Statement for the Record
of
U.S. Department of Homeland Security

FOR A HEARING ON

"Election Security"

BEFORE THE
UNITED STATES SENATE
SELECT COMMITTEE ON INTELLIGENCE

Wednesdy, March 21, 2018

Washington, DC

Chairman Burr, Vice Chairman Warner, 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. Almost a year ago, DHS appeared before this Committee to testify on the same topic. Today, DHS is pleased 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. 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. Safeguarding and securing cyberspace is a core homeland security mission.

Election security and integrity covers a number of issues. Of primary importance to this committee are two. The first is election security – the physical and cyber security related to voting and the tallying of the votes. The second is efforts to counter foreign influence of voters themselves. Within the federal government, DHS has the primary responsibility for the former and that is what this testimony will cover. While countering foreign influence is a critical issue in its own right, it involves the leadership of multiple other departments and agencies.

Under our Constitution and laws, the administration of elections is the responsibility of state and local officials. The Department's mission is to provide *assistance* to election officials in the form of advice, intelligence, technical support, and incident response planning with the ultimate goal of building a more resilient and secure election enterprise.

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, to develop plans for the EIS partnership, and to lay the groundwork for developing an EIS 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.

Additionally, DHS and EAC have worked with election industry representatives to launch an industry-led Sector Coordinating Council (SCC). In general the SCC is self-organized, self-run, and self-governed, 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. The collaboration of the GCC and SCC is through an established process 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. This structure is used in each of the critical infrastructure sectors established under Presidential Policy

Directive 21—Critical Infrastructure Security and Resilience. It provides 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.

In addition to the work of the EIS-GCC and SCC, NPPD continues to directly engage state and local 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 brought together stakeholders from across the Department and other federal agencies as part of an Election Task Force (ETF). The ETF increases the Department's efficiency and effectiveness in understanding, responding to, communicating, and sharing information related to cyber threats. The ETF 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, the Department's testimony will address the unclassified assessment of malicious cyber operations directed against U.S. election infrastructure. DHS's testimony will outline its efforts to help enhance the security of elections that are administered by state and local jurisdictions around the country, our progress to date, and our strategy moving forward.

Assessing the Threat

DHS regularly coordinates with the 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.

In addition to working directly with state and local officials, we have partnered with trusted third parties to analyze relevant cyber data, including the Multi-State Information Sharing and Analysis Center (MS-ISAC), the National Association of Secretaries of State and the National Association of State Election Directors. We also used our field personnel deployed around the country, to help further facilitate information sharing and enhance outreach. Such engagement paid off in terms of identifying suspicious and malicious cyber activity targeting election infrastructure in 2016. A body of knowledge grew throughout the summer and fall of 2016 about suspected Russian government cyber activities, indicators, and understanding that helped drive collection, investigations, and incident response activities. On October 7, 2016, DHS and the Office of the Director of National Intelligence (ODNI) released a joint statement on election security and urged state and local governments to be vigilant and seek cybersecurity assistance. Our message today remains the same.

Enhancing Security for Future Elections

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 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.

Improving Coordination with State and local partners. Increasingly, the nation's election infrastructure leverages information technology, or IT, for efficiency and convenience. While the benefits are many, reliance on IT introduces cybersecurity risks, just like in any other enterprise environment. Just like with other sectors, NPPD helps stakeholders in federal departments and agencies, state and local 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. Created by DHS over a decade ago, the MS-ISAC is partially funded by NPPD. The MS-ISAC's membership is limited to state and local government entities, and all fifty states and U.S. territories are members. 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. Through engagements with state and local election officials, including working through the Sector Coordinating Council, NPPD actively promotes a range of services to include but are not limited to the following:

Cyber hygiene service for Internet-facing systems: Through this automated, remote scan, NPPD provides state and local officials with 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). RVAs are more in-depth and executed on-site by NPPD cybersecurity experts. These

evaluations include a system-wide understanding of vulnerabilities, focused on both internal and external systems. When NPPD conducts these assessments, we provide a full report of vulnerabilities and recommended mitigations following the testing.

Incident response assistance: We encourage state and local election officials to report suspected malicious cyber activity to the NCCIC. Upon request, the NCCIC can provide on-site 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 is core component of these efforts, ensuring officials are able to communicate transparently and authoritatively 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 shares relevant information on cyber incidents. Information is shared directly with stakeholders and also through trusted third parties. For instance, the NCCIC works with the MS-ISAC, allowing election officials to connect with the MS-ISAC or their State Chief Information Officer to rapidly receive information they can use to protect their systems. State election officials may also receive information directly from the NCCIC. 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.

Classified information sharing: To most effectively share information with all of our partners—not just those with security clearances—DHS works with the intelligence community to rapidly declassify relevant intelligence or provide tearlines. While DHS prioritizes declassifying information to the extent possible, DHS also provides 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 the Office of the Director of National Intelligence and the Federal Bureau of Investigation, 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

This year our Nation is preparing for upcoming primary and special elections as well as the general election in November. Some states such as Arizona, Texas, and Illinois have already conducted primary elections. Just yesterday, NPPD teammembers observed and supported election security efforts Chicago, demonstrating our close partnership with State and local election officials. 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 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 past eight months, 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 signfiicant technology deficit across State and local governments, and State and local election systems, in particular. It will take signficant and continual investment to ensure that systems are upgraded and insecure or vulnerable systems are retired.

While the activities described above deal with DHS's efforts to secure election infrastructure, there is a whole of government approach under this administration to address election infrastructure security as well as countering foreign influence. Two weeks ago, the leaders of DHS, DOJ, FBI, DNI, NSA and others convened a meeting at the National Cybersecurity and Communication Integration Center to futher coordinate our efforts. Tthe White House is holding a follow up meeting on this topic later today. As a group, this Administration – this President – is committed to addressing these risks.

In closing, 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.

Thank you for the opportunity to appear before the Committee today. The Department looks forward to your questions.