Security Awareness

AN INTRODUCTORY GUIDE FOR TEMPORARY ELECTION WORKERS

YOUR COUNTY ★ BOARD OF ELECTIONS

Basics of Information Security

The "CIA" Triad

- **Confidentiality** refers to protecting information from unauthorized access.
- **Integrity** means that data and information are trustworthy and complete and have not been altered by unauthorized activity.
- **Availability** means that data is available to authorized parties when it is needed.

Every cybersecurity incident can be related back to one or more of these basics being inadvertently or purposely affected:

- Theft of official sensitive voter registration information such as driver's license, or theft of personal information for voters with "confidential" status, such as victims of domestic violence. That is an example of a violation of *confidentiality.*
- Unauthorized changes to your party affiliation. That is an example of a violation of the *integrity* of your voter registration information.
- An elections office affected by ransomware, or a voter lookup website taken offline by a denial of service attack. These types of incidents affect *availability.*

Understanding "Our Part"

The basics of how we secure elections

There are many actions our office takes to ensure our elections are secure. This includes, but is not limited to:

- **Official Domains:** Implementing the .gov domain that is restricted for use by government entities so voters know their information is coming from an official source.
- **Data Backups:** Taking regular backups of important data is an essential step to protect your information in the event of a cybersecurity incident.
- **Security Patch Installation:** Hardware and software manufacturers generally release patches and security updates in response to new security vulnerabilities and known exploits. Installing patches is a critical step in maintaining the security of Internet-connected systems.

- **Least Privilege Access:** Granting users and applications minimum permissions necessary to perform tasks.
- **Segmentation:** Dividing the network into smaller parts, limiting an attacker's ability to move within the network.
- **Information Sharing:** Partnering with organizations such as EI-ISAC, CISA and state organizations to share information on threats and vulnerabilities.
- **Protect Infrastructure:** Using secure locations; limiting access; and following standard operating procedures, best practices and chain of custody protocols.
- **Test and Verify:** Testing systems prior to the election and performing audits to verify the results after the election.

Understanding "Your Part"

The actions you can take to make sure our security practices hold up

There are many actions you can take to ensure our elections are secure. This includes, but is not limited to:

- **Password Security:** Create strong, unique passwords for your accounts. Never share your passwords, and never use the same password for multiple accounts.
- **Safe Internet Practices:** Be wary about clicking on unknown links, visiting suspicious websites and downloading files from untrusted sources.
- **Social Media and Privacy:** Be aware of the risks of sharing personal information on social media sites. Become knowledgeable of privacy controls to limit unauthorized access to information shared via online sources.
- **Phishing Awareness:** Be skeptical of suspicious emails, especially those that request personal information or encourage you to take immediate action. Be especially cautious of emails from unknown senders, or unexpected emails with attachments.
- **Suspicious Activity Reporting:** When you see something, say something. When you notice anything out of the ordinary, report it promptly to appropriate IT or security personnel. Studies have shown that even when an incident does occur, the shorter the time for first response, the better the chances of containing any malicious infections.
- **Stick to the Plan:** Follow your office's procedures and ensure you are completing any proper documentation, such as chain of custody forms.
- **Physical Security:** Lock devices when not in use, properly store sensitive documents, and information and monitor devices when they are located in public spaces can help prevent incidents due to unauthorized access.
- **Sensitive Information Security:** Be aware of the risks of leaving sensitive information unmonitored or accessible to unauthorized personnel, such as internal procedure documentation, staff rosters and contact information or emergency procedures.