CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

Key Steps for Election Officials to Take to Improve Their Cybersecurity Posture

Election officials can improve their cybersecurity posture by taking advantage of any of the following cybersecurity services that are provided by the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA). All of these services are free.

Step 1: Join the EI-ISAC

Information sharing is key to security. You can't secure your infrastructure without first knowing the threats to protect against, the assets to protect, and how to mitigate the threats to those assets. The Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) was created to serve the election community by providing near real-time threat and risk sharing as well as cybersecurity best practices geared towards election officials.

The EI-ISAC is a dedicated resource that gathers, analyzes, and shares information on critical infrastructure and facilitates two-way cybersecurity threat information sharing between the public and the private sectors. The EI-ISAC supports the election infrastructure community through:

- 24 x 7 x 365 network monitoring
- Election-specific threat intelligence
- Threat and vulnerability monitoring
- Incident response and remediation
- Training sessions and webinars
- Promotion of security best practices

Membership in the EI-ISAC is open to all state, local, tribal, and territorial (SLTT) government organizations and associations that support elections in the United States. To join the EI-ISAC, visit https://learn.cisecurity.org/ei-isac-registration.

Step 2: Know Your System

Knowing your election infrastructure means that you have identified your network and system vulnerabilities, are able to recognize the warning signs of strange network behavior and have policies in place to mitigate issues as they arise.

For assistance with identifying vulnerabilities, consider enrolling in CISA's **Vulnerability Scanning**, which is a voluntary, free scanning of internet-accessible systems for known vulnerabilities on a continual basis.

As potential issues are identified, DHS notifies impacted customers so they may proactively mitigate risks to their systems prior to exploitation. The service incentivizes modern security practices and enables participants to reduce their exposure to exploitable vulnerabilities, which decreases stakeholder risk while increasing the Nation's overall resiliency.

Administered by CISA staff, Vulnerability Scanning is conducted remotely and is fully automated. You will receive weekly assessment results detailing current and previously mitigated vulnerabilities, high-risk hosts, and other port, device, and network attributes that organizations working to improve their cybersecurity posture should examine. The report also provides recommended mitigations for each vulnerability discovered via the scanning process. For additional information or to enroll in Vulnerability Scanning, contact nccicustomerservice@hq.dhs.gov.

Step 3: Test the Security of Your Infrastructure

Test the security of your externally accessible systems through CISA's **Remote Penetration Testing**, which utilizes a dedicated remote team to assess and identify vulnerabilities and work with customers to eliminate exploitable pathways.

Administered by CISA staff, the assessment takes place over a six-week period and simulates the tactics and techniques of real-world threats and malicious actors. Potential scenarios for the assessment include an external penetration test, an external web application test, and targeted phishing attacks. An assessment report is provided two weeks after the conclusion of the assessment. The report provides guidance and recommendations for mitigating any vulnerabilities uncovered over the course of the assessment. For additional information or to sign up for Remote Penetration Testing, contact ncciccustomerservice@hq.dhs.gov.

Step 4: Train to Withstand Phishing

Fortify your staff and further strengthen your election infrastructure through CISA's **Phishing Campaign Assessment**, which measures the susceptibility of an organization's staff to social engineering attacks, specifically email phishing attacks.

Administered by CISA staff, the assessment takes place over a six-week period. An assessment report is provided two weeks after the conclusion of the assessment. The report provides guidance, measures effectiveness, and justifies resources needed to defend against and increase staff training and awareness of generic phishing and the more personalized spear-phishing attacks. For more information and to arrange the assessment, contact ncciccustomerservice@hq.dhs.gov.