Testimony

Kim Wyman

Senior Election Security Lead
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

ON

"Protecting Our Democracy's Frontline Workers"

BEFORE

UNITED STATES SENATE
COMMITTEE ON THE JUDICIARY

August 3, 2022

Washington, D.C.

Chairman Durbin, Ranking Member Grassley, and members of the Committee, thank you for the opportunity to testify on behalf of the Cybersecurity and Infrastructure Security Agency (CISA) regarding our efforts to support election officials and their private sector partners to manage risk and build resilience in our Nation's election infrastructure. I look forward to sharing with you the extensive progress that has been made in improving the security of the country's election infrastructure over the last three election cycles; describing CISA's numerous no-cost and voluntary services and resources for the election infrastructure community; and providing an update on how CISA is postured to support our stakeholders for the 2022 midterm election cycle.

Free and fair elections are a hallmark of American democracy. The American people's confidence that their vote will be counted as cast relies heavily on the security and resilience of the infrastructure that makes the Nation's elections possible. Accordingly, an electoral process that is both secure and resilient is a vital national interest and one of the Department of Homeland Security's (DHS) and CISA's highest priorities. Indeed, from federal agencies to the local election offices that handle the nuts and bolts by administering elections in all corners of the country, election security remains a central national security priority for all levels of government.

As demonstrated in the 2016, 2018, and 2020 election cycles, our democracy faces a continuing threat from foreign cyber and influence operations targeting U.S. election infrastructure and voters. This persistent threat reaffirms the need for continued federal support to state and local election officials. State and local election officials cannot be expected to combat sophisticated, nation state-sponsored threat actors alone. This served as the rationale for the designation of election infrastructure as a critical infrastructure subsector, and it remains true today.

With support from CISA and its federal partners, since 2016, the election infrastructure subsector has made incredible progress improving the security and resilience of our elections. I will highlight three areas that demonstrate this progress.

First, CISA and its federal partners are better positioned than ever before to get timely and actionable intelligence and information out to the election infrastructure subsector and into the hands of the owners and operators of election infrastructure. All 50 states and more than 3,200 local jurisdictions are members in the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC), which is CISA's main mechanism for sharing alerts with the community. CISA has sponsored over 150 security clearances for election officials and key private sector election infrastructure partners, with clearances available to election officials in all 50 states. And our relationships across the intelligence community and with federal law enforcement have never been stronger, including a shared commitment to sanitize, downgrade, or declassify intelligence that may be helpful to the election community to the greatest extent possible. This progress enabled the federal government to rapidly warn election officials and the broader public about Russian and Iranian threat activity in the immediate pre-election period in 2020. Having these structures in place helps us to facilitate intelligence and law enforcement briefings to the elections community on the evolving threat landscape. These threat briefings include cybersecurity, malign foreign influence, insider threats, domestic violent extremism and increasing physical security threats to the election infrastructure subsector, including election officials.

Second, we have strengthened our situational awareness of cyber activity and the cybersecurity risk landscape for election infrastructure by building strong relationships across the election infrastructure subsector. All 50 states and hundreds of local election officials have now deployed CISA-funded or state-funded intrusion detection sensors known as Albert sensors through the Multi-State Information Sharing and Analysis Center (MS-ISAC), giving MS-ISAC incredible visibility on election infrastructure entities' network traffic, so that when new threat activity is uncovered, we can rapidly understand the scale of the threat and work with our partners to mitigate and remediate the potential impact. Similarly, hundreds of election officials and private sector election infrastructure partners have signed up for CISA cybersecurity services, ranging from recurring scanning for known vulnerabilities on internet-connected infrastructure to in-depth penetration testing designed to provide CISA and our partners valuable insight into common cybersecurity risks across the subsector and informing our mitigation guidance and broader activities. And, perhaps most importantly, the election infrastructure subsector continues to do the essential work of voluntarily sharing information about potential cybersecurity incidents and anomalous activity on their networks to CISA, the EI-ISAC, and the FBI. The situational awareness and risk understanding provided from this information are key elements of the strengthened resilience across this subsector – simply put, while there is more work to be done, we are better positioned to detect and respond to a cybersecurity incident in the election infrastructure subsector than ever before.

Finally, election officials are committed to doing the hard and essential work of securing and building resilience in the Nation's election infrastructure. To illustrate this point:

Election officials continue to make meaningful progress in replacing paperless voting equipment. In 2020, an estimated 93 percent of ballots were cast on paper. The use of paper ballots or voting systems that produce paper records is a defense-in-depth measure that enables election officials to "roll back the tape" and confirm that voting equipment is functioning as intended.

Election officials continue to improve their incident response plans. They test those plans and build incident response muscle memory through exercises. CISA has provided more than 5,800 customized "Last Mile" products to state and local officials across 21 states that support incident response, and we expect strong attendance at CISA's annual National Tabletop the Vote Exercise this summer. Our most recent national tabletop in 2021 garnered participation from 45 states.

Despite this progress, we should not be complacent about the real security challenges facing U.S. election infrastructure. Sophisticated, state-sponsored threat actors continue to target U.S. elections, including through influence campaigns that seek to sow discord and undermine confidence in U.S. democratic institutions. Ransomware gangs continue to target state and local governments, which could impact networks that manage some election functions.

To contend with these challenges, CISA and DHS have been working hand-in-hand with federal partners to provide election officials and their private sector partners with information and capabilities that enable them to better manage risk to their infrastructure.

I will address CISA's broader role in election security and describe the work we undertake to safeguard our elections, including how we partner with state and local governments and provide them no-cost and voluntary resources and services, and our posture and priorities for the 2022 midterms elections.

CISA's Role in Election Security

In January 2017, in response to attempted Russian interference in the 2016 elections, DHS designated election infrastructure as a critical infrastructure subsector. The designation recognizes that the United States' election infrastructure is of such vital importance to the American way of life that its incapacitation or destruction would have a devastating effect on the country. Further, the designation allows DHS to prioritize federal assistance to election officials and their private sector partners in a similar manner as other critical infrastructure sectors, such as our ports and dams, the electric grid, and nuclear facilities.

CISA's election-focused mission is to ensure that state and local election officials, and their private sector partners, have the necessary information and tools to successfully manage risk and build resilience into the nation's election infrastructure. Our support to the election community is bolstered by the work of our federal partners in the intelligence community, federal law enforcement, and other agencies like the U.S. Postal Service and the Election Assistance Commission (EAC). Collectively, we have brought incredible resources to bear to support state and local election officials as we take a whole-of-government approach to election security.

CISA leads a voluntary partnership between the federal government and state and local election officials, with all partners regularly sharing cybersecurity risk information. CISA engages 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 convenes stakeholders from across the Federal Government through CISA's Election Security Initiative (ESI).

As the Sector Risk Management Agency (SRMA) for the election infrastructure subsector, CISA convenes federal government and state and local election officials regularly to share cybersecurity risk information and to determine how the federal government can best assist election officials in mitigating risks to their infrastructure. The Election Infrastructure Subsector (EIS) Government Coordinating Council (GCC), established in 2017, works to establish goals and objectives and develop plans for the EIS partnership. Participation in the council is voluntary and does not change the role of state and local jurisdictions in overseeing elections.

CISA also works with election equipment and service vendors to facilitate 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. It has been invaluable in helping CISA understand the systems, processes, and relationships unique to the operation of the election infrastructure.

CISA Support & Services for the Election Community

CISA helps systems owners and operators in federal departments and agencies; state, local, tribal, and territorial (SLTT) governments; and private sector to manage potential risks across critical infrastructure sectors, including the election infrastructure subsector. Consistent with CISA's long-standing partnerships with state and local governments, CISA works with election officials to share information about risk and to provide voluntary, no-cost resources and technical assistance to manage those risks.

Information Sharing:

CISA leads efforts to promote effective communication among state and local officials, industry experts, and the federal government. Alongside intelligence community and federal law enforcement partners, CISA shares timely and actionable intelligence and information with the subsector to foster situational awareness about the evolving threat landscape and inform risk management decision-making by election infrastructure owners and operators.

CISA administers a security clearance program for the election infrastructure subsector so that classified information can be shared when warranted. When appropriate, CISA convenes classified briefings for these individuals to ensure that they receive relevant and timely threat information that may impact their work. Through the Joint Cyber Defense Collaborative (JCDC), CISA also works to share cyber threat information provided by JCDC industry and interagency partners, host unclassified community threat briefings, and raise awareness of no-cost services available to election infrastructure stakeholders.

CISA funds the EI-ISAC, which enables rapid communication, information sharing (including cyber alerts from CISA), and situational awareness across the Election Infrastructure community. CISA and the EI-ISAC provide a variety of situational awareness capabilities, including hosting a virtual platform prior to, during, and after state and national elections for election stakeholders to swiftly identify, react to, and share real-time information on potential cybersecurity incidents. Membership in the EI-ISAC is voluntary, no-cost, and open to all SLTT organizations that support election officials in the United States.

Cyber and Physical Security Support Services:

CISA works with SLTT and private sector officials to improve their security posture. CISA's cyber and physical services range from vulnerability scanning of internet connected systems to highly technical open-ended vulnerability research and penetration testing of technology used in the election sector to physical security services to improve their security posture and respond to incidents. These services are described in more detail below.

Field-Based Cybersecurity Advisors and Protective Security Advisors:

CISA has Cybersecurity Advisors (CSAs) and Protective Security Advisors (PSAs) throughout the country to provide expert guidance to help ensure the physical security, cybersecurity and resilience of the nation's critical infrastructure, including election infrastructure. CISA's CSAs

are trained personnel that help private sector entities and SLTT officials prepare for and protect themselves against cybersecurity threats. CSAs introduce stakeholders to CISA products and services, offer education and awareness briefings, perform cyber assessments, and serve as liaisons to other public and private cyber programs. CISA's PSAs are trained in the physical aspects of infrastructure protection. PSAs meet with election infrastructure stakeholders to share information, conduct physical security assessments of election facilities, conduct resilience surveys, assist with obtaining security clearances, and offer resources, training, and access to other DHS products and services.

Cyber Hygiene Services:

CISA offers several scanning and testing services to help organizations reduce their exposure to threats by taking a proactive approach to mitigating attack vectors. This includes vulnerability scanning through which CISA provides a weekly cyber hygiene 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. Other services include Web Application Scanning, Phishing Campaign Assessments, and Remote Penetration Testing.

.gov Top Level Domain (TLD):

CISA also manages the .gov TLD, which is exclusive to U.S. government organizations. CISA supports all official U.S. government organizations, including state and local governments – and has made .gov signups for election officials a priority. A .gov domain name lends legitimacy to all associated websites and online tools and helps ensure customers are accessing content from trusted sources. Increasing the public's expectation that government information is at .gov will make it harder for malicious actors to succeed when they attempt to impersonate governments.

Risk and Vulnerability Assessments:

CISA has 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.

Additionally, CISA also provides a range of cybersecurity assessments that evaluate operational resilience, cybersecurity practices, organizational management of external dependencies, and other key elements of a robust cybersecurity framework. CISA funds Malicious Domain Blocking and Reporting (MDBR) services via the EI-ISAC. MDBR technology prevents IT systems from connecting to harmful web domains, helping limit infections related to known malware, ransomware, phishing, and other cyber threats. This capability can block many ransomware infections by preventing the initial outreach to a ransomware delivery domain. The MDBR capability is a central component of our no-cost cybersecurity services to prevent successful cyber incidents against our election infrastructure and it is a service we are actively recommending entities take advantage of if they are not already.

Incident Response Planning Assistance:

CISA assists election officials and their private sector partners to develop, improve, and test their incident response plans. Knowing what steps to take to address a security incident - 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 can communicate transparently and authoritatively when an incident unfolds. CISA can also provide direct incident response assistance and coordination in certain circumstances.

We encourage election officials to share information about suspected malicious cyber activity to CISA and the EI-ISAC. Upon request, CISA can aid in identifying and remediating a cyber incident by deploying incident response teams to provide technical expertise and build capacity to find the root cause of an incident. CISA's incident response team responds to incidents such as malware infections, data theft, data corruption, ransomware encryption, denial of service, control systems intrusions, and other threats against critical assets. CISA's incident response engagements are just one example of the types of incident response and recovery services we offer.

Election Security Trainings and Exercises Offerings:

CISA offers no-cost, cybersecurity and physical security trainings and exercise services to enhance security and resilience of election infrastructure. The trainings seek to raise awareness in the election community about the evolving threat landscape, promote election security best practices, including on cybersecurity topics like phishing and ransomware, and help election officials build resilience against foreign malign influence, as well as better communicate their election security safeguards.

CISA hosts an annual national level exercise called Tabletop the Vote in coordination with the National Association of Secretaries of State (NASS) and the National Association of State Election Directors (NASED). The three-day virtual tabletop exercise assists CISA and our federal partners, state and local election officials, and vendors in identifying best practices and areas for improvement in cyber and physical incident planning, preparedness, identification, response, and recovery. The exercise covers traditional security concerns, but also evolving challenges since the 2020 election including threats, harassment, and incitement of violence against election officials. FBI and the United States Postal Inspection Service provide a law enforcement perspective on the federal level, but CISA encourages state and local partners to involve their state and local law enforcement and emergency responders to participate as well. This year's exercise is scheduled for August 17th-19th.

Election Security Efforts during the 2022 Midterms

For the 2022 midterm election cycle, CISA has identified five main priorities:

- First, alongside our intelligence community and federal law enforcement partners, CISA remains committed to sharing actionable information with election officials and their private sector partners in a timely manner and maintaining open channels of information sharing about threats and risks to election infrastructure. Importantly, CISA also works to share information up-stream that it receives from local election officials and its private sector partners to support efforts to implement a whole of government response to election security incidents.
- Second, we are providing guidance, services, and expertise to help election officials secure voter registration systems and information. The recent indictments of Iranian cyber threat actors for interference activity in 2020 as well as lessons from 2016 remind us that voter registration systems and information remain a target for malicious threat actors.
- Third, we are redoubling our efforts to promote cyber hygiene practices across the election infrastructure subsector. While incredible progress has been made in this area since 2016, more can be done, and we must remain vigilant in the face of ongoing cyber threats. Basic cyber hygiene practices such as implementing multi-factor authentication and patching software can go a long way toward protecting election officials from ransomware and other cyber threats. We are particularly focused on the "last mile," which are smaller and mid-sized jurisdictions around the country that oftentimes have difficulty making the necessary cybersecurity investments, but which are so crucial to the election ecosystem. CISA's Last Mile Initiative is a colloborative effort with state and local election officials to create customized tools to support their efforts to communicate security activities and practices. For example, Last Mile products might include customized posters that highlight measures state and local election authorities are taking to strengthen the security of their election systems or election day emergency response guides that provide local election personnel with simple, easily accessible tools for understanding communications steps to take when various incidents occur and how to report the incident to the appropriate authorities. These products enhance awareness of additional services and resources available to local election officials through CISA or from their state. In addition to their operational benefits, election officials often find Last Mile products useful for communicating to voters, lawmakers, and their own personnel to bolster confidence in the security of their election systems.
- Fourth, CISA is expanding efforts aimed at building societal resilience against foreign-influence campaigns that threaten election infrastructure security and seek to undermine public confidence in our elections. DHS conducts these activities consistent with relevant legal authorities and privacy, civil rights, and civil liberties protections.
- Finally, in partnership with the Department of Justice and broader national security and law enforcement community, we are expanding services that help keep election officials and voters safe, and strengthening the physical security of the nation's election infrastructure.

Immediately before, and through federal Election Days in November --and other select Election Days, -- CISA stands up an Operations Center, convening interagency partners, including the intelligence community, FBI, and Department of Defense, private sector partners, campaigns, political parties, and social media companies both in-person and virtually. The Operations Center allows stakeholders to share information in near-real time and ensures appropriate individuals have visibility on activities. The CISA-funded EI-ISAC also opens a cyber situational awareness room, where thousands of state and local election officials are able to share information in real-time in a virtual chat room. As reports come in from the field, CISA is able to rapidly share information with key stakeholders and obtain ground truth to incidents. In addition, CISA stands up a companion situational awareness room to coordinate real-time sharing across the federal interagency, to include federal law enforcement and intelligence agencies.

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

The right to vote is central to the functioning of our democracy. The public's confidence in their vote, and the faith they place in our democratic system of governance, rests upon the country's ability to conduct free and fair elections. At CISA, ensuring the security of our election infrastructure is of the highest priority and we will remain transparent and agile in our vigorous efforts to address new and evolving threats.

END