Statement for the Record

of

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

Before the
U.S. House of Representatives
Subcommittee on Information Technology
Subcommittee on Government Operations
Committee on Oversight and Government Reform

Regarding

State of Play: Federal IT in 2018

March 14, 2018

Chairman Hurd, Chairman Meadows, Ranking Member Kelly, Ranking Member Connolly, and members of the Subcommittees, thank you for today's opportunity to discuss the state of federal cybersecurity. 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. This past December, the House voted favorably on H.R. 3359, the "Cybersecurity and Infrastructure Security Agency Act of 2017." If enacted, this bill would mature and streamline NPPD, renaming our organization as the Cybersecurity and Infrastructure Security Agency to clearly reflect our essential mission and role in securing cyberspace. The Department strongly supports this much-needed legislation and encourages swift action by Congress to complete its work on this legislation.

NPPD is responsible for collaborating with federal agencies to protect civilian federal government networks, as well as with the Intelligence Community; law enforcement; 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 incident 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 on best practices and cyber threats, and strengthen resilience.

Threats

Cyber threats remain one of the most significant and constant strategic risks for the United States, putting our national security, economic prosperity, and public health and safety at risk. We have long been confronted with a myriad of attacks against our digital networks. But over the past year, Americans saw malicious 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. Through vulnerability scanning, NPPD helped federal agencies and other stakeholders identify vulnerabilities on their networks so they could be patched before the incidents occurred. Recognizing that not all users are able to install patches immediately, NPPD shared additional mitigation guidance to assist network defenders.

Since 2009, cyber actors of the North Korean government have targeted the media, aerospace, financial, and critical infrastructure sectors in the United States and globally. The

U.S. Government refers to the malicious cyber activity by the North Korean government as HIDDEN COBRA. Commercial reporting has referred to this activity as Lazarus Group and Guardians of Peace. DHS and FBI have generated analytic products to provide information to network defenders to assist with the detection of malicious network activity. The analytic products provide technical details on the tools and infrastructure used by cyber actors of the North Korean government. Working with U.S. Government partners, DHS and FBI identified Internet Protocol (IP) addresses associated with a malware variant, known as DeltaCharlie, used to manage North Korea's distributed denial-of-service (DDoS) botnet infrastructure. These actors have leveraged their capabilities to target and compromise a range of victims; some intrusions have resulted in the exfiltration of data while others have been disruptive in nature. Tools and capabilities used by HIDDEN COBRA actors include DDoS botnets, keyloggers, remote access tools (RATs), and wiper malware. Variants of malware and tools used by HIDDEN COBRA actors include Destover, Wild Positron/Duuzer, and Hangman. DHS previously released a technical alert, which contains additional details on the use of a server message block (SMB) worm tool employed by these actors. Further research is needed to understand the full breadth of this group's cyber capabilities. DHS and FBI assess that HIDDEN COBRA actors will continue to use cyber operations to advance their government's military and strategic objectives.

In another series of incidents since at least May of last year, working with U.S. and international partners, DHS and FBI have identified advanced persistent threat actors targeting government entities and businesses in the energy, nuclear, water, aviation, and critical manufacturing sectors. DHS assesses that this campaign comprises two distinct categories of victims: staging and intended targets. In other words, through DHS'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 DHS 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. In recent weeks, DHS and the FBI remain active with incident response 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 (EO) 13800, on *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 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.

As part of the EO, NPPD has been working with our interagency partners to modernize the federal government's information technology (IT) infrastructure. This Committee has led this effort by working to enact the Modernizing Government Technology Act last December. We are exploring opportunities to consolidate network architectures and embrace shared IT services, while emphasizing cybersecurity is a foundational element of all new IT services. As federal agencies begin to leverage cloud computing and mobile technologies, we acknowledge that security solutions need to evolve. DHS is focused on the objectives that Trusted Internet Connections (TIC) mandate expected to achieve, such as gaining situational awareness across the federal civilian landscape, as opposed to driving a specific technical approach. We will continue our work with the Office of American Innovations, Office of Management and Budget and the federal civilian agencies to ensure agencies understand their roles and responsibilities to secure their data, maintain situational awareness and have appropriate security protections for their cloud environments. We must work quickly to replace legacy IT. No amount of investment in innovative cybersecurity capabilities will fully succeed in protecting our IT until we address the pervasive problem of legacy equipment and software across the federal enterprise. We must also modernize how the government manages IT risk in order to ensure effective, sustainable and secure investments. As such, we are taking steps to ensure that our investment planning and prioritization in future capabilities are driven by a threat informed approach. Leveraging the legislation passed by this committee, we are working with the agencies to modernize their systems.

The challenges posed by antiquated, end-of-life, legacy Federal IT systems has been apparent in the implementation of DHS's binding operational directives (BODs). Some legacy systems can no longer be patched, others are not supported by vendors, and some experience significant performance issues if not re-configured during the security upgrade/enhancement process. Many of these legacy systems simply were not designed for the current environment and the need for modern security approaches. As an example, during the implementation of BOD 15-01 (Mitigating Critical Vulnerabilities) and BOD 16-02 (Securing Network Infrastructure Devices), the DHS team identified and monitored dozens of end-of-life systems preventing the agency from quickly securing the system based on the BOD action. Fortunately, in most cases, DHS and the agency were able to address these issues and either upgrade, transition, or mitigate. While the use of more modernized IT equipment has many benefits for users and administrators, the benefits to cybersecurity are significant.

Across the Federal government, agencies have been implementing action plans to use the industry-standard Department of Commerce's National Institute of Standards and Technology 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, NPPD has been evaluating the totality of these Agency reports in order to comprehensively assess the adequacy of the Federal government's overall cybersecurity risk management posture. DHS works with agencies and OMB to ensure agencies have adequate resources to address their cybersecurity risk.

DHS is embracing our statutory responsibility to administer, in consultation with OMB, the implementation of federal agency cybersecurity policies and practices by leading the effort to secure the federal civilian executive branch enterprise following a risk-based approach. This

committee played a key role in championing the passage of FISMA 2014 and clarifying these important authorities for DHS. The overarching goal of federal cybersecurity is to ensure that every agency maintains an adequate level of cybersecurity, commensurate with its own risks and with those of the federal enterprise. E.O. 13800 makes clear that cybersecurity risk within the Executive Branch shall be managed as an enterprise. At the same time, agencies implement their cybersecurity programs and manage their own risk, as they are best positioned to understand how their unique mission environments need to be protected.

DHS supports these efforts by providing shared services and essential architecture and, along with the OMB, ensuring an adequate level of security enterprise-wide, including addressing systemic risks and interdependencies. We are working to assess risks at agencies, particularly systemic risks that could affect the Executive Branch as a whole; making recommendations to agencies and adjusting government-wide policies as necessary; making budgeting recommendation to OMB to ensure that cybersecurity risks are appropriately accounted for and funded; and furthering our analysis support to OMB to ensure that policies are adhered to and agencies are held accountable.

Our efforts, in collaboration with the Office of Management and Budget (OMB) and the General Services Administration, are guided by three principles: risk-based, cost-effective, and scalable. DHS addresses the greatest risks first and focuses on the highest impact systems, assets, and capabilities through cost-effective and scalable approaches. DHS leads through direct action and offerings, but also through collaboration and communication with agencies and partners, such as OMB, the General Services Administration, and the National Institute of Standards and Technology.

Cybersecurity Protections for Federal Networks

Although federal agencies have primary responsibility for their own cybersecurity, DHS, pursuant to its various authorities, provides a common set of security tools across the civilian executive branch and helps agencies manage their cyber risk. NPPD's assistance to federal agencies includes:

- providing tools to safeguard civilian executive branch networks through the National Cybersecurity Protection System (NCPS), which includes "EINSTEIN", and the Continuous Diagnostics and Mitigation (CDM) programs;
- measuring and motivating agencies to implement policies, directives, standards, and guidelines;
- serving as a hub for information sharing and incident reporting; and
- 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 private sector and the federal government.

EINSTEIN is a signature-based intrusion detection and prevention capability that takes action on known malicious activity, protecting unclassified networks at the perimeter of each federal government 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. We could not achieve such situational awareness through individual agency efforts alone.

NPPD is also leveraging investments in EINSTEIN to move beyond current reliance on signatures through pilot projects that are yielding positive results in the discovery of previously unidentified malicious activity. The pilot efforts are helping us to define the future operational needs for tactics, techniques, procedures, and skill sets required to operationalize the non-signature based approach to cybersecurity.

EINSTEIN 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 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 federal dashboard, the NCCIC will be able to operationalize this visibility, initially through improved vulnerability management. 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 BOD to agencies. In 2016, the Secretary issued a BOD on securing High Value Assets (HVA), 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 the United States' national security interests, foreign relations, economy, or to the public confidence, civil liberties, or

public health and safety of the American people. NPPD works with interagency partners to identify and prioritize HVAs for assessment and remediation activities across the federal government. For instance, NPPD conducts security architecture reviews on these HVAs to help agencies assess their system architecture and configurations. DHS has also coordinated with NIST to develop and issue an HVA Control Overlay. This guidance articulates specific guidance for implementing security controls that HVA system owners should implement, in addition to existing controls they have selected, to mitigate against known threats and weaknesses.

In addition to security architecture reviews, DHS conducts in-depth vulnerability assessments of the priority agency HVAs 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 NPPD cyber operators send emails to agency personnel and test whether recipients click on potentially malicious links. NPPD has focused these assessments on federal systems that may be of particular interest to adversaries or support uniquely significant data or services. In combination, security architecture reviews and vulnerability assessments provide system owners with recommendations to address identified vulnerabilities. DHS also works with the General Services Administration to ensure that contractors can provide assessments and other services to agencies that align with our HVA initiative. In the coming months DHS will be issuing an update to the BOD for securing HVAs that outlines required agency actions, senior agency leadership engagement, and an enhanced focus on the tracking and remediation of findings to further promote secure outcomes in alignment with the IT Modernization Report to the President.

Another BOD issued by the Secretary in 2015 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 BOD, 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. NPPD attributes this significant decrease in "stale" critical vulnerabilities to the clear cross-government expectation set up the BOD which enabled increased awareness across agency management teams which, in turn, prioritized agencies' efforts to quickly take action. By providing transparent reports to Agency executive leadership and engaging operational teams routinely on mitigation progress, NPPD continues to make progress in aligning its roles with regard to cybersecurity performance management and operational and technical assistance to help agencies find and fix vulnerabilities to secure their networks before an incident occurs. The progress made across Federal agencies to decrease the time it takes to mitigate critical vulnerabilities to Internet-facing systems has been encouraging. Because of the success of these efforts and the increased involvement of Agency executives to help drive positive organizational change and the prioritization of vulnerability management, NPPD is working to ensure the Federal government is meeting or exceeding industry standards and best practices related to vulnerability and patch management. Either through guidance, recommendations, or operational

direction, NPPD will continue working closely with the Federal community to rapidly address vulnerabilities by shortening mitigation timelines where practical in order to further reduce agencies' exposure to cyber risks.

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. As required by the Cybersecurity Act of 2015, NPPD expanded a capability operated by the NCCIC, known as automated indicator sharing (AIS), to automate our sharing of cyber threat indicators in real-time. The Cybersecurity Act establishes the NCCIC as a civilian hub for sharing cyber threat indicators and defensive measures with and among federal and non-federal entities, including the private sector. AIS protects the privacy and civil liberties of individuals by requiring removal of known personal information not directly related to a cybersecurity threat.

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. More than 230 agencies and private sector partners have connected to the AIS capability. AIS is still a maturing capability and we expect the volume of threat indicators shared through this system to substantially increase. As more indictors are shared from other federal agencies, state and local governments, and the private sector, this information sharing environment will become more robust and effective.

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 (I&A) 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 in collaboration with I&A. Analysts from the Departments of Defense, Energy, Treasury, Health and Human Services; the FBI, and other agencies are also collocated within the NCCIC and working together to understand the threats and share information with their sector stakeholders.

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 (C-SCRM) 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 High Value Assets.

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 federal networks and critical infrastructure from cyber threats. Our information technology is increasingly 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" (IoT) 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 we look forward to any questions you may have.