CHAPTER 13
ELECTION SECURITY

TABLE OF CONTENTS

ELECTION SECURITY

Elections are designated as **critical infrastructure** due to their importance and the potential threats they face. Understanding both the general risks to elections security and the specific threats to election day can help prepare for potential security incidents.

Be Aware of Threats & Create a Plan

Cyber threat actors, foreign nation states, and physical disruptors all represent potential threats to the elections process. These bad actors may attempt to utilize a variety of digital or real-world attacks, including but not limited to:

- **Hacking:** Attackers may attempt to infiltrate voting systems or access voter data through exploiting vulnerabilities, brute-force attacks, or phishing scams. These attempts can lead to unauthorized changes, data theft, or disruption of services.
- **Social Engineeering Attacks:** Criminals often employ psychological tactics to deceive victims into revealing sensitive information or granting access to restricted systems. Common examples include phone pretexting, email phishing, and impersonation scams.
- **Bomb Threats/Physical Violence:** Threats of violence, bomb threats, or physical altercations may be used to disrupt elections or cause a shut-down of polling locations. Large scale protests or other demonstrations could also take place in times of heightened tensions.
- **Insider Threats:** Individuals with authorized access may intentionally or unintentionally misuse their privileges for personal gain or malicious purposes, posing a significant risk to the security of voting systems and voter data.
- **Suspicious Packages or Substances:** Some organizations may handle large amounts of ballots or other packages that need to be opened, while others may rarely interact with mail. Attackers may use the mail to deliver potentially dangerous substances or chemicals.
-

Having and rehearsing an **Incident Response Plan (IRP)** for cyber or physical security issues is a best practice recommended by CISA (the Cybersecurity and Infrastructure Security Agency) and other Elections Officials. This helps you prepare and practice for an issue, before it impacts your organization.

CISA IRP Basics: https://www.cisa.gov/resources-tools/resources/incident-response-plan-irp-basics

Computer Security Considerations for Elections

These 4 simple steps can help keep Elections Software and other computer systems secure every day:

- **Strong passwords:** Use passwords that are long, random, and unique to each account, and use a password manager to generate them and to save them.
- **Multifactor authentication:** Use MFA to protect our most important data and systems, including email, elections software, and other related accounts.
- **Recognize and report phishing:** Think before you click! Be cautious of unsolicited emails, texts, or calls asking you for personal information.
- **Update software:** Enable automatic updates on software so the latest security patches keep our devices continuously protected.

CISA provides detailed guidance and security awareness training on these and many other topics **available at no cost**! They also offer free cyber hygiene, vulnerability scanning, and physical security assessments for elections offices.

Review the resources provided by their "Secure our World" Toolkit and elections guides located at:

- https://www.cisa.gov/resources-tools/resources/secure-our-world-resources-cybersecurity-awareness-month-2024-toolkit
- https://www.cisa.gov/cyber-hygiene-services.

Protecting Voter Data

Threat actors may use the attacks discussed previously and other tactics to compromise **sensitive Voter Data or PII** (Personally Identifiable Information). It is our duty as elections workers to safeguard this sensitive information.

- **Use secure transfer processes**: Use approved secure means such as encrypted email, secure file transfer protocols (SFTP), or a dedicated, encrypted storage platform. Avoid sending sensitive data via unencrypted channels like regular email attachments or text messages.
- **Understand the systems in use**: Make sure you understand the differences between voting systems and their security requirements including in test/stage/development/production and on Poll Pad devices.
- **Need to Know**: Ensure that anyone receiving data or asking for sensitive information has the proper authorization to view it and a valid "need to know" that information.

Ransomware

Ransomware is a type of malware that accesses a victim's data or systems and then locks or encrypts them while demanding a payment to get the data back. Attackers use these attacks in combination with phishing or other threats to trick a user to click on an attachment that appears legitimate but instead delivers the malware.

Elections are a high priority target for attackers due to the nature of the data involved.

The FBI recommends the following best practices to minimize ransomware risks:

- **Data Backups:** Have copies of important data & system configurations
- **Authentication:** Always utilize Multi-Factor Authentication
- **Software Updates:** Patch & Update All Systems for known vulnerabilities
- **IRP:** Review & Test Incident Response Plans

FBI Ransomware Guidance & Support https://www.ic3.gov/Home/Ransomware

Know Important Election Security Contacts

Knowing who to contact in an emergency or security incident is critical. Reaching out to establish contact with local agencies, State & County IT teams, and national elections support can streamline communications when time is of the essence. **Consider establishing or revisiting relationships** with elections security organizations ahead of election day:

- **Local Law Enforcement & Emergency Services:** Sheriffs, Local Police, Fire & EMS, Capitol police if on Capitol Grounds, and other agencies are all important partners in elections security.
- **CISA Elections Cyber Security Support:** CISA provides cyber incident support and response to various elections focused areas.
- **EI-ISAC Membership:** The Elections Infrastructure ISAC provides real time support & networking on election day via a virtual meeting room. Additionally, security analysts and other elections official share intelligence and best practices in briefings & trainings at no cost throughout the year.
- **State & County IT/Security Teams:** Local IT teams, VREMS Support & VREMS security, and State Security organizations like OCDC (Office of Cyber Defense Coordination) can also assist.

Appendix: Election Security Contacts

Point of Contact	Details
Nevada Office of Cyber Defense Coordination	OCDC@ocdc.nv.gov 775-431-6360
VREMS Security Team	Email: vremssecurity@sos.nv.gov
Nevada Region CISA & DHS Contact	Mayrene (May) Acosta (Las Vegas) Supervisory Cybersecurity Advisor (NV, AZ, Pacific) Email: Mayrene.acosta@cisa.dhs.gov Cell: (771) 217-0684
CISA Cyber Incident Support & Response	https://www.cisa.gov/reportreport@cisa.gov 888-282-0870
FBI Field Office Support	Nevada Special Agent in Charge - Spencer L. Evans 1787 West Lake Mead Boulevard Las Vegas, NV 89106-2135 lasvegas.fbi.gov (702) 385-1281

Appendix: Election Security Resources

Resource	Link
VREMS Security Resources SharePoint	VREMS Security Resources
Join the EI-ISAC!	https://learn.cisecurity.org/ei-isac-registration
EI-ISAC Essential Guide to Election Security	https://essentialguide.docs.cisecurity.org/en/latest/README.html
CISA Protect 2024	https://www.cisa.gov/topics/election-security/protect2024
CISA Secure World Toolkit	https://www.cisa.gov/resources-tools/resources/secure-our-world-resources-cybersecurity-awareness-month-2024-toolkit
CISA's Free Cyber Hygiene Services	https://www.cisa.gov/cyber-hygiene-services
USPS Suspicious Package Guidance & Reporting	https://www.uspis.gov/report/report-suspicious-mail
FBI Ransomware Resources	https://www.ic3.gov/Home/Ransomware