Center for Internet Security®

Technology Recommendations for Federal Election Security Funding

In December 2019, Congress appropriated $425 million to states, through the Election Assistance Commission, to improve elections systems and train personnel who administer elections. The Center for Internet Security (CIS) is providing recommendations for state and local election offices to invest these funds in cybersecurity initiatives.

Understand Risk, Manage Strategically

Risk management is a process. With an infusion of resources, one of the best ways to reduce risk is to establish a risk management approach that can serve you in the long term. These activities will help put your election office on a path to ongoing success and help prioritize your investments.

1. Establish a statewide cyber navigator program to support local jurisdictions in making cybersecurity decisions. The Illinois Cyber Navigator program is a good example.
   - *https://www.ncsl.org/Portals/1/Documents/Elections/NCSL_Thomas_Presentation.pdf*
2. Contract with an organization (or use your navigator) to conduct a full assessment of your infrastructure's security posture and policies. CIS' A Handbook of Elections Infrastructure Security provides a valuable framework of 88 security best practices. Election offices can leverage the free Elections Infrastructure Assessment Tool to easily assess their posture against the Handbook.
   - *https://www.cisecurity.org/elections-resources/elections-infrastructure-handbook-part-1/*
   - *https://www.cisecurity.org/elections-resources/election-security-self-assessments/*
3. Verify your risk assessment with a vulnerability analysis of high risk technology systems and mitigate identified vulnerabilities. In addition, implement a plan for ongoing risk management and vulnerability assessment activities. One option is CISA's cyber hygiene program and Risk and Vulnerability Assessments.
   - *https://www.dhs.gov/sites/default/files/publications/19_0531_cisa_election-security-resources-guide-may-2019.pdf*

Implement Known Effective Mitigations

Once you have a clear picture of your risk profile, prioritize mitigations that will lower your overall cybersecurity risk. These are some recommendations that election officials should consider to address their risks.

1. Conduct security awareness training for all staff and election officials. Consider training available on DHS's Federal Virtual Training Environment such as the "Election Officials as IT Managers" course. Discounted end user awareness training is also available from SANS through the CIS CyberMarket.
   - *https://fedvte.usalearning.gov/*
   - *https://www.cisecurity.org/services/cis-cybermarket/training/*
2. Implement multi-factor authentication (MFA) on all election infrastructure to reduce the chances that malicious actors will access sensitive accounts or resources. MFA can include a variety of techniques, to include the use of smart cards, certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods.
   - *https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-multi-factor-authentication/*
3. Install security sensors that provide traffic monitoring for network-connected elections components. Albert sensors are available to all U.S. state and local election offices at a low cost from CIS.
   - *https://www.cisecurity.org/services/albert-network-monitoring/*

4 Complement Albert with endpoint detection and response (EDR) software on devices to identify and block malware and anomalous activity. CIS is currently developing an EDR solution for state, local, tribal, and territorial governments to secure high value assets, including election infrastructure.
   https://www.cisecurity.org/services/edr/

5 Appropriately segment your network to protect sensitive election systems. Sharing network space with non-election systems increases the risk of compromise.
   https://www.cisecurity.org/elections-resources/security-best-practices-for-non-voting-election-technology-1/

6 Establish Distributed Denial of Service (DDOS) Mitigation services. Denial of service attacks have the potential to disrupt systems at critical times. Many services are available to mitigate these attacks at no-cost to election offices, but additional funded support may be needed to protect components not covered by these programs.
   https://www.cisecurity.org/white-papers/technical-white-paper-guide-to-ddos-attacks/

7 Deploy Web Application Firewalls (WAFs). WAFs secure web applications from common attacks and exploits, such as SQL injection. Some providers offer free WAFs to election offices, but they may not cover everything you need. Consider negotiating to add WAFs to applications not covered by these programs.
   https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-web-attack/

8 Add protections for removable media by buying write-block USBs, USB formatters, or investing in USBs with hardware-based encryption. Removable media are the most likely vector for compromising indirectly connected infrastructure, so extra protections are encouraged.
   https://www.cisecurity.org/elections-resources/security-best-practices-for-non-voting-election-technology-2/

9 Invest in a patch management system to prevent known vulnerabilities and respond quickly when new patches become available.
   https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-patching/

10 Implement and test a thorough system recovery program. Go beyond data backups to address rapid restoration and recovery with minimal downtime.
   https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-backups/
   https://www.cisecurity.org/spotlight/cybersecurity-spotlight-disaster-recovery-plan-drp/

11 Deploy secure configuration profiles across all devices. Consider using CIS Benchmarks for local systems and CIS Hardened Images for cloud deployments.
   https://www.cisecurity.org/cis-benchmarks/
   https://www.cisecurity.org/cis-hardened-images/

For more information on these and other security best practices, see *https://www.cisecurity.org/elections-resources/*

About The Center for Internet Security (CIS)

www.cisecurity.org
info@cisecurity.org
518.266.3460

31 Tech Valley Drive
East Greenbush,
New York 12061

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments. We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously refine these standards to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the cybersecurity needs of U.S. elections offices.