Statement for the Record

The Honorable Christopher C. Krebs
Under Secretary
National Protection and Programs Directorate
U.S. Department of Homeland Security

FOR A HEARING ON

"Securing Election Systems and Other Critical Infrastructure"

BEFORE THE
UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY

Wednesday, July 11, 2018

Washington, DC

Chairman McCaul, Ranking Member Thompson, and members of the Committee, thank you for today's opportunity to testify regarding the U.S. Department of Homeland Security's (DHS) ongoing efforts to assist with reducing and mitigating risks to our election infrastructure. DHS is eager to share with you the progress we have made to establish trust-based partnerships with our Nation's election officials who administer our democratic election processes.

Safeguarding and securing cyberspace is a core homeland security mission. DHS 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.

Recognizing that the 2018 U.S. mid-term elections are a potential target for malicious cyber activity, DHS is committed to robust engagement with state and local election officials, as well as private sector entities, to assist them with defining their risk, and providing them with information and capabilities that enable them to better defend their infrastructure.

Given the foundational role that elections play in a free and democratic society, in January 2017 the Secretary of Homeland Security designated election infrastructure as a critical infrastructure subsector. Under our system of laws, federal elections are administered by state and local election officials in thousands of jurisdictions across the country. These officials manage election infrastructure and ensure its security and resilience on a day-to-day basis.

As such, DHS and our federal partners have formalized the prioritization of ***voluntary*** cybersecurity assistance for election infrastructure similar to that which is provided to a range of other critical infrastructure entities, such as financial institutions and electric utilities.

Since 2016, DHS's National Protection and Programs Directorate (NPPD) has convened Federal Government and election officials regularly to share cybersecurity risk information and to determine an effective means of assistance. The Election Infrastructure Subsector (EIS) Government Coordinating Council (GCC) has worked to establish goals and objectives, including plans for EIS engagement and the establishment of a sector-specific plan (SSP). GCC representatives include DHS, the Election Assistance Commission (EAC), and 24 state and local election officials. Participation in the council is entirely voluntary and does not change the fundamental role of state and local jurisdictions in overseeing elections.

The Department and the EAC worked with election industry representatives to launch an industry-led Sector Coordinating Council (SCC), a self-organized, self-run, and self-governed council with leadership designated by the sector membership. The SCC serves as industry's principal entity for coordinating with the government on critical infrastructure security activities and issues related to sector-specific strategies, and policies. This collaboration is conducted

under DHS's authority to provide a forum in which government and private sector entities can jointly engage in a broad spectrum of activities to coordinate critical infrastructure security and resilience efforts which is used in each of the critical infrastructure sectors established under Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*. The process is a well-tested mechanism across critical infrastructure sectors for sharing threat information among the Federal Government and critical infrastructure partners, advancing risk management efforts, and prioritizing services available to sector partners in a trusted environment.

NPPD also engages directly with election officials—coordinating requests for assistance, risk mitigation, information sharing, and incident coordination, resources, and services. In order to ensure a coordinated approach from the federal government, NPPD has convened stakeholders from across the Federal Government through an Election Task Force. The task force serves to provide actionable information and offer assistance to assist election officials with strengthening their election infrastructure by reducing and mitigating cyber risk, and increasing resilience of their processes.

Within the context of today's hearing, I will address the unclassified assessment of malicious cyber operations directed against U.S. election infrastructure and our efforts to help enhance the security of elections that are administered by jurisdictions around the country.

Enhancing Security for Future Elections

DHS regularly coordinates with the intelligence community and law enforcement partners on potential threats to the Homeland. Among non-federal partners, DHS has been engaging state and local officials, as well as relevant private sector entities, to assess the scale and scope of malicious cyber activity potentially targeting the U.S. election infrastructure. Election infrastructure includes the information and communications technology, capabilities, physical assets, and technologies that enable the registration and validation of voters; the casting, transmission, tabulation, and reporting of votes; and the certification, auditing, and verification of elections.

DHS 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. DHS 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.

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 ongoing engagements, DHS is working to provide value-added—yet voluntary—services to support their efforts to secure elections.

Improving Coordination with State, local Tribal, Territorial (SLTT) and Private Sector partners. Increasingly, the nation's election infrastructure leverages information technology (IT) for efficiency and convenience, but also exposes systems to cybersecurity risks,

just like in any other enterprise environment. Just like with other sectors, NPPD helps stakeholders in federal departments and agencies, SLTT governments, and the private sector to manage these cybersecurity risks. Consistent with our long-standing partnerships with state and local governments, we have been working with election officials to share information about cybersecurity risks, and to provide voluntary resources and technical assistance.

The National Cybersecurity and Communications Integration Center (NCCIC) works with the MS-ISAC to provide threat and vulnerability information to state and local officials. For nearly a decade, DHS has funded the Multi-State Information Sharing and Analysis Center (MS-ISAC), which has since created the EI-ISAC, to enable its members to share cybersecurity information and collaborate with each other. The EI-ISAC's membership includes almost 1,000 SLTT election-specific entities. Through the MS-ISAC, it has representatives co-located with the NCCIC to enable regular collaboration and access to information and services for state chief information officers.

Providing Technical Assistance and Sharing Information. NPPD actively promotes a range of services including:

Cyber hygiene service for Internet-facing systems: Through this automated, remote scan, NPPD may provide a report identifying vulnerabilities and mitigation recommendations to improve the cybersecurity of systems connected to the Internet, such as online voter registration systems, election night reporting systems, and other Internet-connected election management systems.

Risk and vulnerability assessments: We have prioritized state and local election systems upon request, and increased the availability of risk and vulnerability assessments (RVAs). These in-depth, on-site evaluations include a system-wide understanding of vulnerabilities, focused on both internal and external systems. We provide a full report of vulnerabilities and recommended mitigations following the testing.

Incident response assistance: We encourage election officials to report suspected malicious cyber activity to the NCCIC. Upon request, the NCCIC can provide assistance in identifying and remediating a cyber incident. Information reported to the NCCIC is also critical to the federal government's ability to broadly assess malicious attempts to infiltrate election systems. This technical information will also be shared with other state officials so they have the ability to defend their own systems from similar malicious activity.

Knowing what to do when a security incident happens—whether physical or cyber—before it happens, is critical. NPPD supports election officials with incident response planning including participating in exercises and reviewing incident response playbooks. Crisis communications are a core component of these efforts, ensuring officials are able to communicate transparently and authoritatively to their constituents when an incident unfolds. In some cases, we do this directly with state and local jurisdictions. In others, we partner with outside organizations. We recognize that securing our nation's systems is a shared responsibility, and we are leveraging partnerships to advance that mission.

Information sharing: NPPD maintains numerous platforms and services to share relevant information on cyber incidents. State election officials may also receive information directly from the NCCIC. The NCCIC also works with the EI-ISAC, which allows election officials to connect with the EI-ISAC or their State Chief Information Officer to rapidly receive information they can use to protect their systems. Best practices, cyber threat information, and technical indicators, some of which had been previously classified, have been shared with election officials in thousands of state and local jurisdictions. In all cases, the information sharing and/or use of such cybersecurity risk indicators, or information related to cybersecurity risks and incidents complies with applicable lawful restrictions on its collection and use and with DHS policies protective of privacy and civil liberties.

Classified information sharing: To most effectively share information with all of our partners—not just those with security clearances—we work with the intelligence community to rapidly declassify relevant intelligence or provide tearlines. While DHS prioritizes declassifying information to the extent possible, we also provide classified information to cleared stakeholders, as appropriate. DHS has been working with state chief election officials and additional election staff in each state to provide them with security clearances. By working with ODNI and the Federal Bureau of Investigation (FBI), in February 2018 election officials from each state received one-day read-ins for a classified threat briefing while they were in Washington, DC. This briefing demonstrated our commitment to ensuring election officials have the information they need to understand the threats they face.

Field-based cybersecurity advisors and protective security advisors: NPPD has more than 130 cybersecurity and protective security personnel available to provide actionable information and connect election officials to a range of tools and resources to improve the cybersecurity preparedness of election systems; and to secure the physical site security of voting machine storage and polling places. These advisors are also available to assist with planning and incident management for both cyber and physical incidents.

Physical and protective security tools, training, and resources: NPPD provides guidance and tools to improve the security of polling sites and other physical election infrastructure. This guidance can be found at www.dhs.gov/hometown-security. This guidance helps to train administrative and volunteer staff on identifying and reporting suspicious activities, active shooter scenarios, and what to do if they suspect an improvised explosive device.

Election Security Efforts Moving Forward

DHS has made tremendous strides and is committed to working collaboratively with those on the front lines of administering our elections 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 are significant technology needs across SLTT governments, and State and local election systems, in particular. It will take significant and continual investment to ensure that election systems across the nation are upgraded and secure, with

vulnerable systems retired. These efforts require a whole of government approach. The President and this Administration are committed to addressing these risks.

There is a 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. Our voting infrastructure is diverse, subject to local control, and has many checks and balances. As the threat environment evolves, we 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.

National Risk Management

In addition to addressing election security, we coordinate the overall federal effort to promote the security and resilience of the Nation's critical infrastructure, and is responsible for administering the implementation of federal government cybersecurity policies nad practices. 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. 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, we 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, we shared additional mitigation guidance to assist network defenders. As the incidents unfolded, we 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 been comprised of 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 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. The NCCIC is the civilian government's hub for cybersecurity information sharing, asset incident response, and coordination for both critical infrastructure and the Federal government.

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 May 2018, the Secretary issued a BOD to update a previous BOD related to securing High Value Assets—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, we conduct security architecture reviews on these High Value Assets to help agencies assess their network architecture and configurations. The updated BOD enhances NPPD's approach to conducting these engagements to provide agencies with improved results and finding by expanding system scope, refining assessment methodologies, an dusing less-constratined penetration testing approaches to resemble tactics, techniques, and proceadures used by advanced threat actors attempting to gain unauthorized access.

As part of the effort to secure High Value Assets, DHS conducts in-depth vulnerability assessments of prioritized agency these 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.

In addition to efforts to protect government networks, Executive Order 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.

As part of this effort, DHS is establishing a program office to strengthen support to such entities and improve coordination of interagency support. Through the program office, we will coordinate with federal and non-federal partners to enhance access to classified information, improve incident communication and coordination, and improve cross-sector information sharing, among other efforts.

Conclusion

In the face of increasingly sophisticated threats, DHS employees stand 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 appear before the Committee today, and I look forward to your questions.