CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

Election Infrastructure Questionnaire

The Cybersecurity and Infrastructure Security Agency (CISA) created the following questionnaire to assist state, local, tribal, and territorial (SLTT) governments with implementing cybersecurity best practices to strengthen the security of their election infrastructure.

CISA recommends that organizations complete this questionnaire for internal use in the event of a cyber incident; an organization's answers to the questionnaire can provide significant information to federal and third-party incident response personnel. Although the organization may not immediately have an answer to every question, the process of answering the questions can facilitate valuable discussions. This documentation will give the organization greater understanding of their election infrastructure by providing a comparison between their current configuration and industry best practices.

Due to the sensitive nature of questionnaire answers, CISA recommends organizations store this documentation in a password-protected file in a secure location.

CISA recommends organizations complete the questionnaire prior to an election and before submitting a request for technical assistance from a third party.

GENERAL INFORMATION

Answering these questions will help identify key information regarding technology-related components of the organization's election infrastructure:

- **Review any diagrams that describe the communication paths and data flow (inputs and outputs) used by election-related information systems.** Are the diagrams accurate?
- **Where does the organization store election-related data?** (When answering, be as specific as possible.) What are the means by which the organization makes and receives updates to its election-related data and software (e.g., voter registration information, poll book data, ballot definition files, unofficial election results, campaign finance information, content management system software, electronic voting machine firmware, election management system software, electronic poll book [e-poll book] software)?
- **Is election-related data replicated?** If so, how, where, and for what purpose?
- **What organizations, including vendors, does the organization share election-related data with?**
- **What level of access is granted to the shared data** (e.g., is the data read-only or can the election-related data be modified or deleted)?

WEB PRESENCE

Answering these questions will help identify key information regarding technology-related components of the organization's election infrastructure:

- **Does the organization keep the content management software for its various websites up to date?**
- **Who has administrator access to websites?** What form of authentication is required for administrator access?
- **Does the organization utilize distributed denial-of-service (DDoS) mitigation services?**

- **Does the organization utilize input validation for forms and web applications to guard against attempted Structured Query Language injection?** Web application firewalls?
- **How does the organization secure DNS records related to its web presence?**

SOCIAL MEDIA ACCOUNTS

- **Who manages and has access to social media accounts used by the organization or its employees in an official capacity?**
- **What forms of authentication are used to access the accounts?**

VOTER REGISTRATION

Inventory and Interdependencies

Does the organization maintain an inventory of information systems that are involved in the voter registration process and any system interconnections (e.g., vendor systems, systems within and across state or local election organizations)? This should include the following descriptive information:

- **What software is used** (e.g., operating system(s), applications supporting voter registration, database(s), web servers, customization(s) from vendors)?
- **Does the state, local government, or a vendor, own the various information systems?** Who is responsible for their regular maintenance and security?
- **What, if any, interconnections exist between the voter registration system and other systems** (e.g., those maintained by a state's Department of Motor Vehicles)?
- **Are there any backups of the voter registration data?** If so, where are the backups stored? How often are they updated? When did the organization last test the backups?
- **Are there any devices related to voter registration that are always in use** (e.g., a web server that allows online registration) **or constantly on?**
    - How are these devices configured?
    - How are these devices updated?
    - Who has access to these devices? Who has administrative access to them?

Disposition of Personally Identifiable Information

- In order to register to vote, a citizen may have to provide personally identifiable information (PII), which may be verified against existing databases. **If the organization required registrants' PII, ask the following questions:**
    - **What information is publically available?** For example, some voter rolls list the home address and party affiliation of all registered voters.
    - **Which systems store PII used for voter registration verification?**
    - **What external system dependencies exist** (e.g., access to external systems) **to verify voter registration requests?**
    - **What types of PII are voters required to provide for verification?** How is this PII protected?
    - **How is PII entered into the various systems that support voter registration?** What protections are in place to ensure information is submitted and updated in a secure and accurate manner?
- **What is the process for exporting PII data for use in poll books or to generate mail ballots?**
    - Where is the data stored (e.g., vendor-owned system)? How is the data verified? What safeguards exist to protect the data?
- **Does the organization perform regular, recurring checks on voter data against other records that would change voter eligibility, such as deaths, relocations, name changes, etc.?**
    - If so, what are the processes for running these checks? At what intervals do the checks occur? How does the organization verify that all data used is legitimately sourced?

(E-)POLL BOOKS

- **How are poll books generated?** What information is included in the poll books, including any information not based on voter registration records?
- **What process does the organization use to update poll book data?**
- **What verification processes does the organization have to ensure that the poll books are correct?**
- **If the organization uses e-poll books, how are they configured?**
  - What hardware and operating system do the poll books use?
  - What network connections are available (e.g., Wi-Fi, Bluetooth) to the poll books?
  - When is the last time the e-poll book software was updated?
  - Are both the e-poll books and the underlying operating system patched against known vulnerabilities?
  - Are any additional services or applications running/installed on the e-poll books?
  - Who has administrative access to the e-poll books?
- **If using e-poll books, does the organization support live voter registration updates?** If so, does this include their current voting status?

ELECTRONIC VOTING MACHINES AND ELECTION MANAGEMENT SYSTEMS

- **If applicable, what make, model, and type** (e.g., Direct Recording Electronic, Ballot Marking Devices, Optical Scan) **of electronic voting machine(s) does the organization use?**
- **How does the organization check the integrity and versioning of firmware running on its electronic voting machines?**
- **What kind of election management system(s) (EMS) does the organization use?**
- **What are the associated processes for moving data related to 'programming elections' via the EMS?** For moving data/results from the voting machines, to the EMS, and then their displacement for election night (unofficial) reporting?
  - Is removable storage media used, and what steps are taken to ensure the integrity of data on the storage media?

VOTE TABULATION AND AUDITING

- **By what process does the organization tabulate votes?**
  - Where does the final tabulation take place?
  - What is the communications path for vote tabulation data? Include any associated diagrams formally documenting this process and confirm that the diagrams are up to date.
  - How does the organization check to ensure the integrity of the vote tabulation system/process and any transmitted data?
- **Do the organization's electronic voting machines create a voter-verified paper audit trail or are there paper ballots for all votes cast** (i.e., is there a paper record of all votes cast in polling places or by mail)?
- **Does the organization maintain physical copies of the ballots?** Where and for how long? How does the organization ensure these are secure?
- **Does the organization conduct post-election audits, including risk-limiting audits?** What is the process for conducting the audits?
- **What circumstances trigger an audit?**
- **What IT systems would be involved in an audit?**

ELECTION NIGHT REPORTING AND CERTIFICATION OF RESULTS

- **What is the organization's process for reporting unofficial results?**
    - What data needs to be validated for the organization to report unofficial results?
        - How is the necessary data received?
        - Who is permitted to transmit the data? How is it transmitted? How is it secured during transmission?
- **How are unofficial results communicated publically?**
    - If posted on a website, what content management system or other software solution is used? Is the website vendor-owned or operated?
    - Where else are unofficial results replicated?
- **What is the process for certifying and reporting official election results?** What information systems are relied upon as a part of this process?

NOTICE AND CONSENT BANNERS FOR COMPUTER SYSTEMS

This section identifies recommended elements in computing system notice and consent banners and provides an example banner. This section does not include legal advice, and the information it contains is not guaranteed to be accurate or complete. Anyone reviewing or developing a notice and consent banner should consider consulting an attorney and should note that laws can change rapidly, differ from jurisdiction to jurisdiction, and can be subject to various interpretations by various entities. Further, notice and consent banners can require tailoring based on the specific circumstances and legal jurisdiction at issue. The elements or the examples may be inadvisable depending on the entity or situation. Applicable laws may include the Fourth Amendment to the U.S. Constitution, any similar provisions in State Constitutions, and relevant federal- and state-level statutes.

Notice and Consent Banner Elements

1. The banner expressly covers monitoring of data and communications in transit rather than just accessing data at rest.
    a. Example: "You consent to the unrestricted monitoring, interception, recording, and searching of all communications and data transiting, traveling to or from, or stored on this system."
2. The banner provides that information in transit or stored on the system may be disclosed to any entity, including to government entities.
    a. Example: "You consent, without restriction, to all communications and data transiting, traveling to or from, or stored on this system being disclosed to any entity, including to government entities."
3. The banner states that monitoring will be for any purpose.
    a. Example: "…at any time and for any purpose."
4. The banner states that monitoring may be done by the entity or any person or entity authorized by the entity.
    a. Example: "…monitoring or disclosure to any entity authorized by [ENTITY]."
5. The banner explains to users that they have "no reasonable expectation of privacy" regarding communications or data in transit or stored on the system.
    a. Example: "You are acknowledging that you have no reasonable expectation of privacy regarding your use of this system."
6. The banner clarifies that the given consent covers personal use of the system (such as personal emails or websites, or use on breaks or after hours) as well as official or work-related use.
    a. Example: "…including work-related use and personal use without exception…."
7. The banner is definitive about the fact of monitoring, rather than being conditional or speculative.

    a. Example: "…will be monitored…"

8. The banner expressly obtains consent from the user and does not merely provide notification.
    a. Note: click-through banners can be best because they force the user to interact with the language.
    b. Note: supporting processes should generally also preserve/provide evidence of the user's agreement to the terms.
    c. Example: "By using this system, you are acknowledging and consenting to…"
    d. Example: "By clicking [ACCEPT] below…you consent to…"
9. Nothing in the remainder of the banner or associated policies, agreements, training, etc., is inconsistent with, or otherwise undercuts, the elements of the banner.

Example Banner

By clicking [ACCEPT] below you acknowledge and consent to the following:

All communications and data transiting, traveling to or from, or stored on this system will be monitored. You consent to the unrestricted monitoring, interception, recording, and searching of all communications and data transiting, traveling to or from, or stored on this system at any time and for any purpose by [the ENTITY] and by any person or entity, including government entities, authorized by [the ENTITY]. You also consent to the unrestricted disclosure of all communications and data transiting, traveling to or from, or stored on this system at any time and for any purpose to any person or entity, including government entities, authorized by [the ENTITY]. You are acknowledging that you have no reasonable expectation of privacy regarding your use of this system. These acknowledgments and consents cover all use of the system, including work-related use and personal use without exception.

ADDITIONAL RESOURCES

Elections-Specific Guidance

- **DHS Election Security Resource Library:** https://www.dhs.gov/publication/election-security-resource-library
- **Incident Handling for Elections:** https://www.dhs.gov/sites/default/files/publications/Incident%20Handling%20Elections%20Final%20508.pdf
- **Election Cyber Incident Communications Plan Template for State and Local Officials:** https://www.belfercenter.org/publication/election-cyber-incident-communications-plan-template
- **Securing Voter Registration Data Tip:** https://www.us-cert.gov/ncas/tips/ST16-001
- **Center for Internet Security (CIS) Handbook for Elections Infrastructure Security:** https://www.cisecurity.org/elections-resources-best-practices/

Patch Management Best Practices

- **Understanding Patches and Software Updates Tip:** https://www.us-cert.gov/ncas/tips/ST04-006
- **National Institute of Standards and Technology (NIST) Special Publication (SP) 800-40 Rev. 3: Guide to Enterprise Patch Management Technologies:** https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final
- **CIS Top 20 Security Controls:** https://www.cisecurity.org/controls/

Ransomware Best Practices

- **Protecting Against Ransomware Tip:** https://www.us-cert.gov/ncas/tips/ST19-001

Password Best Practices

- **Choosing and Protecting Passwords Tip:**

https://www.us-cert.gov/ncas/tips/ST04-002

- **Supplementing Passwords Tip:** https://www.us-cert.gov/ncas/tips/ST05-012
- **NIST SP 800-63B Digital Identity Guidelines Authentication and Lifecycle Management:** https://pages.nist.gov/800-63-3/sp800-63b.html

Enterprise Best Practices

- **Securing Enterprise Wireless Networks Tip:** https://www.us-cert.gov/ncas/tips/ST18-247
- **Website Security Tip:** https://www.us-cert.gov/ncas/tips/ST18-006