Frank LaRose
Ohio Secretary of State

DIRECTIVE 2020-12
July 14, 2020

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

Re: 2020 Help America Vote Act ("HAVA") Funds – Security and Accessibility Grants

SUMMARY

As a part of its consolidated Appropriations Act of 2020, Congress appropriated additional HAVA funds to the states to be used to improve the administration of elections for federal office, including enhancing technology, access to polling locations for individuals with disabilities, and making election security improvements. Ohio's share of the appropriated funds is $13,657,222. Each county board of elections will receive a block grant of $40,000 to support continued compliance with the security standards in Section 1.01 of Directive 2019-33 and additional improvements to cybersecurity, physical security, and voter accessibility.

This Directive outlines how boards of elections must use the HAVA funding to improve their cybersecurity, physical security, and accessibility.

INSTRUCTIONS

PART ONE – SECURITY AND ACCESSIBILITY GRANT FUNDING

The Secretary of State's Office is providing a block grant of $40,000 to each county board of elections. This block grant will be referred to in this Directive and future communications as the Security and Accessibility Grant. Initially, $25,000 must be designated toward satisfying the physical and cybersecurity requirements and $15,000 toward the voter accessibility requirements in this Directive. If the Board meets the physical and cybersecurity requirements and expends less than $25,000, the remainder of those funds may be re-allocated to address the voter accessibility requirements.

Each county must enter into the Security and Accessibility Grant Agreement with the Secretary of State's Office and deposit the grant payments 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 HAVA Elections Security Grant in 2019. Each board must submit an expense report (stating the month's expenses and balance of funds) to HAVAgrant@OhioSoS.gov on the first business day of each month. Please return the signed grant agreement to the same email address July 21, 2020.

The Secretary of State's Office requires each county board of elections to use the Security and Accessibility Grant toward improvements related to cybersecurity, physical security, and accessibility prior to the November 3, 2020 general election. Unspent funds must be returned to the Secretary of State's Office by February 1, 2021.

Each board must complete and submit a quote template for items or services estimated to cost at least $1,000. A board must obtain three quotes from vendors offering the required item or service and submit those quotes prior to purchasing or entering a contract for goods or services. 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 a required item or service; however, if the board selects a vendor on state term schedules, the board must still provide three quotes prior to purchasing or entering into a contract. The schedule is available here: https://procure.ohio.gov/proc/contractssts.asp.

PART TWO – CYBER SECURITY

Part Two of this Directive builds on the foundation of the cybersecurity requirements set forth in Security Directive 2019-08, which were incorporated into Chapter 15 of the Election Official Manual (Directive 2019-33). Each county board of elections must immediately share this Directive and the accompanying Technical Document with its Technical Point of Contact. The Secretary of State's Office will present webinars in the coming month to give additional information and answer commonly asked questions.

I. IT SERVICES OFFERED BY THE STATE

A. Cybersecurity Liaisons. The Secretary of State's Office is engaging cybersecurity experts to assist the county boards of elections with their IT support needs. The cybersecurity liaisons will help boards promote best practices to further improve the board's cybersecurity and election security and complement the board's current IT support. For example, cybersecurity liaisons will 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. Additional information regarding the cybersecurity liaison program is forthcoming.

B. Network Intrusion Detection. The Secretary of State's Office is extending funding for the Albert Intrusion Detection Monitoring through December 2022. Boards of elections must continue using this service. The Albert Intrusion Detection Monitoring must be configured to monitor the board of elections' network traffic and may also be used to monitor the overall county network traffic if the board of elections' network traffic is monitored.

C. **Security Information and Event Management ("SIEM") Logging.** The Secretary of State's Office is extending funding for SIEM Monitoring through December 2022. Boards of elections must continue using this 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 Solution.** The Secretary of State's Office is providing an endpoint detection and response solution ("EDR") to all county boards of elections. All critical network-connected board of elections systems, including computer workstations and servers, must begin using EDR by August 28, 2020.

EDR solutions protect system better than the traditional anti-virus products by looking at known bad behavior and characteristics of malicious actors versus looking only for bad files like traditional anti-virus software. It allows first responders to contain an infected machine remotely instead of having to be onsite. Lastly, it gives responders the ability to analyze the system remotely and assess it for other potential nefarious activity.

Installation of EDR will not obstruct the board's current IT infrastructure. The Ohio Secretary of State's EDR solution can replace the board of elections' existing malware protection or be used for added protection.

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

E. **Malicious Domain Blocking.** The Secretary of State is providing a malicious domain blocking service for all county boards of elections. This service will block access to malicious websites, help stop malware from connecting to known command-and-control infrastructure and compliment the ALBERT and SIEM services currently provided. Each board of elections must begin using this malicious domain blocking service by August 28, 2020. While the boards of elections must utilize this service, the entire county is encouraged to take advantage of this service at no cost.

II. ELECTIONS INFRASTRUCTURE INFORMATION SHARING AND ANALYSIS CENTER

Ohio has established itself as a leader in cybersecurity thanks to all 88 county boards of elections' hard work and participation in the Election Infrastructure Information Sharing and Analysis Center ("EI-ISAC"). Every Ohio county board of elections has been a member of the EI-ISAC since July of 2018, and it is imperative that each board of elections remains a member.

The EI-ISAC is an elections-specific sub-component of the Multi-State Information Sharing and Analysis Center ("MS-ISAC") and is supported by U.S. Department of Homeland Security ("DHS"). Active and continued participation provides county boards of elections with timely and actionable information regarding threats to the county's election information systems. Each board must update its information with the EI-ISAC after any staffing changes to ensure that the appropriate personnel receive and review emails. Each board must provide information received from the EI-ISAC to its technical point of contacts. New board and staff members may register at https://learn.cisecurity.org/ei-isac-registration.

III. SECURING ONLINE CAPABILITIES

Boards of Elections and their vendors must secure their online election technology by August 28, 2020, utilizing the following security controls:

1. 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.
2. 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 and enable the following services:
    a. Denial of Service ("DDoS") attack prevention;
    b. Block malicious automated scanning;
    c. Block malicious automated processes (bots);
    d. Block common system vulnerabilities such as cross-site scripting, SQL injection, and content management system vulnerabilities; and
    e. Log all web application firewall events to the Secretary of State provided SIEM.
3. Boards of elections, including vendor-provided systems, must utilize Cloudflare to provide these services. Boards of elections are eligible to sign up for the Cloudflare Athenian Project, which provides this service at no cost. If the board of elections, including vendor-provided systems, is unable to implement Cloudflare, the board must explain in writing how their web application firewall and content delivery services will be providing all the services mentioned above.

IV. SECURING ELECTRONIC MAIL

Each board of elections must use a domain name ending in ".gov" for its board of elections website and any vendor-provided websites referenced on the board of elections website for election and voter-related information. All email addresses used to conduct official business of the board of elections must end in ".gov" by August 28, 2020. If a board of elections has not yet transitioned from a ".us" domain or email address, it must have a written transition plan on file with the

Secretary of State's Office by July 15, 2020, to transition both the email and the website address to a ".gov" address no later than August 28, 2020.

All email systems must be protected with Domain-Based Message Authentication, Reporting and Conformance ("DMARC"), Domain Key Identified Mail ("DKIM"), and Sender Policy Framework ("SPF"). These services, when combined, assist email users with identifying when an email is from a legitimate source and helps prevent email spoofing. Email spoofing involves forging the sender's address and tricking the recipient into thinking the email is from a legitimate source. If a board of elections is not currently using these services, it must have a written transition plan on file with the Secretary of State's Office by July 15, 2020, explaining how it will begin using these services no later than August 28, 2020.

As stated in Chapter 15 of the Election Official Manual, no member, director, deputy director, or employee of a board of elections is permitted to use or forward to an email address other than a ".gov" email address to conduct official business of the board of elections.[1]

V. DHS SERVICES

As a result of the DHS critical infrastructure designation, election officials can take advantage of a full menu of DHS resources for no additional cost.[2] 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 following two DHS services:

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, it is highly recommended that the entire county 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, it is highly recommended that the entire county take advantage of this no-cost service.

[1] Directive 2019-33.

[2] www.dhs.gov/publication/election-security-resources.

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.

A. 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.

B. 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.

C. 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.

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

Each county board of elections must request the services listed above no later than August 14, 2020. It is also highly recommended that the entire county take advantage of these no-cost services.

VI. VULNERABILITY MANAGEMENT

To prevent cyber-crime and attacks that breach or cause harm to infrastructure, the boards of elections must continue to improve their ability to identify and mitigate vulnerabilities in a timely fashion. Understanding and managing vulnerabilities has become a continuous activity. Attackers have access to the same information and can take advantage of the gap in time between when a fix for a vulnerability becomes available and when the fix is applied. For example, when researchers report new vulnerabilities, a race starts among all parties, including: attackers (to "weaponize," deploy an attack, exploit), vendors (to develop, deploy patches or signatures and updates), and defenders (to assess risk, regression-test patches, install). Tools such as the DHS Cyber Hygiene (Vulnerability Scan) allow the board to proactively identify and address discovered flaws in their systems.

As such, the Secretary of State's Office requires the boards of elections to follow the guidelines below when in receipt of vulnerability information pertaining to their organization and IT infrastructure.

Critical and high vulnerabilities in network-connected systems must be remediated in a timely manner:

- Critical vulnerabilities must be remediated within 15 calendar days of initial detection.
- High vulnerabilities must be remediated within 31 calendar days of initial detection.

If these timelines are not achievable then the board of elections must file a detailed report to the Secretary of State's Office outlining the issue, providing the mitigation steps and timeline to achieve resolution. Evidence that these scans were completed and acted upon must be kept for at least one year in accordance with a retention schedule.

VII. ANNUAL TRAINING ON CYBERSECURITY

Each board of elections must train its board members and staff annually on cybersecurity. Each board is required to use the programs set forth in the Technical Security Document that accompanies this Directive. The programs cover topics such as knowing how to detect a phishing email, the importance of using strong passwords, and general cybersecurity awareness.

VIII. CRIMINAL BACKGROUND CHECKS

Consistent with the security requirements in Directive 2019-33, 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, 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 was completed, and that no ineligible criminal offenses were committed. Each board must have a policy that sets forth the procedures for reviewing background checks and determining whether any convictions should bar employment.

IX. CENTER FOR INTERNET SECURITY ("CIS") GUIDE FOR ENSURING SECURITY IN ELECTIONS TECHNICAL PROCUREMENTS CONTRACT REQUIREMENTS

Consistent with the security requirements in Directive 2019-33, each board of elections must follow the CIS Guide for Ensuring Security in Elections Technical Procurements and include any applicable contract requirements in any contract that the board enters with IT vendors. These requirements govern the security requirements involving externally hosted contractor information systems, information systems hosted in board of elections' or county facilities that directly connect to the board of elections' network, cloud information systems, or mobile applications.

PART THREE – PHYSICAL SECURITY

Each board of elections must regularly train its staff on the board's physical security practices and policies. Requirements for securing the board of elections' office, voting equipment, and ballots are outlined in Chapter 2, Section 1.07, of the Ohio Election Official Manual. Each board must review these requirements and ensure that its practices and policies meet or exceed the requirements set forth in the Election Official Manual.

I. SECURING THE BOARD OF ELECTIONS' OFFICE

Physical security provides the first line of defense to any board of elections against potential threats. Pursuant to the Security Section of Directive 2019-33, each board of elections completed a physical security assessment from the Department of Homeland Security. Boards of elections must mitigate security vulnerabilities identified in the report and adopt a security policy regarding the overall security of its office if it has not done so already. At a minimum, each board must have the following in place by October 2, 2020:

A. An after-hours monitored security system. When an alarm is signaled by the security system, the director and deputy director must be notified. This system must cover the room(s) used to store the voting equipment, ballots, tabulation, and voter registration servers/networking and include the following:

1. Door/Window Contact Sensors;
2. Glass Break or Motion Sensors;
3. Panic Alarm;
4. Fire and Smoke Sensors;
5. Proper fire suppression equipment; and
6. Video monitoring system (for interior rooms and exterior drop box).

B. Exterior lighting of the office building's perimeter, focusing on entrances, exits, and the external drop box.

C. Proper safety-security film on the office exterior windows.

D. Restricted access, sign-in, and supervision of visitors to areas of the board's office that house voting equipment, election materials, and its tabulation and voter registration servers, networks, and computers. During in-person absentee voting, it is sufficient that voters sign the signature book after providing identification.

E. Semi-annual audits of security policies and procedures to ensure they are being followed.

F. A reporting process to address violations of the security policy, which involves reporting to the director or deputy director at a minimum.

G. A dual-control lock system for all equipment, along with the cases, cabinets, and shelving units that house the voting equipment, which ensures access to the equipment requires a bipartisan team.

II. EMERGENCY PLANNING

Challenges, whether natural or man-made, will inevitably occur on Election Day or during the early voting period. Contingency plans are required as part of the county Election Administration Plans to ensure boards are prepared for any incident that could occur on Election Day or during the early voting period. Coordination with local law enforcement and emergency management agencies is key to a successful contingency plan. By August 28, 2020, each board of elections must request that its County Emergency Management Agency and Sheriff's Office review its emergency contingency plans. These contingency plans should appropriately address natural and human-caused disasters that could occur at the board of elections, early voting center, or any polling location in the county. Funding is available for items necessary to execute the board's emergency contingency plans.

PART FOUR – VOTER ACCESSIBILITY

Title II of the Americans with Disabilities Act ("ADA") prohibits discrimination against qualified individuals with disabilities and requires public entities to administer their programs, services, and activities in the most integrated setting appropriate to the needs of qualified individuals with disabilities. Boards of elections must use their voter accessibility portion of the Security and Accessibility Grant to ensure that people with disabilities have a full and equal opportunity to vote. The ADA's provisions apply to all aspects of voting, including voter registration, polling location selection, board offices, early vote centers, websites, and the casting of ballots, whether on Election Day or during the absentee voting period.

To assist in this goal, the Secretary of State is directing boards of elections to first complete the accessibility checklist at the main board office and early vote center, and have their websites evaluated for disability compliance by a third-party. Boards must have a clear understanding of their *current* needs. This step is vital for a board to understand how to prioritize their needs with this grant.

I. ACCESSIBILITY CHECKLIST AND WEBSITE EVALUATION

All county boards of elections must complete the following assessments:

A. Accessibility Checklist for the Board Office and Early Vote Center

Every two years, each county board of elections must complete an accessibility checklist on its office and early vote center (if applicable) using the most current version of the Ohio Secretary of State Polling Place Accessibility Checklist. The board of elections must maintain a copy of its completed checklist and develop an internal procedure for periodic review of its board office and early vote center (if applicable).[3] Each board of elections must submit its accessibility checklist for the board of elections' office and early voter center to bharbage@OhioSoS.gov by July 31, 2020.

B. Website Evaluation

Each county board of elections must have their sample ballots, voter look-up, and contact forms evaluated by a web accessibility evaluation tool, such as WAVE or AXE, to ensure conformance to the minimum requirements set forth by the Web Content Accessibility Guidelines (WCAG) level 2.1, Level AA. The tool must be capable of generating a report that can be exported. Boards must complete the website evaluation by July 31, 2020 and submit the results of their assessment to nfernandes@OhioSoS.gov. If an evaluation was performed using tools provided by Triad Government Systems after July 1, 2019, the board may send the previous report to nfernandes@OhioSoS.gov and is not required to complete a new assessment of the board's website.

II. MITIGATION FUNDING

Each county board of elections must ensure that the following features of their county board of elections website, office, and early vote center (if applicable) are accessible to all voters. Any accessibility compliance issues identified after completion of the accessibility checklist and website assessment must be mitigated to ensure people with disabilities have full and equal access to the board's programs, services, and activities.

Any construction or remediation on physical features of the main board office or early vote center (items 1, 2, 3, and 4 below) must be completed by October 2, 2020. Remediation for document or website accessibility (item 5 below) must be completed by September 15, 2020.

Boards are strongly encouraged to permanently fix features, but if this is not feasible due to construction timelines, funding may be used for temporary fixes for the 2020 November 3, 2020 election.

Boards that use funding for temporary fixes must email the ADA Coordinator, Brett Harbage, at bharbage@OhioSoS.Gov, to explain how the temporary fix will bring the county into compliance with the ADA.

[3] *See* Election Official Manual, Chapter 2, page 49.

The following items are key priorities that boards of elections must consider when deciding the order in which they will expend their allocated grant funds:

1. **Ballot Drop Box** – Ballot drop boxes must be installed in a manner that allows for people with disabilities to approach, maneuver, and reach any operable parts to drop off any election-related documents independently. To be more specific, the approach and clearance to the ballot drop box must have at least 30 inches by 48 inches of clear space; changes in level are not permitted; the slope surface must be 1:48 (2.08%) or less; and the ballot drop slot must be no more than 48 inches high from the ground surface. For all the specific and detailed accessibility requirements, please refer to the Directive 2020-12 Technical Document.

2. **Accessible Parking** – Each county board of election must provide accessible parking for people with disabilities at the board office and early vote center (if applicable).

3. **Exterior Accessible Route** - People with disabilities must be able to enter and exit their vehicle, approach the building, and enter as freely as everyone else.

4. **Accessible Entrance** - An accessible board of elections office and early vote center must have at least one accessible entrance that a person with a disability can independently access. The entrance must connect to an accessible route to the area open to the public.

5. **Document and Website Accessibility – The following are the order of priorities for website accessibility, and must be completed by September 15, 2020:**

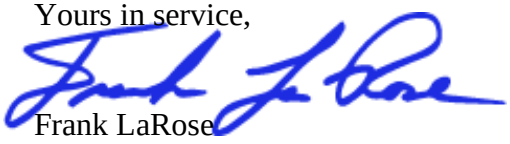
    a. **Sample Ballots** - Sample ballots must be accessible to enable voters with disabilities to preview their ballots prior to voting either in person or by mail.

    b. **Voter Look-Up** - Voter look-up on the board's website must be accessible to enable voters with a disability to find their polling location.

    c. **Contact Forms** - Any contact forms where one may send a question to the board must be accessible to voters with disabilities. This should include a properly labeled link to any direct email addresses on the website.

If a board is fully compliant in each of those areas, please contact the Secretary of State's Office and further guidance will be given regarding the expenditure of remaining grant funds from the Security and Accessibility Grant. If you have any questions regarding this Directive, please contact the Secretary of State's Elections Counsel at (614) 728-8789 or the specific staff members listed in the email accompanying this Directive.

Yours in service,



Frank LaRose
Ohio Secretary of State