Frank LaRose
Ohio Secretary of State

DIRECTIVE 2023-16
August 28, 2023

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

Re: Elections Security

SUMMARY

Beginning in 2019, this office prepared and issued security directives to establish standards for vendors, strengthen physical security requirements, and modernize cybersecurity capabilities to ensure safe elections and continue Ohioans' confidence in our democratic process. What began as a pilot project has now been successfully deployed in all of Ohio's 88 county boards of elections.

Over the past several years, each of you have risen to this challenge and continued to work at a peak level of efficiency to secure our election systems in every community across the state. When it comes to election integrity and legal responsibility, we have worked hard together to establish a national reputation for election security excellence and positioned Ohio as the gold standard state.

This work is ongoing because the threats change daily. Building off the success of previous directives, we continue to prioritize cybersecurity while making sure you have the support and tools needed to ensure you are prepared for 2024. We are excited to collaborate and further strengthen our partnership to serve Ohioans. The below multi-faceted security strategy will help provide the redundancy required for a strong election system infrastructure.

This Security Directive (2023-16) includes, but is not limited to, the following information:

- Grant funding to support the implementation of this Security Directive;
- An update on required Department of Homeland Security resources;
- Registration for Elections Infrastructure Information Sharing ("EI-ISAC");
- No-cost vulnerability disclosure program services;
- Reminders of ongoing board responsibilities and training opportunities;
- Reminders of continued secretary of state services to assist counties;
- Incident response planning and reporting; and
- Critical system supports and backup instructions.

Each county board of elections must share the Security Directive and the accompanying Technical Document with its Technical Point of Contact. All requirements in this Directive must be completed by December 29, 2023, unless otherwise specified.

GRANT FUNDING

The Secretary of State's Office will provide funding up to $10,000 to each county board of elections that requires assistance implementing this Security Directive. This funding will be referred to in this Directive and future communications as the 2023 Help America Vote Act ("HAVA") Security Funding.

Boards of elections must submit a Request for HAVA Grant Funding form ("Grant Request Form") and enter into an Elections Security Grant Agreement ("Grant Agreement") with the Secretary of State's Office in order to receive the funding. The Grant Request Form must be submitted by September 29, 2023, and include a list of the associated requirements, equipment or services, and estimated costs for which the funding will be used to implement this Security Directive.

A signed Grant Agreement must be returned to the Secretary of State's Office on or before October 13, 2023. Once the Secretary of State's Office receives a signed Grant Agreement, the board will be issued a check in the amount requested. These grant funds must be deposited into an interest-bearing fund separate from all other funds of the Board. The board of elections may use the same fund that was set up for the 2019, 2020, or 2022 HAVA grants.

Boards of elections must follow all current federal, state, and county laws and purchasing rules when making purchases to implement this Directive. Boards must obtain three quotes from vendors for any item, service, or total purchase that is estimated to 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 that is 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://ohiobuys.ohio.gov/page.aspx/en/ctr/contract_browse_public

INSTRUCTIONS

I. 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 many free DHS services. Election officials can obtain information on these resources and services by contacting DHS at: CISAServiceDesk@cisa.dhs.gov.

Each board of elections must continue *to use* the Cyber Hygiene Vulnerability Scanning Service from DHS. 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 board of elections must enroll in the following services when an invitation from DHS is received:

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."

B. **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.

C. **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.

D. **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.

E. **Web Application Scanning**. This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations.

II. 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 at the board of elections and/or county IT 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.

III. VULNERABILITY DISCLOSURE PROGRAM

A Vulnerability Disclosure Program ("VDP") is a formalized process to receive, validate, remediate, and communicate vulnerability information identified by security researchers on specific technology systems. VDPs have proven successful in many industries, from the largest tech companies to small governments. They can be an effective and efficient way for an organization to improve its security posture.

The EI-ISAC offers a vulnerability disclosure program to all boards. It is highly recommended that all boards take advantage of this no-cost service. For additional information please email elections@cisecurity.org and copy dlessard@ohiosos.gov.

IV. CONTINUATION OF BOARD RESPONSIBILITIES

A. 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 October 6, 2023.

B. CRIMINAL BACKGROUND CHECKS

As stated in Chapter 3 of the Election Official Manual, all permanent board of elections employees and vendors or contractors that perform sensitive services for the board of elections are required to have an Ohio Attorney General's Bureau of Criminal Investigation ("BCI") statewide criminal background check conducted[2], at a minimum, every ten years.

"Sensitive services" means those services that (i) require access to customer/consumer/agency employee information, (ii) relate to the board of election or Secretary of State's computer networks, information systems, databases, or secure facilities under circumstances that would permit modifications to such systems, or (iii) involve unsupervised access to secure facilities ("sensitive services").

Vendors and contractors may be required to pay for any background check services or may attest that a background check has been completed, and that no ineligible criminal offenses have been committed.

---

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

Each board must have a policy that sets forth the procedures for reviewing background checks and determining whether any convictions should bar employment.

V. 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 are cyber liaisons 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 ("Albert"). 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 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.

VI. 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 Security 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. CONTINUOUS VULNERABILITY MANAGEMENT

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. Boards must retain evidence that these scans are completed and acted upon for at least one year.

Boards of elections must remediate vulnerabilities in network-connected systems in a timely manner. Critical and high vulnerabilities must be remediated within 15 calendar days of initial detection; all other vulnerabilities must be remediated within 30 calendar days of initial detection. In order to meet the specified timelines, boards of elections are encouraged to utilize a patch management solution.

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.

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 also comply with the security and complexity standards in Chapter 3 of the Election Official Manual and must not be reused 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 other than 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.[3]

F. ADMINISTRATOR ACCOUNTS

Each board of elections must review user accounts on all systems utilized by the agency on a quarterly basis and upon change in personnel with administrator account access. 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 account only has access to those systems that are necessary to their role at the board.

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

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 threat vector 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. BOARDS OF ELECTIONS' WEBSITES

Each board of elections and their vendors must continue to utilize TLS/SSL certificates for any publicly facing or internal web-based applications (e.g., the county board of elections website) and ensure that its existing certificates do not expire.

All board of elections websites, including vendor provided systems for election and voter related information, must be protected by a web application firewall and content delivery services.

VII. SOFTWARE AND HARDWARE LIFE CYCLE MANAGEMENT

Boards of elections must monitor vendor websites 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.[4] 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.

Boards of elections may NOT use any products from known hostile nation states, or any reseller of their products. Boards of elections should refer to the links below for a list of vendors that shall not be used and a list of equipment for which Hikvision is the Original Equipment Manufacturer ("OEM").

https://cyber.dhs.gov/directives/

List of Equipment and Services Covered By Section 2 of The Secure Networks Act | Federal Communications Commission (fcc.gov)

Hikvision OEM Directory 2023 (ipvm.com)

[4] End of life refers to the following but not limited to examples: (1) voting equipment that is entirely unsupported by a voting equipment manufacturer or (2) component part products' hardware or software that are no longer capable of receiving required updates from their operators, including but not limited to security updates.

Hikvision OEM List [All Companies] - Learn CCTV.com

Additionally, the Board of elections must ensure that future purchases do not include prohibited equipment. Language also must be added to purchase requests requiring vendors to attest that prohibited equipment will not be used.

VIII. INCIDENT RESPONSE PLANNING

All boards of elections are required to maintain an incident response plan which describes the process of how the boards deal with individualized events, e.g., ransomware, phishing, insider threat. Boards are required to exercise these plans on an annual basis by conducting or participating in a tabletop exercise.

Boards of elections must submit an updated copy of their Incident Response and Continuity of Operation Plans to the Secretary of State's Office.

As part of Incident Response planning, boards of elections are strongly encouraged to request that their website providers perform load tests on the boards of elections website. This testing will ensure the websites can accommodate a large increase in traffic in preparation for the 2024 election cycle.

Boards of elections must have a process in place for reporting vulnerabilities and other technical issues with the board website to the website provider. Boards must ensure the reports are submitted to the appropriate personnel who can take action to remediate vulnerabilities or resolve technical issues.

IX. SECURITY EVENT REPORTING

In the case of a security event in your county during the early voting period through Election Day, the board of elections must immediately notify the Secretary of State's Office. A detailed list of events that must be reported are outlined in Directive 2019-07 (redacted version) and Directive 2022-45, Section III.

X. 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 daily. 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. 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.[5]

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

XI. 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 accessible only to authorized personnel.

All equipment, along with the cases, cabinets, and/or shelving units that house the equipment, must be locked under a dual-control lock system.

B. SECURITY OF THE BOARD OFFICE

Physical security provides the first line of defense to any board of elections against potential threats. Boards of elections must adhere to the security requirements outlined in Chapter 3 of the Election Official Manual. This also requires boards of elections to adopt a security policy regarding the overall security of its office.

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