CISA
CYBER+INFRASTRUCTURE

Election Infrastructure Security Funding Considerations

by Election Infrastructure Subsector Government Coordinating Council

March 12, 2020

Executive Summary

In 2018, Congress provided $380 million in funding under the Help America Vote Act (HAVA) to state and local election officials for activities to improve the administration of elections for Federal office, including to enhance election technology and make election security improvements. State and local election officials are utilizing the funds to reduce risk in the election infrastructure and to build resiliency in the election process. Congress recently provided an additional $425 million in funding to continue those efforts.

Federal, state and local election organizations comprising the Election Infrastructure Subsector (EIS) Government Coordinating Council (GCC) have developed this document to provide suggestions for use of the investment for each of the following categories:

- **People** Ensuring election officials have access to election security staff with the necessary expertise to operationalize and install critical products, policies and practices is one of the best steps election officials can take to manage risk to their systems. Some states use a "cyber-navigator" program to provide IT assistance to local election offices that lack the resources to invest in the necessary staff.

- **Products** - In much of the country, the elections infrastructure is old and no longer supportable. In places without a paper artifact that can be audited officials are investing in new auditable voting systems. All election infrastructure should be supported and able to be patched.

- **Practices** – Good security practices to help protect, detect and recover from potential security incidents are critical to securing an election. These include robust auditing of the process, pre-election testing of all systems to be used in the election, incident response planning and exercising of those plans, and implementing strong access controls on all systems, ensuring only those who need access to the systems have that access and only the access they need to accomplish their job.

Since the HAVA grant funding is administered by the U.S. Election Assistance Commission (EAC), election officials are advised to consult with the EAC before making any purchase to ensure it is an appropriate expenditure of funds under the rules governing the grants.

The EIS GCC recommends state election officials consider the following recommendations related to people, products and practices when making decisions about how to invest the newly appropriated federal funds. We understand that many states have already implemented programs and practices or made purchases in line with the following recommendations. We recommend states focus on the areas where they have identified gaps and priority needs through their risk assessments.

PEOPLE

Provide Additional Human Support – "Cyber Navigators"

Some states already have, or are considering investing in, a "cyber navigator" or a cyber liaison program. These programs provide practical cybersecurity knowledge, support and services to local election officials who otherwise may not have access to them. These navigators can conduct assessments of local election offices, work with county IT staff or vendors to create cyber security policies, mitigate vulnerabilities discovered during the assessments, and establish cyber hygiene best 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 make them state election employees. Others use existing state personnel, such as the National Guard, or contractors as cyber navigators. Speak with colleagues to determine the methods that have worked well in the election ecosystem, but also fit the needs of your state.

Make Existing People Better – Training

Phishing Assessments: 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.

IT & Cybersecurity Awareness Training: Most incidents occur because of human error or lack of understanding of the systems that are in use. Regularly training staff on general cybersecurity awareness and best practices decreases the risk that the human element brings into the process. Providing additional training for users who have access to specific IT and election systems which covers how the system works, the vulnerabilities of the system, the security that is built into the system, and their responsibilities is important to ensuring system security.

Tabletop Exercises: We all play the way we practice. The more you prepare, train, and exercise your processes, the higher likelihood that you will perform at the highest level. Further, in times of pressure, we tend to be reactive, falling back on the processes and knowledge that have been ingrained in us. Putting your staff and election support through regular exercises facilitates good practices, reducing the likelihood of reacting to a situation incorrectly during a crisis. CISA now has a "Table Top in a Box"[1] product available. This product is designed to allow state and local officials to take specific scenarios, tailor them to their election environment and exercise their ability to respond to those scenarios.

Build a Management and Staffing Plan to Support Your Efforts

Collecting, analyzing and triaging data is vital to an operation to seek the highest performance in this environment. Identify what you will need to build an operations center that will work for your jurisdiction. Take the time, spend the money and effort, to determine what you will need, who you can partner with, and where the gaps are that need to be filled. Develop standard operating

[1] CISA: Elections Cyber Tabletop in a Box, https://www.cisa.gov/publication/elections-cyber-tabletop-box

procedures (SOPs) for the things that can be delegated out. All of this may require hiring more staff to help run a more efficient and secure election. In addition to people there are tools and resources that can be leveraged to assist you and your staff in this process. For example Harvard's Belfer Center recently released a "Battlestaff Bootcamp"[2] product designed to support election officials as they plan and implement their election operations center.

PRODUCTS

Voting Equipment

The use of any voting system without a paper backup is higher in risk than systems with paper records. Prioritizing this funding for the replacement of any remaining voting systems which lack an auditable paper record along with the implementation of regular audits will allow election officials and voters to have higher confidence that no undetected error in the voting system could change the result of the election.

Secure Voter Data

The integrity of voter data is paramount. Consider investing in tools to protect your voter registration database against erroneous changes, detect intrusions or unwanted modifications, and recover from any issues once detected. Protecting voter data requires implementing safeguards on multiple systems including any system utilized in the process of determining voter eligibility, such as voter registration systems and electronic poll books, as well as the systems used for distributing files, such as an sFTP for transferring voter files to the poll book printer or for distributing them to parties, campaigns, educational institutions, media, etc.

Although integrity is of the utmost importance, protecting the confidentiality and availability of voter data is additionally important. Consider investing in tools that limit the release of sensitive data, such as encryption for data in transit and at rest. Investment in tools which help maintain the availability of the data so that it does not get held for ransom or be made unusable through a denial of service (DoS) attack is critical. This can be done in a couple different ways:

1) Investment in regular backups (both online and offline) of critical systems' data (like voter registration data) and software. Having a backup or access to all critical software is just as important as having backups of the data themselves. Ransomware can lock up an entire system, including the software, so to recover, you must have copies of all the critical software and data. Also, make sure to test all those backups to ensure you can recover from possible ransomware or other attacks intended to destroy or alter data.

2) Distributed Denial of Service (DDOS) protections. There are many products that can limit the impact of a DDOS attack particularly for your most utilized and visible internet connected webpages such as polling place lookup, online voter registration portal, election night reporting website, etc. There are private sector companies that provide both detection and prevention capability from DDOS attack. Some of these companies are making these products available for

[2] Harvard Kennedy School, Belfer Center for Science and International Affairs: Elections Battle Staff Playbook, https://www.belfercenter.org/publication/elections-battle-staff-playbook

free to election jurisdictions. In addition, election officials should invest in rollover capability for any important websites. Beyond having a rollover site, election offices should plan and invest in additional avenues to share the information on their website, such as participating in the Voting Information Project (VIP) for voter lookup or implementing other channels for reporting election night results like Twitter or local media partnerships.

Update Operating Systems & Software

Whether it's your computer, smartphone, or other network devices, the best defense against viruses and malware is to update to the latest security software, web browsers, and operating systems.

Prioritize upgrading all your systems, not just election systems, to technology that is running on the most current, secure, operating system available.[3] Many election systems or back office systems are running on a Windows 7 or older operating system, which is no longer supported by Microsoft. If your systems are still running an unsupported version of Windows (Windows 7 or older) and you cannot upgrade for some reason, purchase Microsoft extended service.

Incident Tracking Systems & Software

As described in the Belfer Center Elections Battle Staff Playbook, "Incident tracking allows leaders to remain informed about conditions on the ground and provides visibility of their teams' responses to issues being faced in the field. In addition to the real-time benefits to empower informed decision-making, these systems also help improve future opera-tional performance by using the information to identify areas that need more attention before the next voting period."[4]

Find a solution that allows you to track incidents, assign criticality levels, and visualize the data in a way that allows you to efficiently and effectively make informed decisions and identify trends: filtering by criticality or type, understand what issues remain open at any given time, map/geolocate where incidents are occurring, etc. Also, if you have a way to easily export an incident, it can facilitate efficient communications with state, federal and private sector partners who can support. For instance, if an election worker reports a voting machine needing replacement at a specific precinct, you can export the information into an email and send it directly to the rover with all the necessary information for her/him to respond.

Multi-Factor Authentication Products

Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know, like a password or PIN; (ii) something you have, like a cryptographic identification device, token, phone with text, or authenticator application; or (iii) something you are (e.g. fingerprints, biometrics, etc.). Upgrading voter registration systems, election night

---

[3] In September 2019, Microsoft announced it will support Windows 7 for voting systems through 2020, but this does not apply to any other election or business processing systems. (https://blogs.microsoft.com/on-the-issues/2019/09/20/extending-free-windows-7-security-updates-to-voting-systems/)

[4] (Ibid. p. 2)

reporting systems, or other election office IT systems to use multi-factor authentication can drastically limit the risks of phishing attacks.

Password Management Software

Use password managers to generate and remember different, complex passwords for each of your accounts. Some password managers are offering free service for election officials in perpetuity. Ensuring that passwords used for election systems are changed after each election by using a password manager or other management product is critical to limiting the risks posed to these systems.

PRACTICES

Audit the Entire Election Process

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 voting equipment, post-election tabulation auditing has become a common practice for many election jurisdictions. Hiring additional temporary staff to help with the audit is an effective way to lessen the burden on under-staffed election offices while improving the overall resilience of the process. In addition, states considering implementing risk-limiting audits (RLAs) can improve the quality and efficiency of the audit by investing in RLA software to assist with the process. CISA recently invested in the development of a free open-source auditing tool[5] that can be used by any election jurisdiction that is interested.

Looking beyond tabulation audits, consider policies that include regular audits of the voter registration system for anomalies and correct district assignments, robust, pre-election testing of voting equipment, reconciliation and chain of custody audits, and regular security audits. This can be done using a third-party to audit the security of your technology and the quality of your policies and practices. Consider investing in tools that can assist with internal audits such as tools to track ballots and voting equipment for chain of custody and tools for analyzing changes to your voter registration system.

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 and vulnerabilities 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 days of detection.

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 and implement practices that ensure timely deployment

[5] Voting Works: Arlo, https://github.com/votingworks/arlo

of those patches.

Network Architecture and Cybersecurity Assessment

Defensibility begins with an understanding of what systems and data you are defending. Having a full accounting of the 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 can be a critical starting point for risk mitigation decisions. Know which systems are connected to which networks and understand who to rely upon for making changes.

Access control practices, providing access to data or systems to only those who need it and limiting access to only what they need to do their job, can 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 and other attacks that use trusted access to systems.

Network Segmentation and Air-Gapping

Air-gapping and network segmentation can limit, but not eliminate, the exposure of vulnerable systems to compromise. A third-party assessment or audit of security processes and procedures to include air gapping and network segmentation can help identify weaknesses like the use of contaminated media or insecure vendor practices.

In order to maintain an air-gap it is essential to make sure that all forms of data transfer are performed using best practices. This may require the use of write-once, use-once external media, but it may also include the use of hardware and software to block non-approved external media and/or software.

APPENDIX 1: Free Resources from CISA and EI-ISAC

To make best use of these limited funds, consider using existing, no-cost resources where available and appropriate while applying these funds to people, products, and practices that fill gaps or supplement no-cost products and services. Below is a short list of some of the free services being offered by or through CISA.

For a full catalog of services that CISA offers, visit https://www.cisa.gov/election-security.

EI-ISAC

Funded by CISA and operated by the Center for Internet Security, Inc. (CIS), the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)[6], as established by the Election Infrastructure Subsector Government Coordinating Council (GCC), is a critical resource for cyber threat prevention, protection, response and recovery for the nation's state, local, territorial, and tribal (SLTT) election offices.

The mission of the EI-ISAC is to improve the overall cybersecurity posture of SLTT election offices through collaboration and information sharing among members, the U.S. Department of Homeland Security (DHS) and other federal partners, and private sector partners are the keys to success. The EI-ISAC provides a central resource for gathering information on cyber threats to election infrastructure and two-way sharing of information between and among public and private sectors in order to identify, protect, detect, respond and recover from attacks on public and private election infrastructure.

The EI-ISAC provides an election-focused cyber defense suite through its 24-hour watch and warning center, real-time network monitoring, dissemination of early cyber threat warnings, vulnerability identification and mitigation, along with education and outreach aimed at reducing risk to the nation's SLTT election cyber domain.

Threat and Vulnerability Information Sharing

Funded by CISA 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.

Cyber Situational Awareness Room

As part of EI-ISAC membership, on Election Day, CISA provides a platform for election officials to share information, incidents, and issues of concern with their colleagues, vendors, and federal government via a live chat room. Any member who is logged in may see what is being shared by their colleagues to understand what they are experiencing within their jurisdiction. Many times, what may seem like an isolated incident in your jurisdiction may be something more systemic. By sharing your experience, you can get feedback from your colleagues that may have experienced similar issues, but you may also provide them information that will prevent them from experiencing a similar issue. Additionally, if something erroneous is trending in the media, social or

[6] EI-ISAC, https://www.cisecurity.org/ei-isac/

traditional, CISA can assist by working with the companies, campaigns, candidates, or other non-governmental entities to quickly dispel the information and/or get the correct information out to your voters.

Vulnerability Scanning

Scanning of internet-accessible systems for known vulnerabilities on a continual basis as a no-cost service. As potential issues are identified, CISA 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 resilience. Contact: cisacustomerservice@hq.dhs.gov.

Remote Penetration Testing

Remote Penetration Testing (RPT) uses a dedicated remote team to assess, identify, and mitigate vulnerabilities to exploitable pathways into networks or election systems. While similar to a Risk and Vulnerability Assessment, an RPT focuses entirely on externally accessible systems.

After completing RPT, the organization receives a final report with recommendations for executive-level personnel, specific findings, potential mitigations, and technical attack path details. An optional debrief presentation summarizing preliminary findings and observations can be provided upon request. Contact: cisacustomerservice@hq.dhs.gov.

Phishing Campaign Assessment

The Phishing Campaign Assessment (PCA) evaluates an organization's susceptibility and reaction to phishing emails of varying complexity.

After the assessment, the organization will receive a Phishing Campaign Assessment Report that highlights organizational click rates for varying types of phishing emails and summarizes metrics related to the proclivity of the organization to fall victim to phishing attacks.

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: cisacustomerservice@hq.dhs.gov.

IT & Cybersecurity Awareness Training

The Federal Virtual Training Environment (FedVTE) is a free, online, on-demand cybersecurity training system managed by CISA that is available to federal and SLTT government personnel, veterans, and federal government contractors. It also includes the *Election Officials as an IT Manager* training, which is an election specific IT & cybersecurity awareness training that CISA worked with EAC to provide online and provides in-person. For more information, visit https://fedvte.usalearning.gov/.

Tabletop Exercises

CISA provides cyber exercise and incident response planning to support election infrastructure partners. There is a full spectrum of cyber exercise planning workshops and seminars. It also conducts full-scale, and functional tabletop exercises. These events are designed to assist

organizations at all levels in the development and testing of cybersecurity prevention, protection, mitigation, and response capabilities. For instance, CISA's "Table Top in a Box" product helps facilitate state and local election officials develop their own exercises. For information from CISA on planning an exercise, contact CISA.Exercises@cisa.dhs.gov.

Risk and Vulnerability Assessments

A Risk and Vulnerability Assessment (RVA) collects data through onsite assessments and combines it with national threat and vulnerability information in order to provide an organization with actionable remediation recommendations prioritized by risk. This assessment is designed to identify vulnerabilities that adversaries could potentially exploit to compromise network security controls.

After completing the Risk and Vulnerability Assessment, the organization will receive a final report that includes recommendations for decision makers to consider, specific findings and potential mitigations, as well as technical attack path details. Contact: cisacustomerservice@hq.dhs.gov.

Critical Product Evaluation

The Critical Product Evaluation (CPE) is a cybersecurity evaluation used to improve national resiliency of our critical infrastructure. It is a multi-week, comprehensive cybersecurity evaluation of an election system; typically, one that is provided by a third-party vendor. The CPE is most valuable when your vendor submits its election system, specifically a voting system, electronic pollbook, remote voting solutions, or election night reporting system, so that each jurisdiction does not have to pay to have their system evaluated.