Homeland Security

DHS Election Infrastructure Security Funding Consideration

by the National Protection and Programs Directorate
Department of Homeland Security

June 13, 2018

Purpose

The purpose of this document is for the Election Infrastructure Subsector (EIS) Government Coordinating Council (GCC) to provide direction to the election community regarding possible considerations, both short and long term, for the use of the newly available election funding, as well as to provide support for procurement decisions regarding use of the funding.

Introduction

Recently congress made available to state and local election officials $380 million in funding for the improvement of federal elections. This money was intended to help states build on their existing funding and human capital investments by giving an additional infusion of funding for new resources and personnel to improve federal elections. This document, which was developed by the EIS GCC, is intended to raise awareness of resources and helpful practices that can assist election officials to do more with the resources afforded to them.

Election officials are advised to consult with the U.S. Election Assistance Commission before making any purchase to ensure it is an appropriate expenditure of funds.

Cyber Navigators

Some states already have, or are considering investing in, a "cyber navigator" or cyber liaison program. The purpose of these navigators is to provide practical cybersecurity knowledge, support and services to local election officials who otherwise would not have access to them. These navigators can conduct assessments of local election offices. After conducting assessments, the navigators can work with county IT staff or vendors to create cyber security policies, mitigate vulnerabilities discovered during the assessments, and establish best cyber hygiene practices within the office. Additionally, these navigators can serve as a resource to local election offices as they consider the purchase of new systems or services to improve the cybersecurity of the office. For example, they may participate in the procurement review process alongside local election officials.

States are approaching the use of cyber navigators in a variety of ways. Some are opting to make the navigators state election employees. Others plan on utilizing existing state personnel, such as the National Guard, or using contractors as cyber navigators.

Address Common Vulnerabilities

Listed below are common vulnerabilities seen in critical infrastructure sectors. Under each vulnerability are listed common mitigation strategies. Targeting resources toward mitigating these vulnerabilities is an effective and data-driven way of reducing risk in the election sector.

- **Spear-phishing** – These are highly targeted attacks that attempt to trick individuals into disclosing sensitive personal information through deceptive computer-based means.
  Possible mitigations may include:
    - **Phishing Assessments and IT Training**: Identify your organization's susceptibility to phishing attacks and establish practices for recognizing, removing, and reporting possible phishing campaigns. Staff need constant reminders and training to avoid phishing attacks.

- **Multi-Factor Authentication**: Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Upgrading voter registration systems, election night reporting systems, or other election office IT systems to multi-factor authentication can drastically limit the risks of phishing attacks.
- **Email Authentication:** Upgrading election office email systems to include SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) allow a sending domain to effectively "watermark" their emails, making unauthorized emails (e.g., spam, phishing email) easy to detect. When an email is received that doesn't pass an agency's posted SPF/DKIM rules, DMARC (Domain-based Message Authentication, Reporting & Conformance) tells a recipient what the domain owner would like done with the message. Setting a DMARC policy of "reject" provides the strongest protection against spoofed email, ensuring that unauthenticated messages are rejected at the mail server, even before delivery. Additionally, DMARC reports provide a mechanism for an agency to be made aware of the source of an apparent forgery, information that they wouldn't normally receive otherwise. Multiple recipients can be defined for the receipt of DMARC reports.
- **Access Control**: Access control practices, such as role-based access control, will not prevent phishing attacks but may limit the potential impacts of stolen credentials. Using a third-party assessment or audit to identify vulnerabilities and proactively define effective access control policies and configurations for your system helps limit the impact of phishing campaigns.

- **Unpatched Software –** Typically, new operating system and application vulnerabilities are patched when they are discovered. However, system administrators and users may fail to apply patches for a variety of reasons. When patches are not applied in a timely fashion, the affected machines remain vulnerable to exploitation.

  Possible mitigations may include:

  - **Patch Management**: Patch management describes the practices by which an organization tests and deploys security patches to their systems. Security patches are updates that correct specific problems for an operating system, application, or other software. Patches are developed and deployed as vulnerabilities are discovered, and proper patch management helps reduce the number of vulnerabilities that are present in your system. Federal patch management practices include attempting to patch or remediate high risk vulnerabilities within 30 day of detection.
  - Investing in a full system review, including a review of all needed system updates and patches is the simplest way to mitigate known vulnerabilities.
  - In addition, purchasing or building a patch management and ticket system will ensure ongoing patching processes.
  - Regularly monitor your systems and software manufacturers' websites for announcements regarding new vulnerabilities and patches.
- **Unsupported Operating System or Application** – Software which is no longer maintained by the vendor and therefore does not receive security updates for newly identified vulnerabilities.
  Possible mitigations may include:

    - Replacement of unsupported operating systems and applications is the preferred mitigation for this vulnerability.
    - Air-gapping can also limit, but not eliminate, the exposure of these vulnerable systems to compromise. A third party assessment or audit of security processes and procedures to include air gapping can help identify weaknesses like the use of contaminated media or insecure vendor practices.
- **Data Disclosure** – Vulnerabilities and/or configuration errors which make organizational data accessible to individuals through unauthorized means.
  Possible mitigations may include:
    - **Vulnerability Scanning and Penetration Testing:** Penetration testing is when evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability. This can help identify where and how datasets can be accessed in an unauthorized manner and provide mitigations for those vulnerabilities. Only well-vetted vendors of penetration testing services should be used because of their potential full access to critical election networks and systems during a test. See Apprendix for some suggested techniques for selecting vendors.
    - **Whitelisting:** An approved list of entities or applications that are provided a particular privilege, service, or access. Whitelisting can be an effective form of access control. Whitelisting recommendations may be included in a full security review or audit that is procured by an election office.
- **Insecure Default Configuration** – The configurations of out-of-the-box of hardware and software are often more permissive than necessary and are commonly known and understood by potential malicious actors.
  Possible mitigations may include:
    - Include in procurement language that the vendor shall install firmware updates available for the computer or network device certified by the system manufacturer at the time of installation and provide documentation.
    - Perform all security updates and always avoid use of default passwords.
    - Utilize system hardening guidance provided by the vendor or third party experts to ensure proper configuration for your operating environment. Jurisdictions may wish to contract with a third party for a full security review, including review of system configurations, to identify possible ways to better lock down the systems.

<u>Improving Your Overall Cybersecurity Posture</u>

Leveraging funds to hire people or procure tools and capabilities toward the following near-term objectives can provide direct, observable improvements to the resilience of the election process for this election cycle:

- **Auditability:** Deploying auditable voting systems is critical to the resilience of the process and is being prioritized by many states. With the continued move to auditable systems, post-election

auditing has become a common practice for many election jurisdictions. However, for many offices, the post-election audit process is time consuming and costly. Improving the overall efficiency and effectiveness of post-election audits is a quick way to improve the overall integrity of the process. Simple steps like hiring more temporary staff to organize and run the post-election audit is an effective way to lessen the burden on already over-worked and under-staffed election offices while improving the overall resilience of the process.

- **Planning and exercising:** Consider developing, implementing, training, and exercising a cyber incident response plan. A comprehensive well-exercised incident response plan can ensure a resilient process that is able to respond to and recover from possible disruptions. Election officials, as natural contingency planners, already have well-thought-out contingency plans. Using resources to update those plans to include cyber disruptions and exercising those plans is a relatively low-cost, high-benefit area of focus.
- **Training:** Consider training staff on IT and cybersecurity practices. Regular training and testing raises awareness. All staff are responsible for system security, not just the IT staff.
- **Defensibility:** Defensibility begins with an understanding of what systems and data you are defending. Having a full accounting of what systems you own and operate within your organization and which of these systems are high-value or high-risk targets provides the ability to prioritize security resources and funding decisions towards the highest impact items. Investing in a full system architecture review and risk analysis can be a critical starting point for risk mitigation decisions.
  Additionally, targeted purchasing of new systems or updates and following the above listed guidance regarding out-of-the-box software can reduce the level of risk surrounding the election process very quickly. For instance, several states have already indicated that they are looking to upgrade their voter registration databases to include items like two-factor authentication, or are moving to a top-down structure to support a more secure registration process.
- **Resilience**: Improving not only the defense posture but the ability to detect and recover from possible incidents is critical to maintaining the integrity of the election process. Investments in regular backups (both online and offline) of critical data (like voter registration data) and testing of those backups will ensure the ability to recover from possible ransomware or other attacks intended to destroy or alter data.

As a reminder, DHS and the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) provide election officials with several no-cost resources for your consideration. The full list of cybersecurity services provided by DHS can be found at https://www.dhs.gov/topic/election-security.

Some free services to consider taking advantage of include:

- **Cyber Hygiene Vulnerability Scanning:** Scanning of internet-accessible systems for known vulnerabilities on a continual basis as a no-cost service. As potential issues are identified, DHS notifies affected customers so they may proactively mitigate risks to their systems prior to exploitation. The service incentivizes modern security practices and enables participants to reduce their exposure to exploitable vulnerabilities, which decreases stakeholder risk while increasing the Nation's overall resiliency. Contact: nccicustomerservice@hq.dhs.gov.

- **Phishing Campaign Assessment (PCA)**: A six-week engagement that evaluates an organization's susceptibility and reaction to phishing emails. The results of a PCA are meant to provide

guidance, measure effectiveness, and justify resources needed to defend against spear-phishing and increase user training and awareness. Contact: nccicustomerservice@hq.dhs.gov.

- **Risk and Vulnerability Assessment (RVA)**: An offering that combines national threat and vulnerability information with data discovered and collected through onsite assessment activities to provide customers with actionable remediation recommendations prioritized by risk. Engagements are designed to determine whether and by what methods an adversary can defeat network security controls. Components of the assessment can include scenario-based network penetration testing, web application testing, social engineering testing, wireless testing, configuration reviews of servers and databases, and evaluation of an organization's detection and response capabilities. Contact: nccicustomerservice@hq.dhs.gov.
- **Threat and Vulnerability Information Sharing**: Funded by DHS to support election officials, the EI-ISAC provides early cyber threat warnings, vulnerability identification and mitigation, incident response, and education and outreach on best practices aimed at reducing cyber risk to state and local election infrastructure. To sign up, visit https://learn.cisecurity.org/ei-isac-registration.

APPENDIX: VENDOR SELECTION CONSIDERATIONS

The process of writing requirements, reviewing responses, and selecting technology and security vendors can be difficult. Often, vendor responses are highly technical and difficult to evaluate. It is recommended that IT staff be involved in the vendor selection process. However, local officials may not have technical IT staff available to them. State offices should work to provide some technical support to local offices if requested to aid in the creation of requests for purchase, review of responses, and selection of vendors. As mentioned above, several states are looking at spending money to deploy cyber navigators who could help with these types of purchasing decisions.

This Appendix is intended to provide information and suggestions for procurement processes. Some of the information may or may not apply to all systems or services that are being procured. It is recommended you review this information with procurement officials and IT officials to ensure it is consistent with the needs of your organization.

Below are a few recommendations for evaluative questions and considerations when selecting vendors:

- Consider using or referencing a GSA or state procurement schedule. GSA vets and maintains a list of vendors to meet a series of technical and security competencies. Many states have similar lists of state vendors that can be useful when evaluating possible vendors.
- In addition to these considerations, the GCC has developed the following series of questions which may be useful in discerning and differentiating between proposals.
    - What is the vendor's patch management and update process?
    - What assurances are in place for protecting data? When key vendor personnel leave or change positions, what is the procedure for removing their access to vendor data?
    - What intrusion detection measures does a vendor maintain for their systems?
    - What conditions will trigger vendor reporting of cyber incidents to purchasers?
    - What cybersecurity training does the vendor require of its staff and sub-contractors?
    - Does the vendor conduct background assessments of its personnel and sub-contractors?
    - What are the disclosure requirements within the contract with the vendor? Who, if anyone, can they report their findings or information to, beyond you as the primary purchaser?
    - Does the vendor have a cyber incident response plan? When was the last time it was exercised?
    - What other government clients does the vendor have? Can you have contact info for these clients?

Security Considerations When Contracting with Vendors

After reviewing security best practices across different critical infrastructure sectors, we suggest organizations consider requesting the following information or actions from vendors either during the vetting or contracting process. Organizations may seek that vendors:

Update Software

- Provide documentation detailing all applications, utilities, system services, scripts, configuration files, databases, and all other software required and the appropriate configurations, including

revisions and/or patch levels, for each of the systems associated with the election infrastructure procurement.

- Provide a listing of services required for any computer system running election system applications or required to interface with election system applications. Organizations can ask that the listings include all ports and services required for normal operation, as well as any other ports and services required for emergency operation. Additionally, organizations can require an explanation or cross reference to justify why each service is necessary for operation.
- Verify and provide documentation that all services are patched to current status.
- Provide, within a pre-negotiated period, appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.
- Remove and/or disable all software components that are not required for the operation and maintenance of the system and provide documentation on what is removed and/or disabled.
- Generate and provide an image of each system procured to be used later as a control baseline.
- Have a patch management and update process the includes:
    - Details on their patch management and update process, before a contract is awarded.
    - Identifying the responsibility for installation and update of patches.
    - Notification of patches affecting security within a pre-negotiated period as articulated in the patch management process. Organizations should ask that vendors apply, test, and validate the appropriate updates and/or workarounds on a baseline reference system before distribution.
    - Notification of known vulnerabilities affecting vendor-supplied or required operating systems, applications, and third-party software within a pre-negotiated period after public disclosure.
- Ensure that mitigation of vulnerabilities shall occur within a pre-negotiated time period.

Provide Access Controls

- Configure hosts so users have the least amount of access to files and accounts as is necessary for each role, and provide documentation of the configuration.
- Configure the necessary system services to operate at the lowest user privilege level possible for that service, and provide documentation of the configuration.
- Document when changing or disabling access to such files and functions has been completed.
- Disable, through software or physical disconnection, all unneeded communication ports and removable media drives, or provide engineered barriers, and provide documentation of the results.
- Password protect the BIOS from unauthorized changes unless it is not technically feasible, in which case document and provide mitigation measures.
- Provide a written list of all disabled or removed ports, drives, and other removable media devices.
- Recommend which accounts need to be active and those that can be disabled, removed, or modified.
    - Disable, remove, or modify all the identified accounts pursuant to the recommendation, if approved.

    - Disable or remove all default and guest accounts after awarding the contract.
- Configure the network devices to limit access to/from specific locations, where appropriate, and provide documentation of the configuration.
- Configure the system to allow the system administrators the ability to re-enable devices if the devices are disabled by software, and provide documentation of the configuration.
- Do not introduce any new accounts without explicit requirements to do so by the designated authorized individual.
- Do not permit user credentials to be transmitted in clear text.
- Provide the strongest encryption method commensurate with the technology platform and response time constraints.
- Do not allow multiple concurrent logins, applications to retain login information between sessions, any auto-fill functionality during login, or anonymous logins.
- Provide user account-based logout and timeout settings.
- Do not introduce any new session algorithms without explicit requirements to do so by the designated authorized individual.
- Vendors must provide a configurable account password management system that allows for selection of password length, frequency of change, setting of required password complexity, number of login attempts, inactive session logout, screen lock by application, and denial of repeated or recycled use of the same password. Two-factor authentication should be required for all high risk or value systems.
- Do not store passwords electronically or in vendor-supplied hardcopy documentation in clear text unless the media is physically protected.
- Control configuration interface access to the account management system.
- Provide a mechanism for rollback of security authentication policies during emergency system recovery or other abnormal operations, where system availability would be negatively impacted by normal security procedures.
- Establish a role-based access control scheme that is protected (e.g., encrypted). Only approved administrators, who are aware of how roles and permissions can affect the security of the control system, shall be allowed to change the scheme.
- Provide for user accounts with configurable access and permissions associated with the defined user role.
- Adhere to least privileged permission schemes for all user accounts, and application-to-application communications.
- Configure the system so that initiated communications start with the most privileged application controlling the communication. Upon failed communication, the most privileged side will restart communications.
- Verify that the master network device initiates communications. The vendor shall inform the purchaser if this condition cannot be met.
- Verify that a user cannot escalate privileges, under any circumstances, without logging into a higher-privileged role first.
- Provide a mechanism for changing user(s) role (e.g., group) associations.
- Provide documentation defining access and security permissions, user accounts, applications, and communication paths with associated roles.

Monitor Activity

- Provide a system whereby account activity is logged and is auditable both from a management (policy) and operational (account use activity) perspective.
- Time stamp, encrypt, and control access to audit trails and log files.
- Ensure audit logging does not adversely impact system performance requirements and provide read-only media for log creation.

Remediate Flaws

- Have and provide documentation of a written flaw remediation process.
- Provide appropriate software updates and/or workarounds to mitigate all vulnerabilities associated with the flaw within a pre-negotiated period.
- Ensure that after the vendor is made aware of or discovers any flaws, the vendor shall provide notification of such flaws affecting security of Vendor-supplied software within a pre-negotiated period. Notification shall include, but is not limited to, detailed documentation describing the flaw with security impact, root cause, corrective actions, etc.
- Provide a process for users to submit problem reports and remediation requests to be included in the system security. The process shall include tracking history and corrective action status reporting.
- Protect problem reports regarding security vulnerabilities from public discloser and notify Purchaser of all problems and remediation steps, regardless of origin of discovery of the problem.
- Inform the purchaser, in writing, of flaws within applications and operating systems in a timely fashion and provide corrective actions, fixes, or monitoring guidance for vulnerability exploits associated with the flaw.
- Disclose the existence of and reasons for any known or identified backdoor codes.