Frank LaRose
Ohio Secretary of State

DIRECTIVE 2025-29 SECURITY OF CRITICAL INFRASTRUCTURE

May 29, 2025

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

Re: Security of Critical Infrastructure

SUMMARY

Since the beginning of my administration as Ohio Secretary of State, my office has worked with local boards of elections to implement security directives that establish standards for vendors, strengthen physical security requirements, comply with Americans with Disabilities Act (ADA) requirements, and modernize cybersecurity capabilities. Together, we have strengthened the foundation to ensure safe and accessible elections and inspire confidence in Ohio's democratic process. What began as a pilot project has now been successfully deployed in all of Ohio's 88 county boards of elections, establishing our national reputation for election security excellence and positioning Ohio as the gold standard state. The success of Ohio's 2024 General Election demonstrates this excellence.

However, threats change daily, and therefore, our work is ongoing. This directive reinforces critical security requirements from past directives. Our team stands ready to assist you in your efforts.

GRANT FUNDING

In the past, my office utilized federal Help America Vote Act (HAVA) funding to support this work, but we are unable to rely exclusively on consistent federal funding. For this reason, I asked Governor Mike DeWine and the General Assembly for an increase in our General Revenue Fund (GRF) in the state's 2026-2027 operating budget so that we can continue to provide county boards of elections with funding and technology supports needed to operate and sustain these efforts.

If our request is fully funded and enacted by the end of this fiscal year, June 30, 2025, my office plans to fund up to $10,000 to each county board of elections that requires assistance implementing this security directive. If passed, this funding will be available to boards by mid-July 2025 and referred to in this directive and future communications as the 2025 Security of Critical Infrastructure Funding.

Boards of elections will be required to report expenses on this grant, as in years past, and enter into an Elections Security Grant Agreement (Grant Agreement) with the Secretary of State's office to receive the funding. Items or services purchased on or after the issuance of this directive, that are in accordance with this directive can be listed on the expense report as a reimbursement of spending that has already occurred.

PHYSICAL SECURITY

Proper physical security of the board office protects personnel, voting equipment, voting systems, and other IT systems to maintain the confidentiality and integrity of elections. Risks, such as damage from fire or water and unauthorized physical access, must be reduced whenever possible. All requirements must be completed by August 29, 2025.

Boards of elections must review and comply with the security requirements outlined in Chapter 3 of the Election Official Manual (EOM). They must also review and update their Board Office Security Policy regarding the overall security of their office. Security policies and procedures will be audited semiannually to ensure they are up to date and being followed.

All voting equipment, along with the rooms, cases, cabinets, or cages that house the equipment, must be locked under a dual-control lock system, ensuring that any access to the equipment requires a bipartisan team.

Boards of elections are required to secure the voter registration server. Physical security provides the first line of defense for any board of elections against potential threats. Boards of elections must secure the 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.

Exterior lighting for the perimeter of each board's building must be focused on entrances, exits, and the external drop box, and must be regularly inspected to ensure proper function.

Adequate fire suppression equipment must be available and regularly inspected for proper functional capability. Portable extinguishers shall be visually inspected each month for physical damage, such as corrosion, leakage, or dents, and to ensure the pressure gauge is in the proper operating range, if a pressure gauge exists.

Additionally, boards of elections shall maintain approved video monitoring systems for both interior bipartisan rooms and the exterior drop box. Video monitoring systems must retain footage for a minimum of 14 days and be regularly examined to ensure they are operating as expected.

Threats of physical harm to election officials and unauthorized entry or attempts to gain unauthorized access to secured facilities are security events and must be reported as soon as practical, but not more than 24 hours to the Secretary of State's office via [redacted].

CYBERSECURITY

All cybersecurity validations and requirements must be completed by August 29, 2025. Consistent progress toward completion will be tracked in the 2025-29 Compliance Checklist submitted monthly by the boards. This checklist will be reviewed during biweekly meetings with your cyberliaison.

Boards of elections must review and comply with requirements identified in Chapter 3 of the EOM.

I United States Department of Homeland Security (DHS) Services

Boards of elections are designated as critical infrastructure by DHS and accordingly have access to many free DHS services.

Boards of elections must review and 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."

Election officials can obtain information on this service by visiting CISA's website at https://www.cisa.gov/cyber-hygiene-services.

II Multi-State Information Sharing & Analysis Center

Boards of elections must review their personnel information with the Multi-State Information Sharing & Analysis (MS-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 Learn.CISecurity.org/MS-ISAC-Registration, and boards must notify the MS-ISAC of contact information changes via email.

III Ohio Secretary of State Provided 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 at no cost to the county boards of elections.

A. Cyberliaisons

The Secretary of State's office will continue to engage cybersecurity professionals to assist the county boards of elections with their IT support needs. Currently, cyberliaisons are deployed to each region of Ohio: northeast, northwest, southeast, and southwest. The cyberliaisons promote best practices to further improve the board's cybersecurity and complement the board's current IT support. For example, cyberliaisons 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. Boards should review and update their incident response plan related to Albert alerts with their

county cyberliaison. This service is funded by the Secretary of State's office, and the server replacement installation cost is a reimbursable cost under the above-mentioned grant.

C. Security Information and Event Management (SIEM)

Boards of elections must continue using the SIEM Logging service. This service is funded by the Secretary of State's office. 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 traditional antivirus products by scanning for known bad behavior and characteristics of malicious actors, rather than looking only for bad files like traditional antivirus software.

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

E. Malicious Domain Blocking and Reporting

The Secretary of State's office 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.

F. Compliance Audit

Under the leadership of its Chief Information Security Officer, the Secretary of State's office will conduct routine audits of county boards of elections' protocols and procedures for critical security controls in order to ensure compliance with this directive. This cybersecurity audit program will be piloted next month with 12 counties across the

state, and an implementation plan will be shared with all boards during the Secretary of State's annual conference in Columbus on June 30 and July 1.

IV Technical Controls

A. Board of Elections Website

Boards of elections must ensure that their websites can withstand the heavy traffic associated with general elections. Boards 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 their existing certificates do not expire.

All boards 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.

B. Vulnerability Management

The Secretary of State's office will continue to provide an authenticated vulnerability scanning service to the boards of elections at no cost to the boards. Boards of elections must conduct authenticated vulnerability scans at least once a week. 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. To meet the specified timelines, boards of elections are encouraged to utilize a patch management solution.

C. Software Maintenance

All computer and server operating systems must be supported by their manufacturer and receive regular security updates.

V Cybersecurity Awareness Training

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. 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 via email. The Secretary of State's office will continue to provide the training at no cost to the boards of elections. Additionally, boards are required to participate in tabletop exercises, as outlined in Chapter 3 of the EOM. The secretary's office will make tabletop opportunities available.

VI 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 off-network 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.

CONCLUSION

Working together we can ensure Ohio elections are safe, and that Ohioans have confidence in the election outcomes. I am grateful for your partnership and for your leadership. Our boards of elections are often recognized as cybersecurity leaders within local government, and your standards of excellence benefit communities as a whole.

For questions about the technical requirements of this directive, please contact your Secretary of State cyberliaison.

Yours in service,

Frank LaRose
Ohio Secretary of State