Written Testimony

Of

Christopher Krebs
Senior Official Performing the Duties of the Under Secretary
National Protection and Programs Directorate
U.S. Department of Homeland Security

Before the
United States Senate
Committee on Armed Services

Regarding
Roles and Responsibilities for Defending the Nation from Cyber Attack
October 19, 2017

Chairman McCain, Ranking Member Reed, and members of the Committee, thank you for the opportunity to be here today. In this month of October, we recognize National Cybersecurity Awareness Month, a time to focus on how cybersecurity is a shared responsibility that affects all Americans. 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) 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 on 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. The past year has marked a turning point in the cyber domain, at least in the public consciousness. We have long been confronted with a myriad of attacks against our digital networks. But over the past year, Americans saw 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 through attempts to manipulate elections.

Global cyber incidents, such as the "WannaCry" ransomware incident in May of this year and the "NotPetya" malware incident in June, 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.

Historically, cyber actors have strategically targeted critical infrastructure sectors including energy, financial services, critical manufacturing, water and wastewater, and others with various goals ranging from cyber espionage to developing the ability to disrupt critical

services. In recent years, DHS has identified and responded to malware such as Black Energy and Havex which were specifically created to target industrial control systems, associated with critical infrastructure such as power plants and critical manufacturing. More recently, the discovery of CrashOverride malware, reportedly used against Ukrainian power infrastructure in 2016, highlights the increasing cyber threat to our infrastructure.

In one recent campaign, advanced persistent threat actors targeted the cyber infrastructure of entities within the energy, nuclear, critical manufacturing, and other critical infrastructure sectors since at least May 2017. In response, DHS led the asset response, providing on-site and remote assistance to impacted entities, help them evaluate the risk, and remediate the malicious actor presence. In addition, DHS, the Federal Bureau of Investigation (FBI), and the Department of Energy (DOE) shared actionable analytic products with critical infrastructure owners and operators regarding this activity. This information provides network defenders with the information necessary to understand the adversary campaign and allows them to identify and reduce exposure to malicious activity. In addition, DHS has been working together with DOE to assess the preparedness of our electricity sector and strengthen our ability to respond to and recover from a prolonged power outage caused by a cyber incident.

Relationship with the Department of Defense and Intelligence Community

Responding to the full range of cyber threats facing government and critical infrastructure requires a whole-of-government, whole-of-nation effort. As it does with other stakeholders, DHS partners closely with the Department of Defense (DoD), FBI, and the intelligence community in carrying out its cybersecurity mission. DHS, FBI, DoD, and the intelligence community have multiple ongoing lines of effort. We continue to refine and mature planning to identify available resources and outline clear roles and responsibilities. We continue to focus on sharing cyber threat information relevant to defending against the most sophisticated malicious cyber actors. When appropriate, we can leverage existing authorities to provide technical assistance. In the event a significant cyber incident exhausts existing resources within DHS, DHS can leverage DoD resources, capabilities, and capacity to assist domestic response efforts under a well exercised mechanism—defense support of civil authorities. DHS and our partners also regularly participate in joint cyber exercises.

Cybersecurity Priorities

Earlier this year, the President signed Executive Order (EO) 13800, on *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. This EO set in motion a series of assessments and deliverables to understand how to improve our defenses and lower our risk to cyber threats. DHS has organized around these deliverables, working with federal and private sector partners to work through the range of actions included in the EO.

We are emphasizing the security of federal networks. 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, 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, pursuant to its various authorities, provides a common set of security tools across the civilian executive branch and helps federal 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 the 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 suite of 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 U.S. Government could not achieve such situational awareness through individual agency efforts alone.

Today, EINSTEIN is a signature-based intrusion detection and prevention capability that takes action on known malicious activity. Leveraging existing investments in the Internet Service Provider "ISP" infrastructure, 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. NPPD's 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 (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 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 network architecture and configurations.

As part of the effort to secure HVAs, DHS conducts in-depth vulnerability assessments of prioritized 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 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 (SLTT) 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, EO 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.

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 (ISAOs) 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. As more indictors are shared from other federal agencies, SLTT 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 and personnel from the DoD, Energy, Treasury, Health and Human Services, FBI, and others are also collocated within the NCCIC and working together to understand the threats and share information with their sector stakeholders.

Mitigating Cyber Risks

We also continue to adapt to the evolving risks to critical infrastructure, and prioritize our services to mitigate those risks. Facing the threat of cyber-enabled operations by a foreign government during the 2016 elections, DHS and our interagency partners conducted unprecedented outreach and provided cybersecurity assistance to state and local election officials. Information shared with election officials included indicators of compromise, technical data, and best practices that have assisted officials with addressing threats and vulnerabilities related to election infrastructure. Through numerous efforts before and after Election Day, DHS and our interagency partners have declassified and publicly shared significant information related to the Russian malicious cyber activity. These steps have been critical to protecting our elections, enhancing awareness among election officials, and educating the American public. The designation of election infrastructure as critical infrastructure serves to institutionalize prioritized services, support, and provide data protections and does not subject any additional regulatory oversight or burdens.

As the sector-specific agency, NPPD is providing overall coordination guidance on election infrastructure matters to subsector stakeholders. As part of this process, the Election Infrastructure Subsector Government Coordinating Council (GCC) is being established. The Election Infrastructure Subsector GCC will be a representative council of federal, state, and local partners with the mission of focusing on sector-specific strategies and planning. This will include development of information sharing protocols and establishment of key working groups, among other priorities.

The Department also recently took action against specific products which present a risk to federal information systems. After careful consideration of available information and consultation with interagency partners, last month the Acting Secretary issued a BOD directing 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 calls 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 in the

next 60 days, and at 90 days from the date of this 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 information systems. This action is based on the information security risks presented by the use of Kaspersky products on federal information systems.

The Department is providing an opportunity for Kaspersky to submit a written response addressing the Department's concerns or to mitigate those concerns. The Department wants to ensure that the company has a full opportunity to inform the Acting Secretary of any evidence, materials, or data that may be relevant. This opportunity is also available to any other entity that claims its commercial interests will be directly impacted by the directive.

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" (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 I look forward to any questions you may have.