TESTIMONY OF

Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

BEFORE

Select Committee on Intelligence
United States Senate

ON

An Update on Foreign Threats to the 2024 Elections

May 15, 2024
Washington, D.C.

Chairman Warner, Vice Chairman Rubio, 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 private sector partners to manage risk to our Nation's election infrastructure. Since election infrastructure's designation as a critical infrastructure subsector in 2017, CISA and our partners have made extensive progress increasing the security and resilience of our country's election infrastructure.

Elections are the golden thread of our democracy, and the American people's confidence that their vote will be counted as cast is essential. An electoral process that is both secure and resilient is a vital national interest and one of our Agency's highest priorities. From federal agencies to the state and local election offices across the country responsible for administering elections, election security remains a central national security priority for all levels of government.

We remain vigilant to a wide range of possible threats across physical and cyber domains that could target election infrastructure. We are also keenly aware our democracy faces a continuing threat from foreign adversaries that seek to mislead the public regarding U.S. election infrastructure, as demonstrated during previous federal election cycles. These persistent threats reinforce the need for continued federal support to state and local election officials who serve on the frontlines defending our electoral process. State and local election officials cannot be expected to combat sophisticated, nation-state-sponsored threat actors and cyber criminals alone. This served as a rationale for the designation of election infrastructure as a critical infrastructure subsector in the first place, and that remains true today.

Before I get into a more detailed description of how CISA supports the election infrastructure community, I want to emphasize three important points.

First, our election infrastructure is more secure today than ever. CISA's connection with the election stakeholder community has never been stronger, and a larger number of stakeholders are using CISA's voluntary, no-cost services than ever before. This progress, which serves as the foundation for securing election infrastructure during the 2024 election cycle, was made possible by years of incredible work by election officials and private sector election vendors to strengthen the security and resiliency of our elections process. So there is no doubt, let me restate what we have said before: there remains no evidence that any votes were deleted, lost, or changed in the 2018, 2020, or 2022 federal elections.

Second, despite this progress, we are not complacent about challenges facing U.S. election infrastructure. We recognize an increasingly complex threat environment ahead of us in 2024. CISA remains committed to keeping the election community as informed and prepared as possible to meet a range of security risks to election infrastructure. CISA has made election security a top priority throughout 2024, and internally we are prioritizing resources and services to support election entities, as well as taking steps to increase our ability to meet election stakeholders where they are. For example, CISA recently launched our #PROTECT2024 website,[1] designed to provide a consolidated list of our key services and resources for election infrastructure stakeholders to help them reduce risk to the security of election infrastructure during this election cycle.

Third, our ability to work as reliable and effective partners with the election community is enabled by the tremendous work of our Intelligence Community (IC) colleagues. Through our close coordination with our IC partners, including DHS's Office of Intelligence and Analysis, and information sharing channels established with the election infrastructure community, we share actionable intelligence and information about threats to election infrastructure. We facilitate this information sharing through

[1] https://www.cisa.gov/topics/election-security/protect2024

direct communication with our field staff across the country to election stakeholders, classified and unclassified threat briefings, tabletop exercises, election official conference panel participation, Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) notifications, and other efforts. We use intelligence and insights from our federal and private sector partners to warn election officials regarding nefarious cyber activity that help prevent, detect, or stop ransomware attacks and other malign cyber incidents that could target election systems and networks. We also use intelligence to develop and strengthen our risk guidance, services, and other resources to ensure they remain relevant.

It is because of these strong collaborative efforts both within the federal government and across the election infrastructure community that we are confident in the security and integrity of our election infrastructure as we navigate the 2024 election cycle. While incidents may occur, we believe in the ability of election stakeholders to effectively manage risk and the federal government's readiness to assist where appropriate.

Stakeholder Support to Election Infrastructure Risk Mitigation

CISA primarily provides assistance to election infrastructure stakeholders in three ways: (1) information sharing; (2) no-cost, voluntary service delivery; and (3) no-cost trainings.

Information Sharing. CISA shares information via multiple lines of effort, from disseminating timely and actionable intelligence and information directly to stakeholders, to developing best practice security products describing risks and how to mitigate them. CISA and our stakeholders are better positioned to share information with our growing field staff, including recently established regional Election Security Advisor (ESA) positions with direct lines of communication to election stakeholders across the country, and an EI-ISAC with the largest membership yet that includes all 50 states and more than 3,700 local jurisdictions. The EI-ISAC, which is partially funded by CISA, provides cybersecurity services to, and enables rapid real-time situational awareness and cybersecurity information sharing across, the election infrastructure community. For access to classified intelligence reporting, CISA sponsors over 230 security clearances for election officials and key private sector election infrastructure partners, with clearances available to election officials in all 50 states.

Additionally, through our role as the Sector Risk Management Agency (SRMA) for the Election Infrastructure Subsector, CISA convenes federal government and state and local election officials through the Government Coordinating Council (GCC) and works with election equipment and service vendors to facilitate an industry-led Sector Coordinating Council (SCC). CISA regularly engages with these councils to determine how the federal government can best assist election stakeholders in sharing information and mitigating risk.

No-Cost, Voluntary Service Delivery. CISA offers various security assessments, incident management assistance, and cybersecurity services at no-cost. We provide a range of cyber services including continuous scanning of election infrastructure systems and networks for internet-facing vulnerabilities known as Cyber Hygiene, advanced cyber vulnerability assessments, threat hunting and incident response management assistance, and management of the top level domain for .gov. Our field staff—which include Cybersecurity Advisors (CSAs), Protective Security Advisors (PSAs), and ESAs—serve all 50 states and six territories to provide expert guidance and tailored assistance. CISA's CSAs are trained personnel who help private sector entities and state, local, Tribal, and territorial (SLTT) officials prepare for and protect themselves against cybersecurity threats.

CSAs introduce stakeholders to CISA cybersecurity 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 physical security aspects of infrastructure protection. PSAs meet with election infrastructure stakeholders to share information, conduct physical security assessments of election facilities, conduct resilience surveys, and offer resources, training, and access to other CISA products and services. ESAs are now on board and providing election stakeholders tailored support across the country in every one of CISA's 10 regions. ESAs are subject matter experts in state and local elections processes, procedures, and technologies. They work to ensure CISA capabilities and services are being optimally employed to meet the specific needs of each state or local election jurisdiction. ESAs increase the agency's internal election security expertise, augment its ability to coordinate efforts to support elections stakeholders, and ensure CISA provides the most effective risk mitigation assistance possible.

No-Cost Training. CISA offers a wide array of no-cost cyber, physical, and operational security trainings and exercises to ensure stakeholder readiness and resiliency. Training raises awareness about the evolving threat landscape and promotes election security best practices. Topics include phishing, ransomware, generative artificial intelligence (AI)-enabled capabilities, non-confrontational de-escalation techniques for election workers, and securing election offices from physical security threats. Since the beginning of 2023, CISA has provided more than 220 trainings reaching over 9,000 participants. CISA also offers a range of tabletop exercises to include: pre-set scenarios election officials can download and employ; tailored state and local level in-person or virtual custom exercises; and, our annual national level exercise called Tabletop the Vote, which we lead in coordination with the National Association of Secretaries of State (NASS) and the National Association of State Election Directors (NASED). These exercises assist stakeholders to identify best practices and areas for improvement that cover traditional security concerns and more recent evolving security challenges.

Identifying, Assessing, and Mitigating Cyber Risk to Election Infrastructure

To address cybersecurity risks to election infrastructure, CISA works closely with state and local officials and private sector partners to improve their cybersecurity posture. We do this by offering a suite of no-cost, voluntary cybersecurity services, assessments, and risk mitigation guidance products, such as *No Downtime in Elections: A Guide to Mitigating Risks of Denial-of-Service*, to help these officials better understand and reduce their exposure to threats by taking a proactive approach to mitigating attack vectors.

One of CISA's primary tools for improving cybersecurity is our Cyber Hygiene Vulnerability Scanning service, which helps users identify vulnerabilities in internet-facing systems. CISA provides weekly Vulnerability Scanning reports to nearly 1,000 election infrastructure stakeholders 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. Additionally, CISA 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. Since the beginning of 2023, CISA has provided over 340 cyber assessments for election-related entities.

Through EI-ISAC, CISA also funds priority cybersecurity services, specifically Malicious Domain Blocking and Reporting (MDBR) and Endpoint Detection and Response (EDR). MDBR technology prevents IT systems from connecting to known harmful web domains, helping limit infections related to known malware, ransomware, phishing, and other known cyber threats. This capability can block many ransomware infections by preventing initial outreach to a ransomware delivery domain. Over 250 election-related entities are actively receiving this service. EDR is a solution deployed on endpoint devices to identify, detect, respond to, and remediate security incidents and alerts. Today, over 230 election-related entities across 40 states have this capability deployed, covering more than 21,000 election-related endpoints.

CISA also manages the .gov top level domain, which is available to government organizations like election offices, and we work extensively to improve security offerings of the .gov domain and make transitioning easier than ever. CISA made .gov signups for election offices a priority, because of the critically important role it plays in helping the American people understand they are accessing content from official government 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.

Identifying, Assessing, and Mitigating Physical Risk to Election Infrastructure

CISA provides a suite of resources to state and local election officials and security personnel to help them harden the physical security posture of election offices, storage and ballot counting facilities, voting sites, and other physical election infrastructure to reduce the likelihood and potential harmful impact of physical security incidents targeting elections.

Since the beginning of 2023, CISA has provided over 520 physical security assessments of election infrastructure locations. These assessments are designed to rapidly evaluate a facility's security posture and identify options for facility owners and operators to mitigate relevant threats, to include both near term low to no-cost solutions, and longer term infrastructure improvements. CISA also developed and implemented a training program for SLTT law enforcement personnel on how to conduct CISA-developed physical security assessments to increase the number of trained personnel across the country who can help reach a great number of critical infrastructure entities, to include election offices.

CISA is prioritizing the creation and distribution of resources to assist election officials in improving personnel safety and physical security of election infrastructure. This includes:

- Training materials for election stakeholders focused on de-escalation and broader non-confrontational techniques to help poll workers and other front-line election staff navigate potentially escalating situations and evaluate suspicious behaviors holistically at voting sites and election facilities. Training on this topic reached more than 3,100 election stakeholders in the past 18 months, and an abbreviated companion video on de-escalation for election workers was viewed more than 18,000 times on CISA's YouTube channel.
- The *Election Infrastructure Insider Threat Mitigation Guide* and companion training assists election stakeholders in improving existing insider threat mitigation practices and establishing an insider threat mitigation program. These resources reached more than 1,100 election stakeholders.
- CISA developed resources to help mitigate physical and personal threats against critical infrastructure entities writ large, to include the election infrastructure community. In January, CISA released the *Personal Security Considerations Action Guide for Critical Infrastructure Workers* that helps critical infrastructure workers assess their security posture and provides actionable recommendations and resources to prevent and mitigate threats to their personal safety. CISA also released guidance on mitigating the impacts of doxing on critical infrastructure entities and personnel. This resource defines and provides examples of doxing, explains potential impacts of doxing to critical infrastructure, and offers protective and preventative measures, mitigation options, and additional resources for individuals and organizations.

Identifying, Assessing, and Mitigating Risk to Election Infrastructure Operations

In many cases, security best practices are also effective at helping mitigate operational risks to election infrastructure. For example, implementing chain of custody controls and standard operating procedures are primarily intended to ensure election infrastructure systems and assets are used and handled securely, but they also provide a roadmap for election workers to ensure processes are reliable and repeatable. CISA provides a variety of voluntary guidance in these areas for election stakeholders, such as *CISA Insights: Chain of Custody and Critical Infrastructure Systems.*

CISA also offers incident response planning guidance and incident management assistance, including maintaining a 24/7, 365 day operations center through which stakeholders can contact CISA to report an incident and seek technical security assistance. For periods of heightened election operations, CISA stands up an Elections Operations Center, convening federal partners, private sector and non-profit election stakeholders, both in-person and virtually. The Elections Operations Center allows stakeholders to share information in near-real time and ensures appropriate individuals have national level visibility on election infrastructure threats and disruptions.

CISA provides resources like the *Cyber Incident Notification Planning and Incident Response Guide*, designed to form the basis of a cyber incident response plan. CISA works through state election offices to deliver its “Last Mile” initiative, focused on developing tailored products to assist election workers with incident response and security preparedness. So far in the 2024 election cycle, CISA has or is scheduled to deliver more than 380 customized products to more than 2,000 jurisdictions and is working with more states to provide similar, tailored incident response guidance to their local election offices ahead of the November general election.

We recognize that plans are only part of the solution—plans must be paired with training and practice to ensure effective implementation. To that end, CISA works to provide training and exercises for thousands of election infrastructure partners every year. Since the beginning of 2023, CISA has hosted over 70 tabletop exercises for election stakeholders to walk through realistic scenarios and help test incident response plans. In 2023, for our sixth iteration of the annual national-level Tabletop the Vote exercise, CISA hit record participation with more than 1,300 state and local election officials from over 40 states and the District of Columbia.

Mitigating Foreign Malign Influence Operations against Election Infrastructure

The Office of the Director of National Intelligence’s 2024 Annual Threat Assessment highlights how China, Russia, and Iran are the primary nation-state actors leveraging influence operations to target the U.S. elections process, with the aim of exploiting perceived sociopolitical divisions to undermine confidence in U.S. democratic institutions and shape public perception toward their interests. This threat is not new and was witnessed across multiple federal election cycles. America’s adversaries target U.S. elections as part of their efforts to undermine U.S. global standing, sow discord inside the United States, and influence U.S. voters and decision making. CISA is committed to helping defend critical infrastructure, including election infrastructure, against the risk of foreign malign influence operations. We do this in three distinct ways.

First, we develop publicly available security guidance for election officials that address tactics and techniques employed in foreign adversary influence operations so election infrastructure stakeholders can be better postured to identify and respond to these incidents. For example, in April 2024, CISA released *Securing Election Infrastructure against the Tactics of Foreign Influence Operations*, a resource co-authored with the Federal Bureau of Investigation (FBI) and the Office of the Director of National

Intelligence. In January 2024, CISA released the *Risk in Focus: Generative AI and Election Security* guide which provides an overview of how generative AI-enabled capabilities are often used by malicious actors to target the security and integrity of election infrastructure, and basic mitigations to address these threats. In late 2023, CISA worked closely with the National Security Agency and the FBI to release *Contextualizing Deepfake Threats to Organizations,* a fact sheet that provides an overview of synthetic media threats, techniques, and trends.

Second, CISA provides context to common narratives and themes that relate to the security of election infrastructure and related processes through our *Election Security Rumor vs. Reality* website. Established in 2020, this website includes over 25 posts seeking to complement election officials' voter education and civic literacy efforts by addressing common disinformation narratives through accurate information related to election security and related processes.

Third, and most importantly, CISA amplifies accurate election security-related information shared by state and local officials, who understand their processes and systems best. For example, the National Association for Secretaries of State (NASS) relaunched an initiative, first introduced in 2019, as #TrustedInfo2024.[2] CISA amplifies efforts that connect individuals with their state election officials as trusted sources for election information.

Closing

Our election infrastructure is diverse, managed locally by state and local government offices to meet their unique jurisdictional requirements, and involves in-depth layers of defense and redundancies to ensure security and resilience. It is because of these measures and the incredible efforts of election workers across the country that the American people can have confidence in the security of our elections process.

As the threat environment evolves, CISA will continue to work with federal agencies, state and local partners, private sector election infrastructure partners, and partisan organizations to enhance our understanding; and to make essential physical and cybersecurity tools and resources available to the election stakeholder community to ensure the continued security and resilience of our election infrastructure. At CISA, ensuring the security of our election infrastructure is one of our highest priorities and we remain transparent and agile in our vigorous efforts to fulfill this mission.

[2] https://www.nass.org/initiatives/trustedinfo