Testimony

Christopher Krebs
Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

FOR A HEARING ON

Securing U.S. Election Infrastructure and Protecting Political Discourse

BEFORE THE
UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON OVERSIGHT AND REFORM
SUBCOMMITEE ON NATIONAL SECURITY

Wednesday, May 22, 2019

Washington, DC

Chairman Lynch, Ranking Member Hice, 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, and I look forward to sharing with you an update on our work during the 2018 midterm 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. 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, CISA convened stakeholders from across the Federal Government through the Election Task Force.

The Department 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 2016, 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. Participation in the council is voluntary and does not change the fundamental role of state and local jurisdictions in overseeing elections.

DHS and the EAC have also worked with election vendors to launch an industry-led Sector Coordinating Council (SCC), a self-organized, self-run, and self-governed council with leadership designated by sector membership. 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 DHS'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 DHS 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 is similar to what we have seen previously and occurs on the Internet every day. This activity has not been attributed to nation-state actors and along with the Department of Justice (DOJ), we 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 or campaign infrastructure used in the 2018 midterm elections

Assessing the Threat

The Department 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 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 over the past two years, we have partnered with trusted third parties to analyze relevant cyber data, including the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), the National Association of Secretaries of State, and the National Association of State Election Directors. DHS field personnel deployed around the country furthered information sharing and enhanced outreach.

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 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, CISA will continue to work to provide value-added—yet voluntary—services to support their efforts to secure elections in the 2020 election cycle.

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. Just like with other sectors, CISA helps stakeholders 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.

CISA works with the 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 National Cybersecurity and Communications Integration Center (NCCIC) 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 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. 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 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.

Information sharing: CISA maintains numerous platforms and services to share relevant information on cyber incidents. Election officials may also receive information directly from the NCCIC. The NCCIC 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. In all cases, the information sharing and use of such cybersecurity threat 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—DHS works 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.

Field-based cybersecurity advisors and protective security advisors: CISA 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: 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, DHS officials supported a high degree of preparedness nationwide. DHS provided free technical cybersecurity assistance, continuous information sharing, and expertise to election offices and campaigns. EI-ISAC threat alerts were shared with all 50 states, over 1,400 local and territorial election offices, 6 election associations, and 12 election venders.

In August 2018, DHS 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; DOJ; Federal Bureau of Investigation; Office of the Director of National Intelligence; and National Institute of Standards and Technology (NIST).

Through the "*Last Mile Initiative*," DHS worked closely with state and local governments to outline critical cybersecurity actions that should be implemented at the county level. For political campaigns, DHS 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. DHS 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 of the CISA NCCIC. This setup allowed DHS to monitor potential threats across multiple states at once and respond in a rapid fashion.

Our goal has been for the American people to enter the voting booth with the confidence that their vote counts and is counted correctly. I am proud to say that our efforts over the past two years have resulted in the most secure election in modern history.

No Evidence of Material Impact Regarding Election Interference

The Secretary of Homeland Security and the Acting Attorney General have 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 or campaign infrastructure used in the 2018 midterm elections for the United States Congress. The activity we did see was consistent with what we shared in the weeks leading up to the election. Russia, and other foreign countries, including China and Iran, conducted influence activities and messaging campaigns that targeted the United States to promote their strategic interests.

Election Security Efforts Moving Forward

Ensuring the security of our electoral process remains a vital national interest and one of our highest priorities at DHS. In the run up to the 2020 election season, DHS will continue to prioritize elections by broadening the reach and depth of information sharing and assistance that we are providing to state and local election officials, and continuing to share information on threats and mitigation tactics.

DHS goals for the 2020 election cycle include improving the efficiency and effectiveness of election audits, continue to 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. We will also continue to engage any political entity that wants our help. DHS offers these entities the same tools and resources that we offer to state and local election officials, including trainings, cyber hygiene support, information sharing, and other resources.

DHS has made tremendous strides and has been committed to working collaboratively with those on the front lines of administering our elections to secure election infrastructure from risks. Just last week, DHS 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.

We will remain transparent as well as agile in combating and securing our physical and cyber infrastructure. However, we recognize that there is a significant technology deficit 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.

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.