Testimony

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

FOR A HEARING ON

"Securing Federal Networks and State Election Systems"

BEFORE THE
UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON APPROPRIATIONS
SUBCOMMITTEE ON HOMELAND SECURITY

Wednesday, March 13, 2019

Washington, DC

Chairwoman Roybal-Allard, Ranking Member Fleischmann, and members of the Subcommittee, thank you for the opportunity to testify regarding the U.S. Department of Homeland Security's (DHS) ongoing efforts to strengthen the cybersecurity of federal networks and increase the security and resilience of our Nation's critical infrastructure. Safeguarding and securing cyberspace is a core homeland security mission.

At DHS's Cybersecurity and Infrastructure Security Agency (CISA), our mission is to defend against the threats of today, while working with partners across all levels of government and in the private sector to secure against the evolving risks of tomorrow – "Defend Today, Secure Tomorrow."

CISA leads the Nation's efforts to ensure the security and resilience of our cyber and physical infrastructure. We assist agencies with the protection of civilian federal networks and coordinate with other federal agencies, state, local, tribal, and territorial (SLTT) governments, and the private sector to defend our Nation's critical infrastructure from malicious cyber activity. By bringing together all levels of government, the private sector, international partners, and the public, DHS protects against cybersecurity risks, improves our whole-of-government incident response capabilities, enhances information sharing of best practices and cyber threats, and strengthens resilience of our Nation's critical infrastructure.

Cyber Threats

Cyber threats remain one of the most significant strategic risks for the United States, threatening our national security, economic prosperity, and public health and safety. The past several years have marked a growing awareness of the cyber domain in the public consciousness. Federal networks face large and diverse cyber threats ranging from unsophisticated hackers to technically competent intruders using state-of-the-art intrusion techniques. We have seen advanced persistent threat actors, including hackers, cyber criminals, and nation-states, increase the frequency and sophistication of their attacks. Our adversaries develop and use advanced cyber capabilities in attempts to undermine critical infrastructure, target our livelihoods and innovation, steal our national security secrets, and threaten our democratic institutions.

Cybersecurity Priorities

CISA, our government partners, and the private sector are all engaging in a more strategic and unified approach towards improving our Nation's overall defensive posture against malicious cyber activity. In May 2018, DHS published the Department-wide *DHS Cybersecurity Strategy*, outlining a strategic framework to execute our cybersecurity responsibilities during the next five years. Both the Strategy and Presidential Policy Directive 21- Critical Infrastructure Security and Resilience, emphasize that we must maintain an integrated approach to managing risk.

The *National Cyber Strategy*, released in September 2018, reiterates the criticality of collaboration and strengthens the government's commitment to work in partnership with industry to combat cyber threats and secure our critical infrastructure. Together, the *National Cyber Strategy* and *DHS Cybersecurity Strategy* guide CISA's efforts to secure federal networks and strengthen critical infrastructure. DHS works across government and critical infrastructure industry partnerships to share timely and actionable information as well as to provide training and technical assistance. Our work enhances cyber threat information sharing between and among governments and businesses across the globe to stop cyber incidents before they occur and quickly recover when they do. By bringing together all levels of government, the private sector, international partners, and the public, we are enabling a collective defense against cybersecurity risks, while improving our whole-of-government incident response capabilities, enhancing information sharing of best practices and cyber threats, strengthening our resilience, and facilitating safety.

The Department of Homeland Security's Cybersecurity Responsibilities

CISA works with federal civilian departments and agencies to implement common policies and best practices that help manage risk in the face of ever-evolving threats. By protecting systems and sharing information, alerts can be issued at machine speed when events are detected to help protect networks across the government information technology enterprise and the private sector. This enterprise approach helps transform the way agencies manage cyber networks through strategically-sourced tools and services that enhance the speed and cost effectiveness of federal cybersecurity procurements and allow consistent application of best practices.

CISA is embracing our statutory responsibility to administer the implementation of federal agency cybersecurity policies and practices by leading the effort to secure the federal civilian executive branch enterprise. The overarching goal of federal cybersecurity is to ensure that every agency maintains an adequate level of cybersecurity, commensurate with its own risks and with those of the federal enterprise. The result is a mix of decentralization and centralization in governance and implementation. Agencies implement their cybersecurity programs and manage their own risk, as they are best positioned to understand how their unique mission environments need to be protected. While individual agencies ultimately must implement their own cybersecurity risk-management programs because they are best positioned to understand their unique mission environments, DHS works with the Office of Management and Budget (OMB) to ensure an adequate level of security enterprise-wide and to address systemic risks and interdependencies across and between agencies. DHS also supports agency efforts to reduce their vulnerabilities to cyber threats by providing tailored capabilities, tools, and services to protect legacy systems, as well as cloud and shared infrastructure

CISA's efforts are guided by three principles: 1.) risk-oriented, 2.) cost-effective and scalable, and 3.) leading and collaborative. DHS addresses the greatest risks first and focuses on the highest impact systems, assets, and capabilities. This means centering efforts around the most critical systems across the federal enterprise, including High Value Assets (HVA). CISA will be more engaged and focused on identifying and securing these systems. Cost-effective, scalable approaches will achieve the most risk reduction for the investment. Actions like policy changes, analysis, operational planning, and engagement can sometimes have greater cost-effectiveness than additional technical services or capabilities. CISA leads through direct action and offerings, but also through collaboration and communication with agencies and partners, such as OMB, the

General Services Administration (GSA), and the National Institute of Standards and Technology (NIST).

The *Federal Information Security Modernization Act of 2014* provided the Secretary of Homeland Security with the authority to develop and oversee implementation of Binding Operational Directives (BOD) to agencies. In 2016, the Secretary issued a BOD on securing HVAs, or those assets, federal information systems, information, and data for which unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States' national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people. CISA works with interagency partners to prioritize HVAs for assessment and remediation activities across the Federal Government. For instance, CISA conducts security architecture reviews on these HVAs to help agencies assess their network architecture and configurations.

As part of the effort to secure HVAs, CISA conducts in-depth vulnerability assessments of prioritized agency HVAs to determine how an adversary could penetrate a system, move around an agency's network to access sensitive data, and exfiltrate such data without being detected. These assessments include services such as penetration testing, wireless security analysis, and "phishing" evaluations in which CISA network security operators send emails to agency personnel (with consent of the requesting agency) and test whether recipients click on potentially malicious links. CISA has focused these assessments on federal systems that may be of particular interest to adversaries or support uniquely significant data or services. These assessments provide system owners with recommendations to address identified vulnerabilities. CISA also works with the GSA to ensure that contractors can provide assessments that align with our HVA initiative to agencies.

Another BOD issued by the Secretary directs civilian agencies to promptly patch known vulnerabilities on their Internet-facing systems that are most at risk from their exposure. The National Cybersecurity and Communications Integration Center (NCCIC) conducts Cyber Hygiene scans to identify vulnerabilities in agencies' internet-accessible devices and provides mitigation recommendations. Agencies have responded quickly in implementing the Secretary's BOD and have sustained this progress. When the Secretary issued this BOD, CISA identified more than 360 "stale" critical vulnerabilities across federal civilian agencies, which means the vulnerabilities had been known for at least 30 days and remained unpatched. Since December 2015, CISA has identified an average of less than 40 critical vulnerabilities at any given time, and agencies have addressed those vulnerabilities rapidly once they were identified. By conducting vulnerability assessments and security architecture reviews, CISA is helping agencies find and fix vulnerabilities and secure their networks before an incident occurs.

When necessary, DHS can also issue emergency directives to federal agencies in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency. This year, CISA issued the first emergency directive after carefully considering the current and potential risk posed to federal agencies. On January 22, CISA directed federal civilian agencies to take a series of immediate actions in response to a global Domain Name System (DNS) hijacking campaign. DNS is part of the global internet infrastructure that translates the names humans prefer, such as www.dhs.gov, to numbers computers need to access a website or send an email. The hijacking campaign by malicious actors allowed them to obtain access to accounts that controlled DNS records, allowing them to obtain decrypted data on the internet while looking normal to users. This risk necessitated quick action to ensure the security of federal networks, and we did not hesitate.

DHS's two primary federal network protection programs are the National Cybersecurity Protection System (NCPS) and Continuous Diagnostics and Mitigation (CDM). NCPS is an integrated system-of-systems that delivers intrusion detection and prevention, analytics, and information sharing capability for federal networks. NCPS primarily targets traffic flowing into and out of federal networks. One of its key technologies is the EINSTEIN sensor set. This technology provides the Federal Government with an early warning system, improves situational awareness of intrusion threats to federal networks, near real-time identification of malicious cyber activity, and prevention of malicious cyber activity. NCPS provides the technological foundation necessary to enable DHS to secure and defend federal networks.

The CDM program provides federal agencies with a risk-based and cost-effective approach to mitigating threats inside the network. The program fortifies the cybersecurity of government networks and systems by providing federal network defenders with a common set of capabilities and tools they can use to identify cybersecurity risks and threats within their network on an ongoing basis, prioritize these risks based on potential impact, and mitigate the most significant problems first. DHS works with individual agencies to assess their systems and networks, identify risk, and deploy the CDM tools and capabilities they need. By pooling requirements across the federal space, DHS is able to provide departments and agencies with flexible and cost-effective options to mitigate those risks and secure their networks.

The operational side of these programs comes together at CISA's NCCIC. The NCCIC provides entities with information, technical assistance, and guidance they can use to secure their networks, systems, assets, information, and data by reducing vulnerabilities, ensuring resilience to cyber incidents, and supporting their holistic risk management priorities. The NCCIC operates at the intersection of the Federal Government, state and local governments, the private sector, international partners, law enforcement, intelligence, and defense communities. The *Cybersecurity Information Sharing Act of 2015* (P.L. 114-113) established DHS as the Federal Government's central hub for the sharing of cyber threat indicators and defensive measures. By focusing on rapid sharing of the technical features that permit network defenders to identify and respond to threats while minimizing the receipt of personally identifiable information, CISA's automated indicator sharing capability allows the Federal Government and private sector network defenders to share technical information at machine speed in a way that also protects privacy and civil liberties.

CISA's NCCIC provides a broad range of capabilities to assist private sector entities across all 16 sectors of critical infrastructure. In addition to information sharing and incident response, these capabilities include assessments and technical services as well as recommended remediation and mitigation techniques that improve the cybersecurity posture of our Nation's critical infrastructure. Among other services, these include vulnerability scanning and testing, penetration testing, phishing assessments, and red teaming on operational technology that includes the industrial control systems which operate our nation's critical infrastructure.

Supply Chain Risks

There are also steps we can take to secure the actual hardware agencies use to build their networks and the software that runs them. Information and Communications Technology (ICT) is critical to every business and a government agency's ability to carry out its mission efficiently and effectively. Vulnerabilities can be exploited intentionally or unintentionally through a variety of means, including deliberate mislabeling and counterfeits, unauthorized production, tampering, theft, and insertion of malicious software or hardware. If these risks are not detected and mitigated, the impact to the ICT supply chain could be a fundamental degradation of its confidentiality, integrity, or availability and potentially create adverse impacts to essential government or critical infrastructure systems.

CISA recently launched the ICT Supply Chain Risk Management (SCRM) Task Force as a public-private partnership to mitigate emerging supply chain threats. The Task Force is the main private sector point of entry for our SCRM efforts and is jointly chaired by DHS and the chairs of ICT Sector Coordinating Councils (SCC). The Task Force is focused on supply chain threat information sharing, supply chain threat mapping and assessment, establishing criteria for qualified bidder and manufacturer lists, and incentivizing the purchase of ICT from original manufacturers and authorized resellers.

Election Security

One of the highest-profile threats we face today is attempts by nation-state actors to maliciously interfere in our democratic elections. 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 successful implementation of a model that helps illustrate how CISA's cyber and critical infrastructure security missions complement each other, and the critical role CISA plays in bringing stakeholders at all levels together to address a common threat. We are now working to build upon these efforts during the 2020 election cycle.

Since 2016, 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) also convened Federal Government and election officials regularly through the Election Infrastructure Subsector Government Coordinating Council (GCC) to share cybersecurity risk information and to determine an effective means of assistance. DHS and the EAC also worked with election vendors to launch an industry-led SCC, a self-governed council with leadership designated by sector membership that serves as the industry's principal entity for coordinating with the Federal Government. All of these efforts enhanced

DHS's ability to identify, assess, and manage risks to election infrastructure in concert with state and local government partners and the private sector organizations that support elections.

Within the context of today's hearing, I will highlight CISA's efforts in 2018 to help enhance the security of elections administered by jurisdictions around the country, along with our election related priorities through 2020.

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 engages 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 ICT, 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.

We also partnered with trusted third parties to analyze relevant cyber data, including the Multi-State Information Sharing and Analysis Center (MS-ISAC), 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 Election System Security

During the 2018 midterms, CISA provided a coordinated response from DHS and its federal partners to plan, prepare, and mitigate risk to election infrastructure. CISA and our stakeholders increased awareness of potential vulnerabilities and provided capabilities to enhance the security of U.S. election infrastructure and ensure a more secure election.

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. CISA helps stakeholders in federal departments and agencies, SLTT governments, and the private sector to manage these cybersecurity risks. Consistent with our long-standing partnerships with SLTT governments, we work with election officials to share information about cybersecurity risks, and to provide voluntary resources and technical assistance.

CISA also 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 operates the EI-ISAC. The EI-ISAC has representatives co-located with CISA's NCCIC to enable regular collaboration and access to information and services for election officials.

Providing Technical Assistance and Sharing Information

Knowing what to do before a security incident happens, whether physical or cyber, 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 SLTT 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 security of systems connected to the Internet, such as online voter registration, election night reporting, and other 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 is 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 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 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 extent possible, DHS also provides classified information to cleared stakeholders, as appropriate, and 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 helps 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: www.dhs.gov/hometown-security.

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 vendors.

In August 2018, DHS hosted a "*Tabletop the Vote*" exercise, a three-day, first-of-its-kind event to assist 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 simulation of a realistic incident scenario, exercise participants discussed and explored potential impacts to voter confidence, voting operations, and election integrity. Partners for this exercise included 44 states and the District of Columbia; the EAC; the Department of Defense; Department of Justice; Federal Bureau of Investigation; Office of the Director of National Intelligence; NIST; National Security Agency; and the U.S. Cyber Command.

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. This effort partnered DHS with state governments to produce county-specific cybersecurity snapshot posters. The posters contained valuable information for auditors, staff and voters, including a checklist and timeline election officials should follow to ensure security of the elections in their county. 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 which gave election officials virtual access to the 24/7 operational watch floor of the 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.

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. We 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.

DHS goals for the 2020 election cycle include improving the efficiency and effectiveness of election audits, continued incentivizing the patching of election systems, and working with states to develop cybersecurity profiles utilizing the NIST framework. 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 remains committed to working collaboratively with those on the front lines of administering our elections to secure election infrastructure from risks. In February, 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-ins for these individuals regarding the current threats facing our election infrastructure.

We will remain transparent and 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.

Conclusion

In the face of increasingly sophisticated threats, DHS employees stand on the front lines of the Federal Government's efforts to defend our Nation's federal networks and critical infrastructure. The threat environment is complex and dynamic with interdependencies that add to the challenge. As new risks emerge, we must better integrate cyber and physical risk in order to effectively secure the Nation. CISA contributes unique expertise and capabilities around cyber-physical risk and cross-sector critical infrastructure interdependencies, and is where CISA brings unique expertise and capabilities.

I appreciate this Committee's leadership in working to adequately resource CISA as we work to fulfill our mission. Your support over the past few years has helped greatly as we worked to bring federal departments and agencies into NCPS, speed deployment of CDM tools and capabilities, and build our election security efforts. We at CISA are committed to working with Congress to ensure our efforts cultivate a safer, more secure and resilient Homeland while also being faithful stewards of the American taxpayer.

Thank you for the opportunity to appear before the Committee today, and I look forward to your questions.