Frank LaRose
Ohio Secretary of State

DIRECTIVE 2019-08
June 11, 2019

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

Re: Security

SUMMARY

As election officials, it is our duty to protect the security and integrity of Ohio's elections. The threat to our elections infrastructure continues to demand our attention and diligence. On January 6, 2017, the United States Department of Homeland Security ("DHS") designated United States election systems as part of the nation's critical infrastructure ("CI"). In March 2018, the federal government appropriated $380 million in grants to the states to secure and improve election systems.[1] In 2018, the Secretary of State's Office issued Directive 2018-15, which required each board of elections to procure services and take action to enhance its security and infrastructure.

This Directive provides Ohio with the opportunity to continue to strengthen the security of our election systems and become a best practices leader nationwide in the statewide efforts that will be undertaken to do so. The Directive instructs county boards of elections on continuing action and outlines additional requirements that each board must take to enhance its overall election security and protect its information technology ("IT") systems. This Directive also explains the grant funding available to counties to enhance their infrastructure.

As you will see, the security upgrades contained within this Directive are significant, but by working together, our office is confident each county will be able to achieve the requirements. Ohio has a strong history of administering fair, accurate and secure elections. We have long been a national leader in election security and are confident that this Directive will provide the necessary guidance to ensure that continues.

CONTINUING REQUIREMENTS

I. THE ELECTION INFRASTRUCTURE INFORMATION SHARING AND ANALYSIS CENTER ("EI-ISAC") & DHS RESOURCES

Ohio has established itself as a leader in cybersecurity with its participation in 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 remain a member.

[1] Consolidated Appropriations Act of 2018. 115 P.L. 141, 132 Stat. 348, 2018 Enacted H.R. 1625, 115 Enacted H.R. 1625.

The EI-ISAC is an elections specific sub-component of the Multi-State Information Sharing and Analysis Center ("MS-ISAC") and is supported by DHS. Active and continued participation provides county boards of elections with timely and actionable information regarding threats to your 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 should provide information received from the EI-ISAC to its county IT personnel. New board and staff members may register at https://learn.cisecurity.org/ei-isac-registration.

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 NCCICCustomerservice@hq.dhs.gov.

Each board of elections **must continue to use** the following two DHS services:

A. Phishing Campaign Assessment ("PCA"). This assessment is a "no cost six-week engagement … that evaluates an organization's susceptibility and reaction to phishing emails of varying complexity." This service must be utilized **annually** by each county board of elections.

B. Vulnerability Scanning. 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." This service must be utilized **weekly** by each county board of elections.

II. CENTER FOR INTERNET SECURITY ("CIS") ELECTIONS INFRASTRUCTURE PLAYBOOK[3]

Directive 2018-15 required each board of elections to review the CIS checklist and create an Elections Infrastructure Security Assessment ("EISA"). In order to advise and assist the board in fulfilling the mandatory portions of Directive 2018-15, counties contracted with "pathfinder" consultants. Each board of elections was required to provide a copy of its EISA to the Secretary of State's Office and make "best efforts" to address "High Priority" items prior to the November 6, 2018 General Election and address "Medium" items "as soon as reasonably practicable."

Based on the Secretary of State's review of the EISA, there are still a number of "High Priority" items that boards of elections have not addressed. Each board of elections is **required** to address and mitigate all "High Priority" items contained in the EISA no later than January 31, 2020. Additionally, the Technical Security Document, which accompanies this Directive, contains

[2] https://www.dhs.gov/publication/election-security-resources
[3] https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf.

additional details regarding these items that each board must review thoroughly. The "Funding" section of this Directive provides boards of elections with instructions on how to obtain funding to address these items.

III. SECURING ONLINE CAPABILITIES – TLS/SSL,[4] CLOUDFARE, AND GOOGLE PROJECT SHIELD

A. TLS/SSL Certificates. TLS/SSL certificates are inexpensive and increase the security of data being transferred between a user and the website and reduce the risk of the website being flagged as not secure.[5] Each county board of elections **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.

B. Cloudflare Athenian Project. Cloudflare provides a suite of services to elections officials for no additional cost. These services, collectively referred to as the "Athenian Project," include Distributed Denial of Service ("DDoS") attack protection, web application firewall ("WAF") with pre-built and custom rulesets, rate limiting, "Under Attack" emergency support, and 24/7/365 phone, email, and chat support. Each county board of elections is encouraged to consider whether participation in Cloudflare's Athenian Project would be of benefit to the board. Additional information and an enrollment form are available at https://www.cloudflare.com/athenian-project/.

C. Google Project Shield. Google offers a DDoS protection service, Project Shield, to elections officials for no additional cost. Project Shield provides advanced DDoS protection by filtering harmful traffic and absorbing traffic through caching. County boards of elections are encouraged to use Google's Project Shield. Additional information and an enrollment form are available at https://projectshield.withgoogle.com/public/.

NEW REQUIREMENTS

As mentioned above, the Technical Security Document and Ohio Mandatory Security Measures Checklist accompanies this Directive and provides additional details regarding the requirements contained within this Directive. The Technical Security Document and the Ohio Mandatory Security Measures Checklist are security records for official use only and are not subject to disclosure as a public record pursuant to R.C. 149.433. All items in the Technical Security Document and the Ohio Mandatory Security Measures Checklist are an extension of this Directive.

[4] TLS/SSL: "transport layer security" formerly commonly known as "secure socket layer" for use with online communications through secure hypertext transfer protocol, or https

[5] https://security.googleblog.com/2018/02/a-secure-web-is-here-to-stay.html.

I. ADDITIONAL SERVICES FROM DHS[6] & TABLETOP EXERCISE ("TTX")

Each board of elections is **required** to utilize the following additional services from DHS at no additional cost. Election officials can contact DHS to obtain information on these resources and services at NCCICCustomerservice@hq.dhs.gov.

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 these services no later than July 19, 2019. The Secretary of State's Office will issue an Elect Collect survey to confirm each county board of elections' participation in these services.

If critical vulnerabilities are identified based on these services, the board must immediately remediate no later than January 31, 2020.

At least two individuals from each county are required to participate in the TTX facilitated by the DHS on Wednesday, June 19, 2019 from 11:00 a.m. to 4:00 p.m. A county may send up to five individuals to participate in the TTX. County boards of elections should invite county IT staff, county Emergency Management officials, local law enforcement, or representatives from any other agency the board might collaborate with on Election Day to help things run smoothly or in the event of an emergency.

This exercise will assist participants in identifying best practices and areas for improvement in cyber incident planning, identification, response, and recovery. Through tabletop

[6] The CISA Election Infrastructure Security Resource Guide sets forth these resources and provides additional information regarding them.

simulation of a realistic scenario, participants will discuss and explore potential impacts to voter confidence, voting operations, and the integrity of elections.

II. USE OF .GOV OR .US DOMAIN NAME

Each board of elections must use a domain name ending in ".gov" or ".us" for its board of elections' website. All email addresses used to conduct board of elections official business must end in ".gov" or ".us." No board of elections' member, director, deputy director, or employee is permitted to use an email address from an email service provider (e.g., gmail, yahoo, Hotmail, etc.) or internet service provider (e.g., AT&T, Comcast, etc.) to conduct board of elections official business.

Each board of elections must comply with this requirement no later than January 31, 2020.

III. ASSESSMENT AND ANNUAL TRAINING ON CYBERSECURITY AND PHYSICAL SECURITY

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

Each board of elections must request a DHS physical security assessment, which is offered at no cost, by July 19, 2019. Through onsite "Assist Visits" followed by web-based Infrastructure Survey Tool ("IST") security surveys, DHS performs assessments of the physical security of any facility used by a board of elections, identify security gaps, and recommend improvements.

The board must also 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 meet or exceed the requirements set forth in the Election Official Manual.

IV. CRIMINAL BACKGROUND CHECKS

All permanent board of elections employees and vendors or contractors that perform sensitive services for the board of elections are required to have a criminal background check conducted. "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. Each board must have a policy that sets forth the procedures for reviewing background checks and determining whether any convictions should bar employment.

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

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 into 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.

Accompanying this Directive is the CIS Guide for Ensuring Security in Elections Technical Procurements that the county board of elections can use to meet this requirement.

VI. DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING & CONFORMANCE ("DMARC")

DMARC is an email service that assists email users with identifying whether 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. DMARC can be used with your county's existing inbound email authentication process.

Each board of elections is required to utilize this service no later than January 31, 2020. Additional information on using DMARC is found here: https://cyber.dhs.gov/bod/18-01/#introduction-to-email-authentication.

WHAT THE SECRETARY OF STATE'S OFFICE IS DOING

A. New PCs and Windows 10. The Secretary of State provided new computers with Windows 10 for each board of elections for use only on the dedicated state fiber network. Windows 10 has numerous security features which provide increased security to the Statewide Voter Registration Database ("SWVRD") and counties using the state PC with regularity for local administrative purposes.

B. SWVRD Database Modernization. The Secretary of State's Office modernized the software that serves as the backbone of the SWVRD to further enhance the security of the system.

C. Multi-Factor Authentication ("MFA"). The Secretary of State's Office is implementing MFA for all of its web-based applications available to election

officials. It implemented MFA for Outlook 365 and is in the process of implementing it for the BOE Portal.

D. Network Intrusion Detection. The Secretary of State's Office will provide Albert intrusion detection devices to all counties who do not currently have an Albert intrusion detection device or a substantially similar device. Additionally, the Secretary of State's Office will provide Albert intrusion detection devices to the voting system, epollbook, voter registration system, and remote marking ballot device vendors that are operational in Ohio. Additional information regarding this and accompanying services can be found in the Technical Security Document.

E. Security Information and Event Management ("SIEM") Logging. The Secretary of State's Office will provide SIEM and security monitoring services supporting the SIEM.

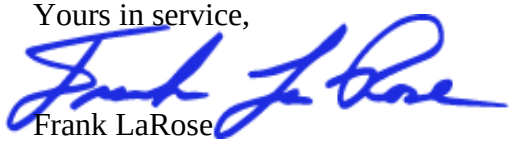
GRANT FUNDING

The Secretary of State's Office is providing one-time grant funding of $50,000 to assist county boards of elections with implementing the high priority items identified in its EISA and the Technical Security Document. Each county is required to enter into a grant agreement with the Secretary of State's Office and deposit the grant funds into a separate, interest-bearing account. Each county also is required to periodically report to the Secretary of State's Office on the balance of funds. Please return the signed grant agreement to havagrant@ohiosos.gov by July 19, 2019.

To document that the funds are spent appropriately and to ensure that the best price is received for any item or service, the board must obtain three quotes from vendors offering the required item or service and submit those quotes with a final invoice to the Secretary of State's Office. If there are fewer than three vendors, which offer the required item or service, a board must certify that fact to the Secretary of State's Office. A board is encouraged to utilize the state term schedules to identify a vendor offering a competitive price for a required item or service. The schedule is available here: https://procure.ohio.gov/proc/contractssts.asp.

If you have any questions regarding this Directive, please contact the Secretary of State's office at (614) 728-8789.

Yours in service,



Frank LaRose
Ohio Secretary of State