TESTIMONY

OF

JEANETTE MANFRA
ACTING DEPUTY UNDER SECRETARY FOR CYBERSECURITY AND COMMUNICATIONS
NATIONAL PROTECTION AND PROGRAMS DIRECTORATE
U.S. DEPARTMENT OF HOMELAND SECURITY

DR. SAMUEL LILES
ACTING DIRECTOR, CYBER DIVISION
OFFICE OF INTELLIGENCE AND ANALYSIS
U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE
THE

SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES SENATE
WASHINGTON, D.C.

ADDRESSING THREATS TO ELECTION INFRASTRUCTURE

JUNE 21, 2017

Chairman Burr, Vice Chairman Warner, members of this Committee, thank you for the invitation to be here and to represent the men and women that serve in the Department of Homeland Security's (DHS) Office of Intelligence and Analysis (I&A) and the National Protection and Programs Directorate (NPPD).

Given the vital role that elections play in a free and democratic society, on January 6, 2017, the Secretary of Homeland Security determined that election infrastructure should be designated as a critical infrastructure subsector. With the establishment of an Election Infrastructure subsector within the existing Government Facilities sector, DHS and its Federal partners have been formalizing the prioritization of cybersecurity assistance and protections for owners and operators of election infrastructure similar to those provided to a range of other critical infrastructure entities, such as financial institutions and electric utilities. Participation in the subsector is voluntary, and the establishment of a subsector does not create federal regulatory authority. Elections continue to be governed by state and local officials, but with additional prioritized effort by the Federal Government to provide voluntary security assistance.

As the Secretary noted to Congress last month, "we know that our Nation's cyber systems are under constant attack." Our testimony today will provide DHS's unclassified assessment of cyber operations directed against the U.S. election infrastructure and political entities during the 2016 elections, but not the overall Russian influence campaign covered in the January 2017 declassified Intelligence Community (IC) Assessment. Our testimony will also outline DHS's efforts to help enhance the security of election infrastructure operated by state and local jurisdictions around the country.

Assessing the Threat

Throughout spring and early summer 2016, the U.S. IC warned that the Russian government was responsible for the compromises and leaks of emails from U.S. political figures and institutions. This activity was part of a decade-long campaign of cyber-enabled operations directed at the U.S. Government and its citizens. As awareness of these activities grew, DHS began in August 2016 to receive reports of cyber-enabled scanning and probing of election-related infrastructure in some states. Some of this activity appeared to originate from servers operated by a Russian company. In addition to these reports and other classified information obtained during the period, DHS also received an unclassified Federal Bureau of Investigation bulletin that described a July 2016 compromise of a State Board of Elections website. The bulletin identified specific tactics and indicators and asked recipients to check their systems for similar activity. It also provided mitigation recommendations for state and local governments. DHS and its partners shared this unclassified information—specifically information regarding targeting of voter registration systems—with state and local governments to further increase awareness of the threat.

Within the Federal Government, DHS, through I&A and NPPD's National Cybersecurity and Communications Integration Center (NCCIC), began coordinating robustly with the Election Assistance Commission, the IC, and law enforcement partners. Among non-Federal partners, NPPD and I&A engaged 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. In addition to working directly with state and local officials, we partnered with stakeholders like the Multi-State Information Sharing and Analysis Center (MS-ISAC) to analyze relevant cyber data, the National Association of Secretaries of State, and the National Association of State Election Directors. We also leveraged our field personnel deployed around the country, inclusive of Intelligence Officers deployed in state and major urban area fusion centers, Cybersecurity Advisors and Protective Security Advisors located across the country, and Department of Justice field personnel, to help further facilitate information sharing and enhance outreach. Throughout September, that engagement paid off in terms of identifying suspicious and malicious cyber activity targeting the U.S. election infrastructure. A body of knowledge grew throughout the summer and fall about suspected Russian government cyber activities, indicators, and understanding that helped drive collection, investigations, and incident response activities.

One comprehensive intelligence report published by I&A in early October cataloged suspicious activity we observed on state government networks across the country. This initial look, largely based on suspected malicious tactics and infrastructure, helped inform a body of reporting directly related to election infrastructure. While not a definitive source in identifying individual activity attributed to Russian government cyber actors, it established that Internet-connected election-related networks, including websites, in 21 states were potentially targeted by Russian government cyber actors. Although we've refined our understanding of individual targeted networks, supported by classified reporting, the scale and scope noted in that October 2016 report still generally characterizes our observations: a small number of networks were successfully compromised, there were a larger number of states where attempts to compromise networks were unsuccessful, and there were an even greater number of states where only preparatory activity like scanning was observed.

With respect to our processes, the IC has noted before that the nature of cyberspace makes attribution of cyber operations difficult, but not impossible. In partnership with members of the IC, DHS applied IC analytic tradecraft techniques to reach a series of judgments about whether these events were isolated incidents, who was the likely perpetrator, that perpetrator's possible motivations, and whether a foreign government had a role in ordering or leading the operation. Using the Department's distinctive view of domestic information and intelligence reporting, our final assessment is based on an evaluation of each incident by the capabilities and tactics employed, the infrastructure used by malicious cyber actors, characteristics of the victimized networks, and adversary capability and intent.

In September, our products at the classified and unclassified levels reported that we had no indication that adversaries or criminals were planning cyber operations against the U.S. election infrastructure that would change the outcome of the coming U.S. election. Further, we assessed that multiple checks and redundancies in U.S. election infrastructure—including diversity of systems, non-Internet connected voting machines, pre-election testing, and processes for media, campaign, and election officials to check, audit, and validate results—make it likely that cyber manipulation of U.S. election systems intended to change the outcome of a national election would be detected.

During that period, we assessed that cyber operations targeting election infrastructure could be intended or used to undermine public confidence in electoral processes and potentially the outcome. This analysis supported an October 7, 2016, statement from then Secretary of Homeland Security and Director of National Intelligence that highlighted Russian cyber activities. This triggered further outreach to share threat information and offer voluntary services to assess cybersecurity of election infrastructure and processes.

The declassified January 2017 IC Assessment, "Assessing Russian Activities and Intentions in Recent U.S. Elections," captured our assessment of the Russian activity, identifying that "Russian intelligence obtained and maintained access to elements of multiple U.S. state or local electoral boards." Additionally, "DHS assesse[d] that the types of systems Russian actors targeted or compromised were not involved in vote tallying."[1] As we continue to judge any and all newly available information, DHS has not altered any of those prior assessments.

Looking ahead to future election cycles, with a recognition that the work to enhance election infrastructure security and resiliency is already under way, we assess that multiple elements of election infrastructure remain potentially vulnerable to cyber intrusions, and that multiple cyber actors may have an interest in targeting such infrastructure. The risk to U.S. computer-enabled election systems varies from county to county, between types of devices used, and among processes used by polling stations.

We continue to assess that mounting widespread cyber operations against U.S. voting machines at a level sufficient to affect a national election would require a multiyear effort with significant human and information technology resources available only to a nation-state. The level of effort and scale required to change the outcome of a national election, however, would make it nearly impossible to avoid detection.

As with other developments in the overall cyber environment, the propagation of disruptive technologies has the ability to disrupt electoral processes. For example, targeted intrusions against individual voter registration databases remain possible. With illicit access, manipulation of voter data or disruptions to their availability may impact a voter's ability to vote on Election Day. Most but not all jurisdictions, however, still rely on paper voter rolls or electronic poll books that are not connected in real-time to voter registration databases, which limited the possible impacts in 2016.

Whether a cyber operation intended to disrupt or alter the vote is successful or not, DHS remains concerned that cyber operations targeting election infrastructure could be intended to undermine public confidence. For instance, although we assess the impact of an intrusion into a vote tabulation system would likely be contained to the manipulation of unofficial Election Night reporting results and not impact the certified outcome, such an operation could undermine public confidence in the results.

Three major elements of DHS's intelligence operations were key to enhancing our awareness and understanding of the threat: integration of intelligence with operational DHS

[1] (U) National Intelligence Council, ICA 2017-01, 5 January 2017, (U) Assessing Russian Activities and Intentions in Recent U.S. Elections.

components, collaboration with IC members, and partnership with state and local governments. I&A's co-location of intelligence personnel with the NCCIC was key to enhancing the quality of information shared with customers and partners. Robust collaboration with other members of the IC helped appropriately coalesce domestic and foreign intelligence issues – a collaboration that continues to pay dividends across analysis of threats to U.S. critical infrastructure. Finally, the ability to use deployed field staff to leverage already established relationships also aided in gathering key information that shaped I&A's understanding of the threat environment.

Enhancing Security for Future Elections

Based on our assessment of activity observed, DHS is engaged with stakeholders across the spectrum to increase awareness of potential vulnerabilities and enhance security of U.S. election infrastructure. DHS continues to work with a diverse set of stakeholders to plan, prepare, and mitigate risk to the election infrastructure. Our election process is governed and administered by state and local election officials in thousands of jurisdictions across the country. These officials manage election infrastructure and ensure its security on a day-to-day basis. 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, DHS is working to enhance efforts to secure their election systems.

Increasingly, the nation's election infrastructure leverages information technology for efficiency and convenience. Like other systems, reliance on digital technologies introduces new cybersecurity risks. DHS's NCCIC helps stakeholders in federal departments and agencies, state and local governments, and the private sector to manage their 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.

Addressing cybersecurity challenges and helping our customers assess their cybersecurity risk is not new for DHS. We have three sets of cybersecurity customers: federal civilian agencies; state local, tribal, and territorial governments; and the private sector. Assistance includes three lines of business to support these customers: information sharing, best practices, and technical assistance. Support to state and local customers, such as election officials, is part of our daily operations.

NPPD shares actionable information about electoral infrastructure incidents through direct outreach to state and local governments and through the Multi-State Information Sharing and Analysis Center (MS-ISAC), enhancing situational awareness and providing election officials with the information needed to protect themselves from similar incidents. The MS-ISAC was created by DHS over a decade ago and is partially grant-funded by NPPD. The MS-ISAC composition is restricted to state and local government entities. It has representatives co-located with the NCCIC to enable regular collaboration and access to information and services for state chief information officers. All states are members of the MS-ISAC.

During the 2016 election cycle, and in future elections, NPPD offered and will continue to offer voluntary assistance from the NCCIC to state and local election officials and authorities interested in securing their infrastructure. The NCCIC provides this same assistance on an ongoing basis to public and private sector partners upon request.

Establishment of coordinating councils for election infrastructure owners and operators. DHS is working collaboratively with election officials and vendors of election infrastructure to establish coordinating councils that will be used to develop a physical and cyber security and resilience strategy for the Election Infrastructure subsector and define how the Federal government will work with election officials and vendors going forward. The coordinating councils will also be used to regularly share information on relevant threats and vulnerabilities quickly and efficiently so that owners and operators can manage their risk. Historically, DHS has not had active engagement directly with the state and local election community, so we're working on broadening and deepening those relationships, identifying requirements, and educating on our capabilities.

Through engagements with state and local election officials, including working through the Sector Coordinating Council, DHS actively promotes a range of services to include:

Cyber hygiene service for Internet-facing systems: This voluntary service is conducted remotely, after which DHS can provide 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: These assessments are more thorough and done on-site by DHS cybersecurity experts. They typically require two to three weeks and include a wide range of vulnerability testing services, focused on both internal and external systems. When DHS conducts these assessments, we provide a full report of vulnerabilities and recommended mitigations following the testing. These assessments are available on a limited, first-come, first-served basis.

Incident Response Assistance: We encourage state and local election officials to report suspected malicious cyber activity to the NCCIC. On 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 states to assist their ability to defend their own systems from similar malicious activity.

Information sharing: DHS will continue to share relevant information on cyber incidents through multiple means. The NCCIC works with the MS-ISAC. Election officials can connect with their state Chief Information Officer or the MS-ISAC directly as one way to benefit from this partnership and rapidly receive information they can use to protect their systems. State election officials may also receive incident information directly from the NCCIC.

Classified information sharing: DHS provides classified briefings to cleared stakeholders upon request, and as appropriate and necessary.

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

Physical and protective security tools, training, and resources: DHS provides advice 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. Officials can also contact a local DHS Protective Security Advisor for access to DHS resources.

In closing, we want to reiterate that the fundamental right of all citizens to be heard by having their vote accurately counted is at the core of our American values. Ensuring the integrity of our electoral process is a vital national interest and one of our highest priorities as citizens in a democratic society. We have confidence in the overall integrity of our electoral system. Our voting infrastructure is diverse, subject to local control, and has many checks and balances built in. As the threat environment evolves, the Department will continue to work with state and local partners to enhance our understanding of the threat and 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 testify, and we look forward to your questions.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu