Frank LaRose
Ohio Secretary of State

DIRECTIVE 2022-38
June 28, 2022

To: All County Boards of Elections
Board Members, Directors, and Deputy Directors

Re: Help America Vote Act ("HAVA") Funds, Security Improvements, and Vendor Contracts

SUMMARY

As election officials, it is our duty to protect the security and integrity of Ohio's elections. Threats to our election infrastructure continue to demand our attention and diligence. Each security directive is built on a foundation of cybersecurity best practices that will help boards of elections improve their cybersecurity programs. This Directive provides boards of elections with the opportunity to continue to strengthen the security of Ohio's election systems. The Directive instructs county boards of elections on continuing security steps and outlines additional requirements that each board must take to enhance its overall election security and protect its information technology ("IT") systems. All items in this Directive must be completed by **December 30, 2022,** unless otherwise specified.

This Directive builds on the foundation of cybersecurity requirements set forth in Security Directives 2020-12 and 2019-08, which were incorporated into Chapter 3 of the Election Official Manual (Directive 2022-07). Each county board of elections must immediately share this Directive and the accompanying Technical Document with its technical point of contact.

HAVA funds are available this year for improving election security. Each county board of elections can receive up to $10,000 to support the implementation of this Directive.

INSTRUCTIONS

I. 2022 HAVA SECURITY FUNDING

Each board of elections may receive up to $10,000 for the implementation of requirements in this Directive. This funding will be referred to in this Directive and future communications as the 2022 HAVA Security Funding. The funds are available only for purposes contained within this Directive.

Boards of elections must enter into a grant agreement with the Secretary of State's Office and will be sent a check for $10,000 upon the Office's receipt of the board of elections' signed agreement. Boards of elections must deposit the grant payments into an interest-bearing fund, separate from all other funds of the board and may use the same fund that was set up for the 2019 or 2020 HAVA grants. Prior to expending any grant funds, boards of elections must complete the following:

(1) Submit a plan identifying how they intend to meet the Directive requirements;
(2) Provide an estimate of the associated costs to HAVAGrant@OhioSoS.gov; and
(3) Receive approval of the plan.

The Technical Document accompanying this Directive provides additional instructions for submitting a plan for the grant. In addition, boards must submit two types of reports after their 2022 HAVA Security Funding plan is approved:

- **Expenditure Report:** On the first business day of September 2022 and on the first business day of January 2023, the board of elections must submit the HAVA 2022 Expense Report and all associated quotes, quote templates, receipts, invoices, and proofs of payment to BOE - SecurityDirectives - All Documents (sharepoint.com).
- **Implementation Progress Report:** On the first business day of each month, the board of elections must submit the HAVA 2022 Security Directive Implementation Progress Report to BOE - SecurityDirectives - All Documents (sharepoint.com)using the Excel templates provided.

Unspent HAVA Security Funding must be returned to the Secretary of State's Office by **February 2, 2023**.

Boards of elections must follow all state and county laws and purchasing rules when making purchases to implement this Directive. Boards must obtain three quotes from vendors offering required items or services that cost $1,000 or more. If fewer than three vendors offer the required item or service, a board must certify that fact to the Secretary of State's Office. Boards are encouraged to use the state term schedules to identify a vendor offering a competitive price for items and services; however, if the board selects a vendor on state term schedules, the board must still provide three quotes. The schedule is available here: https://procure.ohio.gov/bidders-and-suppliers/resources/04_ob+contracts.

II. DEPARTMENT OF HOMELAND SECURITY ("DHS") SERVICES

As a result of the DHS designation of election infrastructure as critical infrastructure, election officials can take advantage of a full menu of free DHS services. Election officials can obtain information on these resources and services by contacting DHS at: CISAServiceDesk@cisa.dhs.gov.

The Secretary of State's Office enrolled each board of elections domain in the DHS Crossfeed service. This service scans web applications and underlying infrastructure for known vulnerabilities and compiles it into a single dashboard. This service is only for public infrastructure; however, the dashboard is publicly available on the internet. More information about this service can be found at Crossfeed | CISA.

Each board of elections must continue *to request* the following services no later than **July 15, 2022**. Requests for these services should be emailed to CISAServiceDesk@cisa.dhs.gov, copying HAVAGrant@OhioSoS.gov.

A. Phishing Campaign Assessment. This assessment is a "no cost six-week engagement that evaluates an organization's susceptibility and reaction to phishing emails of varying complexity." Each board of elections must use this service **annually**. While

required for the boards of elections to utilize this service, the entire county should take advantage of this no-cost service.

B. **Cyber Hygiene (Vulnerability Scan)**. This service provides "vulnerability scanning of Internet-accessible systems for known vulnerabilities on a continual basis as a no-cost service. As potential issues are identified, DHS notifies impacted 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." Each county board of elections must use this service **weekly**, and the board must have DHS include the Ohio Secretary of State's Office and EI-ISAC as recipients of the weekly report. While required for the boards of elections to utilize this service, the entire county should take advantage of this no-cost service.

Each board of elections must request all the following additional services prior to the general election in even-numbered years if it has not done so already. These services must be requested no later than **July 15, 2022**.

C. **Risk and Vulnerability Assessment**. This onsite assessment gathers data and combines it with national threat and vulnerability information to detect vulnerabilities in network security. After completing the assessment, DHS provides a final report with its findings and recommendations for improving network security controls.

D. **Remote Penetration Testing**. DHS provides this service remotely to identify vulnerabilities in externally accessible systems. After completing testing, DHS provides a final report with its findings and recommendations.

E. **Validated Architectural Design Review**. This review is designed to develop a detailed representation of the communications and relationships between devices to identify anomalous communication flows. Following the review, a participating organization will receive a report that includes discoveries and recommendations for improving organizational operations and cybersecurity.

F. **Cyber Threat Hunt**. DHS will perform an in-depth review on site at the board of elections to determine if a network compromise has occurred.

The Secretary of State's Office highly recommends that the entire county government take advantage of these no-cost services.

III. CONTINUATION OF BOARD RESPONSIBILITIES

A. ELECTIONS INFRASTRUCTURE INFORMATION SHARING

Each board must review its personnel information with the Elections Infrastructure Information Sharing and Analysis Center ("EI-ISAC") and make any necessary updates to ensure that the appropriate personnel receive and review emails. New board and staff members must register at https://learn.cisecurity.org/ei-isac-registration, and boards must notify the EI-ISAC of contact information changes via email to elections@cisecurity.org .

B. CYBERSECURITY TRAINING

As stated in Chapter 3 of the Election Official Manual, each board member and employee must complete an approved security awareness training course annually and whenever a new board member or employee starts with the board of elections.[1] A copy of the certificate of completion or a report from the training system must be provided to the Secretary of State's Office within 30 days of completion. If the board of elections does not have security awareness training available to them, the Secretary of State's Office will provide it at no cost to the boards of elections. The training must be completed within 90 days of the individual training courses being assigned.

IV. CONTINUATION OF SERVICES

This section of the Directive outlines the services that the Secretary of State's Office will continue to provide in order to support Ohio's secure elections infrastructure.

A. CYBER LIAISONS

The Secretary of State's Office engaged cybersecurity professionals to assist the county boards of elections with their IT support needs. Currently there is a cyber liaison deployed to each region of Ohio: Northeast, Northwest, Southeast, and Southwest. The cybersecurity liaisons promote best practices to further improve the board's cybersecurity and complement the board's current IT support. For example, cyber liaisons assist boards and local IT support with tools, software or hardware integration, software and patch management support, network analysis review, incident response planning and exercising, tier one incident management forensic collection support, and general engineering technical assistance.

B. NETWORK INTRUSION DETECTION

Boards of elections must continue using the Albert Intrusion Detection Monitoring service. The Albert must be configured to monitor the board of elections' network traffic and may also be used to monitor the overall county network traffic so long as the board of elections' network traffic is included in that monitoring.

C. SECURITY INFORMATION AND EVENT MANAGEMENT ("SIEM")

Boards of elections must continue using the SIEM Logging service. All boards of elections network systems must be configured to log system events to the SIEM. Other county log events

[1] Chapter 3, page 68 of the Election Official Manual.

may also be sent to the SIEM, so long as the board of elections system events are continuously monitored.

D. ENDPOINT DETECTION AND RESPONSE ("EDR") SOLUTION

Boards of elections must continue to use the EDR Solution provided by the Secretary of State's Office. EDR solutions protect systems more effectively than the traditional anti-virus products by scanning for known bad behavior and characteristics of malicious actors, rather than looking only for bad files like traditional anti-virus software.

If the board of elections is unable to implement the Secretary of State's supplied EDR, the board must document how their current EDR solution meets the Secretary of State's requirements.

E. MALICIOUS DOMAIN BLOCKING AND REPORTING

The Secretary of State continues to provide a malicious domain blocking and reporting service ("MDBR") for all county boards of elections. This service blocks access to malicious websites, helps stop malware from connecting to known command-and-control infrastructure, and complements the ALBERT and SIEM services. Each board of elections must maintain the service and continue using this malicious domain blocking service or an approved equivalent. While the boards of elections must utilize this service, the entire county is encouraged to take advantage of this service at no cost.

V. CYBER CONTROLS

The Center for Internet Security ("CIS") publishes a list of critical security controls. These controls are a prioritized set of actions that form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. This framework serves as the guiding principles for cybersecurity practices. This section of the Directive focuses on enhancing the boards of elections' implementation of these controls so they may better adapt and respond to the changing threat landscape. Additional information can be found at CIS Critical Security Controls (cisecurity.org).

A. WEEKLY VULNERABILITY SCANNING

Security Directive 2019-08 and Chapter 3 of the Election Official Manual mandates boards to conduct unauthenticated vulnerability scans. This Directive requires boards to transition to authenticated vulnerability scans.

Each board of elections must conduct authenticated vulnerability scans at least once a week. This capability is available through the services provided by the Ohio Secretary of State's Office, and the cyber liaisons will configure the SIEM solution for authenticated vulnerability scanning at no cost to the board of elections. Boards must retain evidence that these scans are completed and acted upon for at least one year.

B. ASSET MANAGEMENT

Each board of elections must use data from an authenticated vulnerability scan to regularly update an asset management database. This capability is available at no additional cost to the board

of elections through the current SIEM solution and will be configured with the support of the Secretary of State Cyber liaisons.

C. SOFTWARE MANAGEMENT

Each board of elections must have the ability to track new software installed on each asset deployed within the agency. The technical point of contact will be responsible for tracking, maintaining, and updating authorized software on a regular basis. Directors and Deputy Directors must work with their technical point of contact to establish processes to determine if new software is safe for internal use and to ensure software is supported by the vendor(s).

D. REMOTE ACCESS MANAGEMENT

Access to board of elections systems that traverse an external network, such as the Internet, must be monitored and protected. All remote access must meet the following requirements:

- Connections must be logged locally and to the SIEM.
- Sessions must be protected using an encryption algorithm approved in FIPS 140-2.

E. USER ACCOUNTS

In order to increase security, a board of elections must change user passwords at least every 90 days and **immediately** if there is a suspected account compromise. Passwords must comply with the security and complexity standards in Chapter 3 of the Election Official Manual and must not be re-used across different applications.

Boards must maintain secure custody for passwords and log-in information for its voter registration system, voting systems, and central tabulating systems. The board must not maintain passwords on a document that can be accessed by anyone but authorized staff. This means that the posting of a password or even part of a password on a monitor or keyboard is strictly prohibited. If the board finds it necessary to physically document passwords associated with any of its systems, the document must be under double lock and key, controlled only by bipartisan staff when not in use.[2]

F. ADMINISTRATOR ACCOUNTS

Each board of elections must review user accounts on all critical systems utilized by the agency on a quarterly basis. An administrative account is a user account with full privileges intended for use only when performing personal computer management tasks, such as installing updates and application software, managing user accounts, and modifying operating system and application settings. Privileges must be adjusted accordingly after each review, with overprivileged users losing access and unneeded accounts deactivated when necessary.

Administrative accounts must be separate from an account that is utilized for duties such as sending emails, utilizing the internet, and processing voter registrations. Boards of elections must work with their technical point of contact to ensure that any employee with an administrative

[2] Chapter 3, pages 59-61 of the Election Official Manual.

account only has access to those systems that are necessary to their role at the board. Boards are required to review administrative account access at least once a year and whenever there is a change in personnel with administrative account access.

G. SERVICE ACCOUNTS

Service accounts run automated processes and are used by applications, not people (for example, automated system backups). Service account passwords are a common vector threat that actors use to laterally move through an organization because of poor cyber hygiene. The accounts traditionally are unmonitored and may not follow the same password requirements outlined for administrator accounts and user accounts. To reduce the risk of hacking, service accounts must have passwords that expire at least annually.

H. OFFICIAL COUNTY GOVERNMENT WEBSITE BANNER

Building upon the transition to ".gov" websites, it is important to inform the public on how to identify trusted sources of information. Each board of elections must include a website banner that explains how to quickly identify a site as secure and an official county government site. Refer to the Technical Document for an example and go to the following website for instructions on how to include the banner: https://designsystem.digital.gov/components/banner/.

VI. SOFTWARE AND HARDWARE LIFE CYCLE MANAGEMENT

Boards of elections must monitor vendor website for system life cycle timelines and ask about the software or hardware life cycle before making a purchase. Additionally, it is important for boards to plan for aging systems from a budgetary perspective to prevent a situation where an unsupported system is deployed in the organization. Prior to an election, boards must ensure that no equipment or software is past end of life support. Boards can utilize their asset management inventory to track the board's equipment and software with purchase dates to continuously monitor for upcoming budget needs. supply chain, vendor management, and contracts.

A. VENDOR CONTRACTS

Vendor relationships are an important area where security risk mitigation needs to occur. In 2020 and 2021, there were several prominent cyber events that showed the importance of ensuring entities are aware of the risk a vendor poses to their operations. Reflecting on these events, the Secretary of State's Office intends to ensure boards of elections are doing everything they can to protect themselves and account for vendor risk.

Board of elections must work with their statutory legal counsel, the county prosecutor, to include cybersecurity-related terms and conditions in all new contracts and upon renewal of contracts involving voter registration systems, electronic pollbooks, ballot on demand services, voting machines and systems, and information technology services (collectively, "technology services contracts"). Specifically, technology services contracts should include language to ensure that the vendor will comply with the security standards in the Ohio Secretary of State's Security Directives and the Election Official Manual. This should be in the form of a Security Supplement or a substantially similar addition to the main contract. A template for such terms and conditions

accompanies this Directive. Boards must involve their legal counsel, the county prosecutor, and technical points of contact in reviewing and negotiating technology services contracts.

The Security Supplement template includes standard cybersecurity related terms for boards and vendors to include in technology services contracts, not all of which will apply to every technology services contract. However, a strict prohibition on Products from Foreign Vendors Banned by the Federal Government applies to all contracts. A more detailed explanation of the Security Supplement is available in the Technical Document accompanying this Directive. At a high level, the Security Supplement includes provisions for all of the following:

- Data Protection;
- Network Protection;
- Vulnerability Management and Application Security;
- Access Control;
- Secure Channels for Remote Access;
- Strong Passwords and Multi-Factor Authentication (MFA);
- Incident Response Plan;
- Supply Chain Risk;
- Prohibition on Products from Foreign Vendors Banned by the Federal Government
- Software Bill of Materials; and
- Incident Reporting.

VII. CONTINUITY OF OPERATIONS AND INCIDENT RESPONSE

Each board of elections is required to maintain and exercise their continuity of operations and incident response plans. The continuity of operations plan is the playbook an organization follows during an event in which the current location cannot operate its business function, e.g., elections and voter registration. The incident response plan is the process for how the organization deals with specific events such as ransomware, phishing, or insider threats, but should not be limited to cybersecurity-related events.

Moving forward, boards are required to exercise these plans on an annual basis by conducting a tabletop exercise. Tabletop exercises are an effective way to apply incident response to emergency scenarios before they occur. A tabletop exercise should always conclude with an after-action review to ensure lessons learned from the event can be integrated into the existing plans. Your cyber liaison can assist in advising on how to create a tabletop exercise related to cybersecurity.

Boards of elections must submit an updated copy of their Incident Response and Continuity of Operation Plans to the Secretary of State's Office at HAVAGrant@OhioSoS.gov by **December 30, 2022**. Once complete, boards must include their Incident Response Plan in their Election Administration Plan for future reference.

VIII. VOTER REGISTRATION SERVER AND CRITICAL SYSTEM BACKUPS

The board of elections voter registration server and any data processed by the board of elections must be backed up on a daily basis. Other critical systems, such as file servers, must be backed up at least once a week. These backups must be stored in a secure off-site location. Backups can be run more frequently and stored in the cloud as long as the cloud provider is a U.S. based service and the data does not leave the United States. Boards must retain copies of backups for at least three weeks. At a minimum, boards must annually test the backup to ensure that the voter registration server and other critical systems can be fully restored using the off-site backup.[3]

IX. PHYSICAL SECURITY CONTROLS

Physical security of IT systems is essential to maintaining the confidentiality, integrity, and availability of data. Risks, such as damage from fire or water and unauthorized physical access to IT systems, must be reduced whenever possible. This section of the Directive identifies the minimum level of physical security that must be in place to protect voting equipment, voting systems, and other IT systems used or managed by the Ohio Secretary of State's Office and boards of elections.

A. ACCESS SECURITY

Boards of elections are required to secure the voter registration server, Albert server, SIEM server, network equipment, and any other related election equipment (other than individual workstations) in a locked room at all times. The room must only be accessible to authorized personnel. Any access to the secure room must be logged.

B. VIDEO SURVEILLANCE

Boards of elections are required to have video cameras that monitor IT and elections equipment, including all of the following:

- Network Racks;
- Network equipment;
- Voter registration server;
- Albert server;
- SIEM;
- Election Management System/Tabulators ("EMS"); and
- Electronic Pollbook Storage Locations.

C. LOCATION AND ENVIRONMENT

Any room containing voting equipment, voting systems, and other IT systems must be free of water and reasonably safe from flooding. Any room housing voting equipment, voting systems, and other IT systems must have fire suppression capabilities and a fire alerting mechanism, such

[3] Chapter 3, page 64 of the Election Official Manual

as a smoke detector. If the building does not have integrated fire suppression, at a minimum there must be a fire extinguisher within ten feet of the location.

Wherever possible, any room containing voting equipment, voting systems, and other IT systems must have environmental controls to regulate temperature. If room humidity can be regulated, it should be maintained between 45 percent and 60 percent relative humidity.

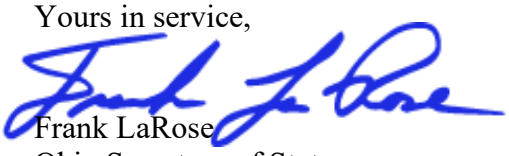
D. POWER SOURCES

Boards of elections must protect power equipment and cabling to prevent accidental damage, disruption, and physical tampering of electrical power to elections infrastructure. To reduce the risk, boards must take the following precautions:

- Place uninterruptible power sources, generators, portable power sources, and internal power cabling in locked cabinets or rooms;
- Employ automatic voltage controls (voltage regulators, voltage conditioners, and voltage stabilizers) where electrical supply frequently fluctuates or is unreliable;
- Employ surge protection on all server and network equipment;
- Have the capability to shut off power to server and network infrastructure in emergency situations; and
- For facilities equipped with a generator, have sufficient uninterruptable power supply ("UPS") capacity to maintain critical systems for the time it takes the generator to supply backup power.

If you have any questions regarding this Directive, please contact the Secretary of State's Elections Counsel at (614) 728-8789 or the cyber liaison assigned to your county.

Yours in service,



Frank LaRose
Ohio Secretary of State