients click on potentially malicious links. DHS has focused these assessments on federal systems that may be of particular interest to adversaries or support uniquely significant data or services. These assessments provide system owners with recommendations to address identified vulnerabilities. DHS provides these same assessments, on a voluntary basis upon request, to private sector and State, local, Territorial, and Tribal partners. DHS also works with the General Services Administration to ensure that contractors can provide assessments that align with our HVA initiative to agencies.

Another BOD issued by the Secretary directs civilian agencies to promptly patch known vulnerabilities on their Internet-facing systems that are most at risk from their exposure. The NCCIC conducts cyber hygiene scans to identify vulnerabilities in agencies' internet-accessible devices and provides mitigation recommendations. Agencies have responded quickly in implementing the Secretary's BOD and have sustained this progress. When the Secretary issued this directive, NPPD identified more than 360 "stale" critical vulnerabilities across federal civilian agencies, which means the vulnerabilities had been known for at least 30 days and remained unpatched. Since December 2015, NPPD has identified an average of less than 40 critical vulnerabilities at any given time, and agencies have addressed those vulnerabilities rapidly once they were identified. By conducting vulnerability assessments and security architecture reviews, NPPD is helping agencies find and fix vulnerabilities and secure their networks before an incident occurs.

In addition to efforts to protect government networks, Executive Order 13800 continues to examine how the 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 are identifying authorities and capabilities that agencies could employ, soliciting input from the private sector, and developing recommendations to support the cybersecurity efforts of those critical infrastructure entities at greatest risk of attacks that could result in catastrophic impacts. DHS coordinates closely with the Sector Specific Agencies across all 16 critical infrastructure sectors by leveraging their sector expertise to improve cybersecurity resiliency and risk management.

For instance, by sharing information quickly and widely, we help all partners block cyber threats before damaging incidents occur. Equally important, the information we receive from partners helps us identify emerging risks and develop effective protective measures.

Congress authorized the NCCIC as the civilian hub for sharing cyber threat indicators and defensive measures with and among federal and non-federal entities, including the private sector. As required by the Cybersecurity Act of 2015, we established a capability, known as Automated Indicator Sharing (AIS), to automate our sharing of cyber threat indicators in real-time. AIS protects the privacy and civil liberties of individuals by narrowly tailoring the information shared to that which is necessary to characterize identified cyber threats, consistent with longstanding DHS policy and the requirements of the Act. AIS is a part of the Department's effort to create an environment in which as soon as a company or federal agency observes an attempted compromise, the indicator is shared in real time with all of our partners, enabling them to protect themselves from that particular threat. This real-time sharing capability can limit the scalability of many attack techniques, thereby increasing the costs for adversaries and reducing the impact of malicious cyber activity. An ecosystem built around automated sharing and network defense-in-depth should enable organizations to detect and thwart the most common cyber-attacks, freeing their cybersecurity staff to concentrate on the novel and sophisticated attacks. More than 129 agencies and private sector partners have connected to the AIS capability. Notably, partners such as information sharing and analysis organizations and computer emergency response teams further share with or protect their customers and stakeholders, significantly expanding the impact of this capability. AIS is still a new capability and we expect the volume of threat indicators shared through this system to substantially increase as the technical standards, software, and hardware supporting the system continue to be refined and put into full production. This information sharing environment will become more robust and effective as more indicators are shared from other federal agencies; State, local, Territorial, and Tribal governments; and the private sector.

Another part of the Department's overall information sharing effort is to provide federal network defenders with the necessary context regarding cyber threats to prioritize their efforts and inform their decision making. DHS's Office of Intelligence and Analysis has collocated analysts within the NCCIC responsible for continuously assessing the specific threats to federal networks using traditional all source methods and indicators of malicious activity so that the NCCIC can share with federal network defenders. Analysts and personnel from the Departments of Energy, the Treasury, Health and Human Services, and Defense join the FBI and others who

are also collocated within the NCCIC and working together to understand the threats and share information with their sector stakeholders, pursuant to NPPD policies that provide appropriate privacy, civil liberties and confidentiality protections.

Mitigating Cyber Risks

We continue to adapt to the evolving risks to critical infrastructure, and prioritize our services to mitigate those risks. For instance, the Department recently took action regarding specific products which present a risk to federal information systems.

After careful consideration of available information and consultation with interagency partners, BOD 17-01 was issued that directed Federal Executive Branch departments and agencies to take actions related to the use or presence of information security products, solutions, and services supplied directly or indirectly by AO Kaspersky Lab or related entities. The BOD called on departments and agencies to identify any use or presence of Kaspersky products on their information systems in the next 30 days, to develop detailed plans to remove and discontinue present and future use of the products within 60 days, and at 90 days from the date of the directive, unless directed otherwise by DHS based on new information, to begin to implement the agency plans to discontinue use and remove the products from federal information systems. This action is based on the information security risks presented by the use of Kaspersky products on federal IT systems.

The Department provided an opportunity for Kaspersky to submit a written response addressing the Department's concerns or to mitigate those concerns, and Kaspersky submitted a written response. The Department wanted to ensure that the company had a full opportunity to provide any evidence, materials, or data that may be relevant. This opportunity was also available to any other entity that claimed its commercial interests will be directly impacted by the directive.

While the information and communications technology supply chain is not the source of all cyber risk, it presents an opportunity for creation of threats and vulnerabilities. Commercial technology is ubiquitous in federal networks, even those that handle the most sensitive information and support essential functions of the government. DHS—through its work with the Department of Defense and the intelligence community to identify key supply chain risks—has established a Cyber Supply Chain Risk Management initiative. Due to the increasing connectivity of the world and the growing sophistication of threats, this initiative will identify and mitigate supply chain threats and vulnerabilities related to High Value Assets.

Election Security

NPPD is committed to ensuring a coordinated response from DHS and its federal partners to plan for, prepare for, and mitigate risk to election infrastructure. We understand that working with election infrastructure stakeholders is essential to ensuring a more secure election. Based on our assessment of activity observed in the 2016 elections, NPPD and our stakeholders are increasing awareness of potential vulnerabilities and providing capabilities to enhance the security of U.S. election infrastructure as well as that of our democratic allies.

As mentioned before, under the Constitution and our system of laws, federal elections are administered by state and local election officials in thousands of jurisdictions. Security awareness for election officials did not begin in 2016, State and local election officials across the country have a long-standing history of working both individually and collectively to reduce risks and ensure the integrity of their elections. In partnering with these officials through both new and existing, ongoing engagements, NPPD is working to provide value-added–yet voluntary–services to support their efforts to secure elections.

This year our Nation is in the midst of primary and special elections as well as the general election in November. We have been working with election officials in all states to enhance the security of their elections by offering support and by establishing essential lines of communications at all levels–public and private–for reporting both suspicious cyber activity and incidents. This information sharing is critical and our goal is to enhance transparency and have visibility of aggregated elections-related cybersecurity efforts. We are also working with election officials, vendors, the Election Assistance Commission (EAC), and NIST to characterize risk to election systems and ensure appropriate mitigations are understood and available in the marketplace. As a part of this process, we work with these stakeholders to recommend best practices to ensure a secure and verifiable vote.

Over the course of the last year, DHS has made tremendous strides and has been committed to working collaboratively with those on the front lines of administering our elections—state and local election officials and the vendor community—to secure election infrastructure from risks. The establishment of government and sector coordinating councils will build the foundations for this enduring partnership not only in 2018, but for future elections as well. We will remain transparent as well as agile in combating and securing our physical and cyber infrastructure. However, we recognize that there is a significant technology deficit across State and local governments, and State and local election systems, in particular. It will take significant and continual investment to ensure that systems are upgraded and secure or vulnerable systems are retired.

We recognize the fundamental link between public trust in our election infrastructure and the confidence the American public places in basic democratic functions. Ensuring the security of our electoral process is a vital national interest and one of our highest priorities at DHS. Our voting infrastructure is diverse, subject to local control, and has many checks and balances. As the threat environment evolves, DHS will continue to work with federal agencies, state and local partners, and private sector entities to enhance our understanding of the threat; and to make essential physical and cybersecurity tools and resources available to the public and private sectors to increase security and resiliency.

Conclusion

In the face of increasingly sophisticated threats, NPPD stands on the front lines of the federal government’s efforts to defend our nation’s critical infrastructure from natural disasters, terrorism and adversarial threats, and technological risk such as those caused by cyber threats. Our infrastructure environment today is complex and dynamic with interdependencies that add to

the challenge of securing and making it more resilient. Technological advances have introduced the "Internet of Things" and cloud computing, offering increased access and streamlined efficiencies, while increasing our footprint of access points that could be leveraged by adversaries to gain unauthorized access to networks. As our nation continues to evolve and new threats emerge, we must integrate cyber and physical risk in order to understand how to effectively secure it. Expertise around cyber-physical risk and cross-sector critical infrastructure interdependencies is where NPPD brings unique expertise and capabilities.

We must ensure that NPPD is appropriately organized to address cybersecurity threats both now and in the future, and we appreciate this Committee's leadership in working to establish the Cybersecurity and Infrastructure Security Agency. As the Committee considers these issues, we are committed to working with Congress to ensure that this effort is done in a way that cultivates a safer, more secure and resilient Homeland.

Thank you for the opportunity to testify, and I look forward to any questions you may have.