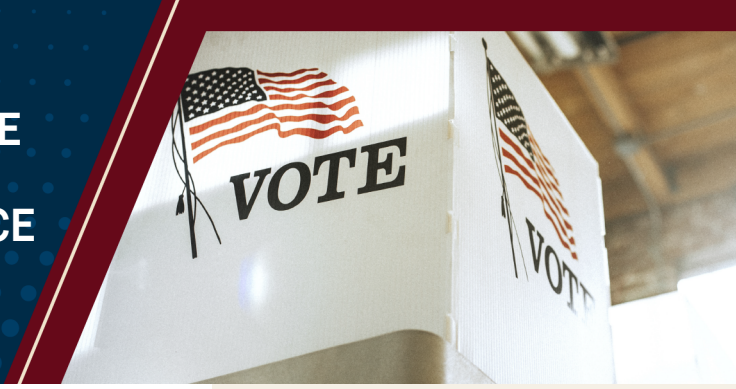
ELECTION INFRASTRUCTURE CYBERSECURITY READINESS AND RESILIENCE CHECKLIST



INTRODUCTION

Network infrastructure and internet-facing applications underpin and enable a variety of functions in the conduct of elections. These may include election infrastructure networks that store, host, or process voter registration information, public -facing election websites that support functions like election night reporting and polling place lookup, as well as email and other critical business operations. Election infrastructure and government infrastructure remain attractive targets for a range of malicious actors from cybercriminals to nation state actors. Network defenders have the power to prevent most security incidents using basic security measures. Take steps now so that even if an incident occurs, critical election operations can continue. The following checklist was designed to help election security officials and their IT teams quickly review existing cybersecurity practices to protect against some of the most common threats like ransomware or distributed denial of service (DDoS) attacks and take steps to enhance your organization's cybersecurity readiness and resilience throughout this election cycle.

HOW TO USE THIS RESOURCE

This checklist provides a series of questions to guide the decision-making necessary to prepare for potential cybersecurity incidents. By answering these questions, elections personnel and their IT teams will be better positioned to assess their current cybersecurity posture against common threats and identify additional actions that may be taken.

SECURITY CHECKLIST

Protect and Respond: Phishing Attempts Targeting Your Email

YES / NO **Have you enabled Multifactor Authentication (MFA) on all accounts?**

- Turn on MFA for **all accounts**.
- Ensure each account has its own unique credentials and do not allow credential sharing.
- Apply the principle of least privilege by separating admin accounts and user accounts.
- Ensure everyone changes their default passwords and strong passwords are required for **all accounts**.

YES / NO **Have you enabled Domain-based Message Authentication Reporting and Conformance (DMARC) for all email accounts?**

- Enable DMARC on all email accounts to make it easier for email senders and receivers to determine whether an email legitimately originated from the identified sender and provides the user with instructions for handling the email if it is fraudulent.

YES / NO **Is email filtered to protect against malicious content?**

- Implement flagging of external emails to alert users to use due care when opening.

YES / NO **Does your elections staff only use official email accounts for official business?**

- Train staff so they know to only use their official email accounts, which often include enhanced security features, for official business.
- Implement filters at the email gateway to filter out emails with known malicious indicators.

YES / NO

Have you trained your staff to spot and report phishing or other suspicious emails?

- Malicious actors are improving their techniques all the time, so training should be provided at regular intervals to educate staff about the latest tactics and how to respond to suspicious communications. Regularly review common signs of phishing so staff are familiar with what to look out for and how to report.

Protect and Respond: Distributed Denial of Service (DDoS) Targeting Your Websites

YES / NO

Have you spoken with your website service and internet providers about preparation for and response to a DDoS incident?

- Review existing contracts and coordinate with both website service providers and internet service providers before an incident occurs. Understand the protections service providers may already have in place.
- Identify what additional DDoS mitigation and redundancy measures are available. Most major service providers have protections available, which may be offered at no cost for basic services, or at additional cost for advanced services. There are a number of no-cost DDoS prevention services available to election officials that can be found at: https://www.cisa.gov/topics/election-security/protect-your-website
- Ensure you know who to contact in event of an incident.
- Share information about important election dates and locations, requesting that ample troubleshooting is available during key periods, and ensuring mutual awareness of any planned maintenance that could impact election operations.
- Ensure network traffic monitoring and analysis is enabled via a firewall or intrusion detection system and that the logs are being reviewed.
- Have an alternate plan for information dissemination in case your website does go down. Make sure to test that plan.

Protect and Respond: Ransomware Targeting Your Nework

YES / NO

Is the election network segmented from other business units by utilizing a firewall configured to only allow known communications?

- Implement and enforce network segmentation. Proper network segmentation is an effective security mechanism to prevent an intruder from propagating exploits or moving laterally within an internal network. This includes not transferring election results on the business network.

YES / NO

Is internal network traffic monitored for malicious traffic, using an endpoint detection and response (EDR) software or similar service?

- Implement EDR software on endpoint devices. If you are a member of the Election Infrastructure Information and Analysis Center (EI-ISAC) you are eligible for no-cost commercial EDR solutions funded by CISA.
- Verify alerts are being created and response process are followed.

YES / NO

Is your network traffic protected from routing to known malicious sites?

- Implement Malicious Domain Blocking and Reporting (MDBR) across your network devices to prevent IT systems from connecting to harmful web domains. MDBR can block the vast majority of ransomware infections just by preventing the initial outreach to a ransomware delivery domain. EI-ISAC members are eligible for no-cost commercial MDBR services funded by CISA.

YES / NO

Do you have a cybersecurity incident response plan and have you practiced using it?

- Develop and maintain incident response plans that specifically detail how to operate mission-critical processes in the event of a cybersecurity incident.
- Test your incident response plans with all key players who would be involved in implementing the response. You can leverage CISA resources like in-person or virtual tabletop exercises to help facilitate the training event (https://www.cisa.gov/topics/election-security/election-security-training).

YES / NO

Do you maintain offline encrypted backups of your critical systems and data for a minimum of 30 days?

- Maintain backups that allow you to recover data at a minimum up to 30 days prior.
- Encrypt backup files and ensure credentials for accessing the backups are not stored in the targeted environment. Ransomware actors often hunt for and collect credentials stored in the targeted environment and use those credentials to attempt to access backup solutions; they also use publicly available exploits to target unpatched backup solutions.
- Ensure backups are maintained offline, as most ransomware actors attempt to find and subsequently delete or encrypt accessible backups to make restoration impossible unless the ransom is paid.

YES / NO

Have you recently practiced restoring from your data backups?

- Test the availability and integrity of backups in a disaster recovery scenario.

Protect and Respond: Known Exploited Vulnerabilities and Your Internet Facing Systems

YES / NO

Do you have cyber hygiene vulnerability scanning that identifies internet facing vulnerabilities?

- Sign up for CISA cyber hygiene vulnerability scanning or an equivalent service that continuously monitors and assesses internet-accessible network assets (public, static IPv4 addresses) to evaluate their host and vulnerability status. CISA's cyber hygiene vulnerability scanning service provides weekly reports of all findings and ad-hoc alerts about urgent findings, like potentially risky services and known exploited vulnerabilities.

YES / NO

Do you have a patch management program in place to enable you to close known or identified vulnerabilities and configuration errors quickly (15 days or less)?

- Develop a patch management plan that (1) makes reducing the significant risk of known exploited vulnerabilities (KEVs) a top priority for remediation; and (2) requires critical vulnerabilities to be remediated within 15 calendar days of initial detection.

RESOURCES

#Protect2024 | CISA
cisa.gov/topics/election-security/protect2024

Critical resources for state and local election officials including cybersecurity services, physical security services, and best practice security guides.

#StopRansomware Guide | CISA
cisa.gov/resources-tools/resources/stopransomware-guide

A comprehensive resource to help organizations reduce the risk of ransomware incidents through best practices to detect, prevent, respond, and recover.

No Downtime in Elections: A Guide to Mitigating Risks of Denial-of-Service | CISA
cisa.gov/resources-tools/resources/no-downtime-elections-guide-mitigating-risks-denial-service

Guidance on how to plan for, respond to, and recover from DDoS attacks.

Cyber Hygiene Services | CISA
cisa.gov/cyber-hygiene-services

Free cybersecurity services to help organizations reduce their exposure to threats by taking a proactive approach to monitoring and mitigating attack vectors.

Malicious Domain Blocking and Reporting (MDBR) | MS-ISAC/EI-ISAC
cisecurity.org/ms-isac/services/mdbr

A web security solution that is free for SLTT government entities and provides an additional layer of cybersecurity protection that is proven, effective, and easy to deploy.

Election Security CISA Tabletop Exercise Packages (CTEPs) | CISA
cisa.gov/resources-tools/resources/election-security-cisa-tabletop-exercise-packages-cteps

Customizable training packages with scenarios, discussion questions, references, and resources.

CYBERSECURITY QUICK TIPS

Election officials and IT professionals play a critical role in ensuring the cybersecurity of critical systems that election officials depend on. These tips can enhance security awareness and contribute to improved cybersecurity hygiene.

Remain Vigilant:
- ☐ If you are not expecting an email, and it seems unusual, call the sender to make sure they intended to send it.
- ☐ Report any suspicious behavior or activities to CISA, EI-ISAC or your local FBI field office.

Understand Contingency Plans:
- ☐ Review and update contingency plans for running critical election processes in the event of an IT systems outage.
- ☐ Practice contingency plans to ensure their effectiveness.

Handle Security Incidents Appropriately:
- ☐ Contact your IT professionals and follow your incident response plan.
- ☐ Report the cybersecurity incident to CISA, EI-ISAC or your local FBI field office.

Stay Informed:
- ☐ Stay up to date on security alerts, announcements, and procedural changes provided by management or election officials.
- ☐ Seek clarification on security measures or protocols if needed.