Testimony

Matthew Masterson
Senior Cybersecurity Advisor
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

FOR A FIELD HEARING ON

U.S. Election Security

BEFORE THE
UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY

Tuesday, October 15, 2019

Washington, DC

Chairman Thompson, Congresswoman Underwood, and Members of the Committee, thank you for the opportunity to testify regarding the U.S. Department of Homeland Security's (DHS) progress in reducing and mitigating risks to our Nation's election infrastructure. DHS has worked to establish trust-based partnerships with state and local officials who administer our elections, as well as political parties and campaigns, and I look forward to sharing with you an update on our work during the 2018 midterm elections and our priorities through the 2020 election cycle.

Leading up to the 2018 midterms, DHS worked hand in hand with federal partners, state and local election officials, and private sector vendors to provide them with information and capabilities to enable them to better defend their infrastructure. On the Federal level, DHS has coordinated closely with the Federal Bureau of Investigation (FBI), the Office of the Director of National Intelligence (ODNI), and Department of Defense (DOD) on these efforts. This partnership led to a successful model that we aim to continue and improve upon in the 2020 election cycle.

Since 2016, DHS's Cybersecurity and Infrastructure Security Agency (CISA) has led a voluntary partnership of Federal Government and election officials who regularly share cybersecurity risk information. CISA has engaged directly with election officials—coordinating requests for assistance, risk mitigation, information sharing, and incident response. To ensure a coordinated approach to assisting election officials protect the election infrastructure they manage, CISA has convened stakeholders from across the Federal Government through CISA's Election Security Initiative.

CISA and the Election Assistance Commission (EAC) have convened federal government and election officials regularly to share cybersecurity risk information and to determine an effective means of assistance. Since 2017, 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 create an EIS Sector-Specific Plan. Participation in the council is voluntary and does not change the fundamental role of state and local jurisdictions in overseeing elections.

CISA and the EAC have also worked with election equipment and service vendors to launch, in 2017, an industry-led Sector Coordinating Council (SCC), a self-organized, self-run, and self-governed council with industry leadership designated by SCC members. The SCC serves as the industry's principal entity for coordinating with the Federal Government on critical infrastructure security activities related to sector-specific strategies. This collaboration is conducted under CISA's authority to provide a forum in which federal 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 SCC has helped CISA further its understanding of the systems, processes, and relationships particular to operation of the EIS.

Within the context of today's hearing, I will address our efforts in 2018 to help enhance the security of elections that are administered by jurisdictions around the country, along with our

election related priorities through 2020. While there was activity targeting our election infrastructure leading up to the midterms, this activity was consistent with typical malicious activity targeting networked IT systems. DHS along with the Department of Justice (DOJ), "concluded that there is no evidence to date that any identified activities of a foreign government or foreign agent had a material impact on the integrity or security of election infrastructure or political/campaign infrastructure used in the 2018 midterm elections used for the United States Congress."[1]

Assessing the Threat

The Department, with and through DHS' Office of Intelligence and Analysis, regularly coordinates with the Intelligence Community and law enforcement partners on potential threats to the Homeland. Among non-federal partners, DHS has engaged with state and local officials, as well as relevant private sector entities, to assess the scale and scope of malicious cyber activity potentially targeting election infrastructure in the United States. 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. Since 2016, state and local election offices and their private sector partners have robustly shared information with DHS regarding activity targeting their systems. As with all networked IT systems, officials are seeing scanning and probing of their networks on a daily basis. Election infrastructure is a target for nation-state and non-state actors seeking access to systems containing sensitive data or what they perceive to be valuable information. DHS and our Intelligence Community (IC) partners continue to assess that the 2020 election remains a likely cyber and influence target for our adversaries. In short, the threat to our elections remains and it is incumbent on all levels of government to work together to respond.

Enhancing Security

During the 2018 midterms, CISA provided a coordinated response from DHS and its federal partners to plan for, prepare for, and mitigate risk to election infrastructure. Working with election infrastructure stakeholders was essential to ensuring a more secure election. CISA and our stakeholders increased awareness of potential vulnerabilities and provided capabilities to enhance the security of U.S. election infrastructure, and shared best practices with other nations facing similar threats.

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, CISA will continue to provide free, voluntary, prioritized services to support their efforts to secure elections in the 2020 election cycle.

[1] "Acting Attorney General and Secretary of Homeland Security Submit Joint Report on Impact of Foreign Interference on Election and Political/Campaign Infrastructure in 2018 Elections." February 5, 2019. Retrieved from: https://www.dhs.gov/cisa/news/2019/02/05/acting-attorney-general-and-secretary-homeland-security-submit-joint-report

Improving Coordination with State, Local, Tribal, Territorial and Private Sector Partners

Increasingly, the nation's election infrastructure leverages information technology for efficiency and convenience, but also exposes systems to cybersecurity risks, just like in any other enterprise environment. Similar to other sectors, CISA helps systems owners and operators in federal departments and agencies, state, local, tribal, and territorial (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 to manage those risks.

Working with the EI-ISAC

CISA works with the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) to provide threat and vulnerability information to state and local officials. Through funding by CISA, the Center for Internet Security created and continues to operate the EI-ISAC. The EI-ISAC has representatives co-located with CISA's operations center to enable regular collaboration and access to information and services for election officials.

Providing Technical Assistance and Sharing Information

Knowing what to do when a security incident happens—whether physical or cyber—before it happens is critical. CISA supports election officials with incident response planning including participating in exercises and reviewing incident response playbooks. Crisis communications is a core component of these efforts, ensuring officials are able to communicate transparently and authoritatively 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. CISA actively promotes a range of services including:

Cyber hygiene service for Internet-facing systems: Through this automated, remote scan, CISA provides a weekly 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 (both onsite and remote): We have prioritized state and local election systems upon request, and increased the availability of risk and vulnerability assessments. These in-depth, on-site or remote 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 CISA. Upon request, the CISA can provide assistance in identifying and remediating a cyber incident. Information reported to CISA 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.

Information sharing: CISA maintains numerous platforms and services to share relevant information on cyber incidents. Election officials may also receive information directly from CISA. CISA also works with the EI-ISAC, allowing 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. CISA incorporates privacy and civil liberties considerations and protections into the design of all its activities. Information sharing and use of cybersecurity threat indicators, or information related to cybersecurity risks and incidents complies with applicable lawful restrictions on its collection and use and with Federal and 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—DHS and its Office of Intelligence and Analysis (I&A) work with the Intelligence Community to rapidly declassify relevant intelligence or provide as much intelligence as possible at the lowest classification level possible. While DHS prioritizes declassifying information to the greatest 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. These clearances have helped enable I&A and the Intelligence Community to deliver a number of classified in-person and secure video teleconferences for a broad audience of state and local elections officials, in the lead-up to the 2018 Midterms and into 2019.

Field-based cybersecurity advisors and protective security advisors: CISA has 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: CISA 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 Leading up to the 2018 Midterms

In the weeks leading up to the 2018 midterm elections, CISA officials supported a high degree of preparedness nationwide. CISA provided free technical cybersecurity assistance, continuous information sharing, and expertise to election offices and campaigns. All 50 states,

over 1,500 local and territorial election offices, 6 election associations, and 12 election venders were engaged in information sharing and receipt of assistance from EI-ISAC.

In August 2018, CISA hosted a "*Tabletop the Vote*" exercise, a three-day, first-of-its-kind exercise to assist our federal partners, state and local election officials, and private sector vendors in identifying best practices and areas for improvement in cyber incident planning, preparedness, identification, response, and recovery. Through tabletop simulation of a realistic incident scenario, exercise participants discussed and explored potential impacts to voter confidence, voting operations, and the integrity of elections. Partners for this exercise included 44 states and the District of Columbia; EAC; Department of Defense, including the Office of the Secretary of Defense, U.S. Cyber Command, and the National Security Agency; DHS I&A; DOJ, including the Federal Bureau of Investigation; Office of the Director of National Intelligence; and National Institute of Standards and Technology (NIST).

Through the "*Last Mile Initiative*," CISA worked closely with state and local governments to outline critical cybersecurity actions that should be implemented at the county level. For political campaigns, CISA disseminated a cybersecurity best practices checklist to help candidates and their teams better secure their devices and systems.

On Election Day, DHS deployed field staff across the country to maintain situational awareness and connect election officials to appropriate incident response professionals, if needed. In many cases, these field staff were co-located with election officials in their own security operations centers. CISA also hosted the National Cybersecurity Situational Awareness Room, an online portal for state and local election officials and vendors that facilitates rapid sharing of information. It gives election officials virtual access to the 24/7 operational watch floor CISA. This setup allowed DHS to monitor potential threats across multiple states at once and respond in a rapid fashion.

Priorities for the 2020 Election Cycle

For the 2020 elections, CISA has identified the following lines of effort to guide the Department's work:

- Protecting Election Infrastructure,
- Supporting Campaigns and Political Infrastructure,
- Raising Public Awareness and Building Resilience, and
- Efficiently Sharing Actionable Intelligence and Identifying Threats.

These priorities include broadening the reach and depth of information sharing and assistance that CISA is providing to state and local election officials, deepening our understanding of the elections risk environment, highlighting the need for regular and consistent resourcing of election infrastructure, extending the CISA suite of services for protecting networks to political campaigns and partisan organizations at the national level, and providing intelligence and threat reporting to the election community. For more information on these priorities, please visit: www.dhs.gov/cisa/protect2020

In addition, CISA is working towards improving the efficiency and effectiveness of election audits, incentivize the patching of election systems, and working with the National Institute of Standards and Technology (NIST) and the states to develop cybersecurity profiles utilizing the NIST Cybersecurity Framework for Improving Critical Infrastructure. The Department will continue to engage any political entity that wants our help. We are continuously working to mature our understanding of risks to this sector, improve our offerings, and to provide meaningful security guidance leveraging leading practices.

CISA has made tremendous strides on these efforts and goals and has been committed to working collaboratively with those on the front lines of administering our elections to secure election infrastructure from risks. In February, CISA officials provided updates to the Secretaries of State, state election directors, and members of the GCC and SCC on the full package of election security resources that are available from the Federal government, along with a roadmap on how to improve coordination across these entities. DHS also worked with our Intelligence Community partners to provide a classified one day read-in for these individuals regarding the current threats facing our election infrastructure.

In June, CISA hosted another "*Tabletop the Vote*" exercise with our federal partners, state and local election officials, and private sector vendors to review coordination protocols and incident response plans. The *Tabletop* covered a number of pre-, post- and day of election scenarios, including voter registration compromises, equipment issues, and misinformation distributed over news and social media. Participants included representatives from 47 states, thousands of local election officials, the District of Columbia, U.S. Virgin Islands, along with our Federal partners.

In July, DHS joined ODNI, DOJ, and DOD in briefing the full Congress on the federal government's coordinated approach to protecting the 2020 elections. DHS highlighted the increase in threat information that is now shared with state, local, territorial governments, the number of intrusion detection sensors, known as Albert sensors, deployed across the country, and the prioritization of intelligence sharing with state and local officials on cyber threats and foreign interference.

CISA, through the EI-ISAC, now provides threat alerts to all 50 states and more than 2000 local and territorial election offices. CISA also provides weekly vulnerability scans for 37 states, 145 local partners, one territory, and 10 private sector partners. In addition, all 50 states, 110 localities, and two territories now have intrusion detection sensors. These sensors are operated and monitored by EI-ISAC as part of the Multi-State Information Sharing and Analysis Center's (MS-ISAC) Albert intrusion detection system. DHS shares intelligence and other cyber threat information with EI-ISAC for use in Albert, which assists with identifying specific threats to election infrastructure networks. EI-ISAC has also deployed Albert sensors within election vendor environments, to protect their networks that host voter registration systems in five states.

CISA is also expanding our level of engagement with political organizations. We have worked in close coordination with both the Democratic National Committee (DNC) and the Republican National Committee (RNC) to share information and best practices. CISA has also engaged directly with Presidential and Congressional campaigns. These efforts have

included a joint threat briefing with the FBI and ODNI for all Presidential campaigns registered with the FEC as well as engaging directly with campaigns to offer services and share information.

We will remain transparent as well as agile in combating and securing our physical and cyber infrastructure. It will take continual investment from all levels of government to ensure that election systems across the nation are upgraded, patched and better secured, with older more vulnerable systems retired. These efforts require a whole of government approach.

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, and I look forward to your questions.