CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

Cybersecurity Best Practices for Election Officials

What steps can election officials take to increase the security of their infrastructure?

Stay Informed of New and Emerging Cyber Threats and Vulnerabilities

Ensure that your organization receives timely and relevant cyber threat indicators and technical vulnerability information. Joining the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) is one recommended solution. This information sharing center 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. Membership in the EI-ISAC is open to all state, local, tribal, and territorial government organizations and associations that support elections in the United States. To join the EI-ISAC for free, visit https://learn.cisecurity.org/ei-isac-registration.

Mitigate Vulnerabilities in a Timely Manner

Your organization should mitigate all internet-accessible vulnerabilities, such as unpatched web applications, in a timely manner. For context, the federal government requires its departments and agencies to mitigate all vulnerabilities at the critical severity level within 15 calendar days and to mitigate vulnerabilities with lower severity levels within 30-60 calendar days.

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, CISA notifies customers so they may proactively mitigate risks to their systems prior to exploitation. To enroll in Vulnerability Scanning, contact nccicustomerservice@hq.dhs.gov. Your organization should have an established Patch Management Policy and utilize equipment that is maintainable with current security patching. Exceptions should be minimized and isolated to limit risk.

Control Access to Your Infrastructure

Your organization should utilize multi-factor authentication and perform regular audits of password policies. Password best practices include ensuring that default passwords are changed, that strong passwords are required, and that administrators utilize encrypted password vaults. For additional information on password best practices, visit https://pages.nist.gov/800-63-3/sp800-63b.html. For additional information on multi-factor authentication, visit https://www.dhs.gov/publication/election-security-resource-library.

Internal network architecture should protect and control access to your most sensitive systems. User workstations should be less trusted and connections to external networks should be isolated, controlled, and monitored. For example, employees with access to voter registration data should utilize a separate workstation for email and internet access.

Have a Plan and Implement Backups

Your organization should have an Incident Response Plan and a Continuity of Operations Plan. The Continuity of Operations Plan should identify a restoration point based on what makes sense for your system, determine the frequency of backups, and include a strong patching methodology for operating systems and third-party products. For best practices on Continuity of Operations Plans and a template for an Incident Response Plan, visit https://www.dhs.gov/publication/election-security-resource-library.