#PROTECT2024

OUR MISSION

Help election officials and election infrastructure stakeholders protect against the cyber, physical, and operational security risks to election infrastructure during the 2024 election

OUR PRIORITIES

1. Enhance Election Stakeholders' Understanding of Risk to Election Infrastructure
2. Assist Election Infrastructure Stakeholders with Taking Risk Mitigating Actions
3. Help Election Stakeholders Ensure the Readiness of Election Infrastructure
4. Provide Election Stakeholders with Threat Intelligence Warning and Response
5. Facilitate Federal Government Operational Integration and Coordination

CISA SUPPORT TO ELECTION INFRASTRUCTURE STAKEHOLDERS

Across the nation, CISA is working to help election infrastructure stakeholders understand and manage risk to 2024 elections. We do this in three ways: 1) information sharing; 2) no-cost, voluntary security services; and 3) no-cost trainings. CISA shares information through multiple means, from publishing products that explain the cyber, physical, and operational risks to election infrastructure and steps to mitigate them, to working with the intelligence community and other partners to provide the most up-to-date understanding of the threat landscape. CISA offers a range of voluntary, no-cost services such as continuous scanning of election infrastructure systems and networks for internet-facing vulnerabilities and incident response management assistance. We also fund additional security services like endpoint detection and response software through the EI-ISAC. CISA also provides no-cost trainings like tabletop exercises and deep dives on specific threat topics.

CISA's cadre of critical infrastructure security experts located around the country also offer tailored local support to election infrastructure stakeholders. CISA Cybersecurity Advisors can perform onsite cyber assessments and provide more targeted cybersecurity guidance based on an organization's specific security posture. Similarly, CISA Protective Security Advisors can assess physical infrastructure and provide options for consideration to reduce vulnerability to physical threats. Crucially, each of CISA's 10 regions now has an Election Security Advisor (ESA) who operates as a kind of a "CISA Navigator" for election stakeholders. ESAs oversee CISA's election security support in each region and work hand-in-hand with state election offices to ensure that CISA is agile in meeting each state's unique needs. ESAs leverage their expertise, as former election administrators, to help CISA rapidly identify and prioritize the most salient risks, and connect stakeholders—state officials, local officials, and election vendors—to the appropriate mitigation resources, services, and tools.

FIRST THINGS FIRST...

ESSENTIAL STEPS TO ENHANCE YOUR SECURITY POSTURE FOR 2024

1. **Enable Multifactor Authentication (MFA).** Passwords alone are not always effective at protecting your organization's data. Requiring MFA is a simple way to protect your organization and can prevent account compromise attacks.
2. **Know and manage your cyber vulnerabilities.** Know and manage what vulnerabilities bad actors can see on your organization's internet-facing systems. Sign up for CISA's no-cost Cyber Hygiene Vulnerability Scanning by emailing **vulnerability@cisa.dhs.gov**.
3. **Get a physical security assessment.** Learn about your physical security posture by contacting your CISA Regional team members or your emergency management partners to discuss receiving a no-cost physical security assessment.
4. **Get a .gov domain.** Transition your website and email to a .gov domain to make it easy for the public to identify you and your office as official government sites and to protect against cybersecurity and impersonation risks.
5. **Rehearse your incident response plan.** Incident response is a team effort. Work with your team and partners, like local law enforcement, critical service providers, and other government offices, to rehearse your incident response plan so your first time using it is not during a crisis. Contact your CISA regional team to request a CISA Tabletop Exercise (TTX).
6. **Join the Elections Infrastructure ISAC (EI-ISAC).** EI-ISAC membership is open to all U.S. state, local, tribal, and territorial organizations that support election officials. Membership is voluntary, no-cost for participants, and provides access to a range of free security services. Join the EI-ISAC online at **learn.cisecurity.org/ei-isac-registration**.

Protect Your...

The following actions can help improve your email security:

- **Sign Up for Malicious Domain Blocking and Reporting:** Blocks attempts to connect to known harmful web domains. This is a free resource for EI-ISAC members.
- **Implement Multi-Factor Authentication for Accounts.**
- **Sign Up for End Point Detection and Response Software:** Deployed on endpoint devices to identify, detect, respond to, and remediate security incidents and alerts. This is a free resource for EI-ISAC members.
- **Transition to a .GOV Domain:** Makes email accounts and websites easily identifiable as a government organization to protect against impersonation.

The following actions can help protect your official websites:

- **Sign Up for Web Application Scanning:** Assesses the health of your publicly accessible web applications by checking for vulnerabilities and weak configurations.
- **Use DDoS Protection Services:** You can find free services offered by CISA's private sector partners on our services page.
- **Transition to a .GOV Domain:** Makes email accounts and websites easily identifiable as a government organization to protect against hijacking and impersonation.

The following actions can help improve your election network:

- **Sign Up for No-Cost CISA Cyber Hygiene Vulnerability Scanning:** Provides enrollees with a recurring report on vulnerabilities and other exploitable conditions visible from the Internet, prioritizing those that are known to be exploited by adversaries.
- **Implement Multifactor Authentication for Accounts.**
- **Sign Up for End Point Detection and Response Software:** Deployed on endpoint devices to identify, detect, respond to, and remediate security incidents and alerts. This is a free resource for EI-ISAC members.
- **Implement Albert Sensors:** EI-ISAC offers 24x7 managed and monitored intrusion detection systems enabling the detection of malicious traffic targeting state, local, tribal, and territorial (SLTT) networks.

The following actions can help secure your election systems:

- **Implement effective chain of custody procedures and policies.**
- **Review CISA's Best Practices for Securing Election Systems.** Organizations can implement these best practices, which harden enterprise networks and strengthen election infrastructure, at little or no cost.
- **Review CISA's Election Infrastructure Insider Threat Mitigation Guide.** Take steps to mitigate against potential threats.

The following actions can help secure your election office:

- **Request a Physical Security Assessment:** A Security Assessment at First Entry (SAFE) helps identify high level physical security vulnerabilities and mitigation options.
- **Request CISA Trainings on Various Security Threat Topics:** CISA provides in-person or virtual trainings on a range of physical and cyber threat topics, such as active shooter and bomb threat preparedness.
- **Request a CISA Tabletop Exercise (TTX) to rehearse your Incident Response Plan:** CISA offers no-cost in-person or virtual TTXs tailored to state and local election stakeholders.

The following actions can help secure your election office:

- **Review CISA Security Best Practice Guides on the #PROTECT2024 website** that cover individual security and personal safety.
- **Enact Strict Security Controls** on all Professional and Personal Accounts.
- **Limit Publicly Available Personal Identifying Information.** Find more information in CISA's guide for "Mitigating the Impacts of Doxing on Critical Infrastructure"

#Protect2024 CISA Trainings and Services

CISA Election Security Trainings

No-cost trainings that can be delivered in-person or virtually. Each typically runs 30-90 minutes. For more information or to request a training, email electionsecurity@cisa.dhs.gov.

Election Security Specific Trainings

- CISA Election Security Overview
- Building Trust Through Secure Practices
- Non-Confrontational Techniques for Election Workers
- Securing Local Election Offices
- Insider Threats
- Generative Artificial Intelligence and Foreign Malign Influence Operations

Cyber Risk Trainings

- Phishing
- Ransomware

Physical Risk Trainings

- Active Shooter Preparedness
- Bomb Threat Preparedness
- Suspicious Items Identification and Response

Operational Resilience Trainings

- Emergency Communications Preparedness
- Communications "PACE" Planning

CISA Election Security Tabletop Exercises (TTXs)

No-Cost In-Person or Virtual State and Local TTXs to help stakeholders rehearse incident response plans. To request an exercise, email **cisa.exercises@cisa.dhs.gov** or reach out to your CISA regional staff.

Election Security "TTX in a Box": Election security scenarios updated for the 2024 election threat environment that are ready for use by election officials to train their teams. For more information, visit **cisa.gov/CTEPS**

7th Annual Tabletop the Vote: Join us in August 2024 for CISA's seventh annual national-level election security TTX that provides the opportunity for SLTT governments, private sector election partners, national political committees, and other members of the election community to come together, plan for various scenarios, and improve response plans. Contact your Regional CISA ESA or **TTXvote@cisa.dhs.gov** for more information.

Physical and Cybersecurity Assessments

CISA security advisors are available throughout the CISA Regions to provide cyber and physical security assessments to help SLTT organizations build mature and resilient cyber and physical security programs. Contact your CISA Regional staff to request an assessment: **cisa.gov/about/regions.**

CISA Cybersecurity Services

Sign-up for CISA's voluntary, no-cost cyber services like: Cyber Hygiene Vulnerability Scanning so you know what vulnerabilities bad actors can see about your organization's internet-facing systems. CISA also offers Web Application Scanning, to evaluate publicly accessible web applications to uncover vulnerabilities and misconfigurations that attackers might exploit. Sign up here: **cisa.gov/cyber-hygiene-services.**

Tailored "Last Mile" Security Best Practice Products

The CISA Last Mile initiative provides election administrators and their partners a range of customizable resources based on security best practices and industry standards to help secure election infrastructure nationwide. Contact **electionsecurity@cisa.dhs.gov** to develop your own Last Mile products and visit **cisa.gov/last-mile-products** to download the "Last Mile Toolkit", which provides an overview of the customizable product templates.

Election Security Resource Library

CISA's election security resource library provides voluntary informational resources for use by State, local, tribal, and territorial (SLTT) governments, private sector election infrastructure partners, and the public.

#PROTECT2024 CHECKLIST

FIRST THINGS FIRST: IF YOU DO NOTHING ELSE, PRIORITIZE THESE:

- □ Implement multifactor authentication for all official network accounts, email accounts, and social media accounts.
- □ Sign up for CISA's no-cost Cyber Hygiene Vulnerability Scanning and Web Application Scanning. Work with your local CISA Cybersecurity Advisor (CSA) to help ensure your office is remediating any identified vulnerabilities.
- □ If you have not had one already, request a no-cost CISA physical security assessment for your election facilities.
- □ Transition your email and website to a .gov domain. Set it up so any traffic to your existing email addresses and website is forwarded to the new .gov email or address. Even if you aren't able to transition to .gov this year, you can still reserve your jurisdiction's domain.
- □ Sign up for a CISA tabletop exercise to rehearse your incident response plan.
- □ Join the EI-ISAC to get access to real-time threat information sharing and free resources and services.

CYBER

- □ Request in-person or virtual CISA trainings on phishing and ransomware.
- □ Request a briefing from your local CSA on CISA's cybersecurity services and how they could assist your office.
- □ Get Endpoint Detection & Response software for your office's systems. This is a free resource for EI-ISAC members.
- □ Implement Malicious Domain Blocking and Reporting to help protect against unintentional access to malicious sites. This is a free resource for EI-ISAC members.
- □ Read the latest CISA publications on cyber threats for a better understanding of the 2024 threat environment.
- □ Ensure all accounts, including social media accounts, have the strongest security settings possible and remove personally identifiable information that may be available online about you, your staff, or your family.

PHYSICAL

- □ Request CISA in-person or virtual trainings on physical threats.
- □ Use CISA's "Physical Security Checklist for Polling Locations" to help mitigate risk at voting locations.

OPERATIONAL RESILIENCE

- □ Request a CISA in-person or virtual training on Emergency Communications and "PACE" Planning.
- □ Request customized "Last Mile" products for your state.
- □ Participate in Tabletop the Vote, CISA's annual national-level election security exercise.
- □ Develop and rehearse your continuity of operations plan.
- □ Establish relationships with state and local law enforcement so you know who to contact to report criminal activity.
- □ Develop and implement a public communications plan to increase the public's understanding of your election processes and security measures.
- □ Develop and practice an incident response communications plan—make sure it includes how to respond to common tactics used in foreign malign influence operations targeting election infrastructure (check out CISA's guide "Securing Election Infrastructure against Tactics of Foreign Malign Influence Operations")