Homeland Security

May 2018

Election Infrastructure - Cybersecurity

PRE-ELECTION ACTIVITIES

Voters Registered

ELECTION DAY ACTIVITIES

Voters Checked In

Voters Cast Ballots

Votes Counted and Tallied

Results Submitted on Election Night

POST-ELECTION ACTIVITIES

Election Results Tallied

CYBERSECURITY CONSIDERATIONS

Auditability

To enhance election system integrity, states are prioritizing the purchase and deployment of auditable voting systems. Post-election audits are an important step to ensuring the integrity and resilience of the process. Consider using funding to hire temporary staff for organizing and running post-election audits. This can quickly improve the efficiency and effectiveness of the audit process and lessen the burden on overworked and understaffed election offices.

Planning and Exercises

A comprehensive, well-practiced incident response plan can ensure a resilient process, enabling response and recovery from potential disruptions. Election officials are natural contingency planners and many already have well-thought-out contingency plans. Consider using resources and funding to update existing plans, to include the development, implementation, and training of cyber-incident response. Developing and exercising these plans can be a relatively low-cost, high-benefit area of focus.

Training

All election staff have a responsibility to keep our elections systems secure. Regular training and testing raises awareness on cybersecurity best practices. Consider funding and implementing cybersecurity training for all staff, not just IT professionals.

Defensibility

Defensibility begins with an understanding of which systems and data need to be defended. Understanding the high-value/high-risk components of election IT systems allows for prioritization of funding. Consider investing in full system architecture reviews, which can be a critical starting point for risk mitigation decisions.

Resilience

The ability to detect, defend, mitigate, and recover from cyber incidents is critical to maintaining the integrity of the election process. Consider investing in regular online and offline backups of critical data (e.g., voter registration data). Testing and refining backup methods can improve the election system's ability to recover from ransomware or other cyber attacks intended to destroy or alter data.

Homeland Security

May 2018

Immediate Resources for Election Officials

The most valuable resource election officials have is time. Every day they are one day closer to another election which means they literally have no time to waste. Identifying the risks to their systems and possible solutions can be time consuming and costly for local election officials who have neither time or money to waste. But a solution exists: The Department of Homeland Security's National Protection and Programs Directorate (NPPD) offers cyber expertise and services at no cost to election officials to augment their arsenal of cybersecurity tools.

NPPD offers a broad range of cyber products and services free to state and local election officials including network and system assessments either self-administered or undertaken by NPPD staff; alerts and bulletins; best practices; and mitigation and incident response.

Local election officials can immediately begin to improve their cybersecurity position through three simple, straightforward steps:

Step 1: Know Your System

Knowing your elections infrastructure means knowing your network and system vulnerabilities and warning signs of strange network behavior – known as "anomalies" – and knowing what to do about them.

NPPD's **Cyber Hygiene** assessment is a voluntary, **FREE** ongoing examination of a network's traffic, data flows, and relationships between devices and provides a sophisticated analysis including identifying unusual and potentially suspicious activity.

Administered by NPPD staff experts, the assessment takes place during a one-week period. After the assessment's conclusion, elections officials will receive an in-depth report of key discoveries and practical recommendations for improving an organization's cybersecurity operation to mitigate known vulnerabilities and sure up its defenses. After the initial report participating election offices will receive ongoing reports every week for continued improvement and response to evolving threats to election systems. **For more information and to arrange the assessment, contact nccicustomerservice@hq.dhs.gov.**

Step 2: Know Your Staff Needs To Withstand Phishing

Elections are at their core a human activity. Election officials rely on professional and temporary staff to support any election. Awareness and training of that staff is critical to improving the security of the election process. Strengthen your elections infrastructure through NPPD's **Phishing Campaign Assessment**, which measures the susceptibility of an organization's staff to social engineering attacks, specifically email phishing attacks.

Administered by NPPD staff, the assessment takes place during a six-week period. An assessment report is provided two weeks after its conclusion. The assessment 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 nccicustomerservice@hq.dhs.gov**.

Step 3: Join the EI-ISAC

Begin improving your cybersecurity status with information sharing. You can't secure your election infrastructure without knowing the threats to protect against, assets to protect, and how to protect them.

Join (for free!) the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC). 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.

The EI-ISAC is a dedicated resource that gathers, analyzes, and shares information on election 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:

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

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. DHS encourages state and local elections agencies to use this initiative to receive the information they need to help protect their systems. **To join the EI-ISAC, please complete the registration form.**

https://learn.cisecurity.org/ei-isac-registration