JON HUSTED
Ohio Secretary of State

180 East Broad Street, 16th Floor
Columbus, OH 43215
(877) 767-6446 | (614) 466-2655
info@OhioSecretaryofState.gov
www.OhioSecretaryofState.gov

DIRECTIVE 2018-15
June 21, 2018

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

Re: Cybersecurity

SUMMARY

At the first summer conference of my administration, we underscored the importance of elections officials beginning to view themselves as complex information technology systems administrators. The security and integrity of the system are increasingly important aspects of the job responsibilities of director, deputy director, and board member of a local elections office. This has only become more important given the U.S. Department of Homeland Security's (DHS) designation of state election systems as critical infrastructure (CI), increased threats to cybersecurity (or increased concerns about cybersecurity), and the availability of additional federal funds recently appropriated by Congress (HAVA II).[1]

This Directive provides instructions to county boards of elections on steps that each must take in the area of improving the security of its information technology systems. It provides recommendations on additional steps that boards of elections may take, if desired, and offers services from the Secretary of State's Office, in which a board may voluntarily choose to participate.

I. ELECTION INFRASTRUCTURE INFORMATION SHARING AND ANALYSIS CENTER (EI-ISAC)

Each board of elections must join the newly established EI-ISAC by completing the enrollment form available at https://learn.cisecurity.org/ei-isac-registration. This group is an elections specific, sub-component of the larger Multi-State Information Sharing and Analysis Center (MS-ISAC) and is supported by the U.S. Department of Homeland Security. There is no cost for membership in EI-ISAC. Active participation will provide your board of elections with timely and actionable information on threats to your elections information systems. Each board must confirm its membership enrollment in the EI-ISAC with the Secretary of State's Office no later than July 1, 2018.

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

II. U.S. DEPARTMENT OF HOMELAND SECURITY RESOURCES

As a result of the critical infrastructure designation by DHS, election officials can take advantage of a full menu of resources for free.[2] Each board of elections must sign up for the following two services from DHS:

A. Phishing Campaign Assessment (PCA) - This is a "no cost six-week engagement … that evaluates an organization's susceptibility and reaction to phishing emails of varying complexity."

B. Vulnerability Scanning – This 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."

To request these two services from DHS, email NCCICCustomerservice@hq.dhs.gov. Boards of elections must confirm with the Secretary of State's Office no later than July 1, 2018 that they have requested these two services from DHS.

An Elect Collect survey to confirm each board's enrollment in the EI-ISAC and participation in the PCA and vulnerability scanning will be sent under a separate cover.

C. Albert Monitors – DHS has funded "Albert monitors" for several of the state's larger elections jurisdictions. Albert monitors identify suspicious internet traffic entering your elections IT environment and reports it to MS-ISAC for analysis. Because malicious actors often use the same technical approach against multiple targets, Albert monitors are a useful tool to alert other elections jurisdictions of "attack vectors" so that they can adjust to known threats. Counties that have been contacted by DHS for Albert installation are strongly advised to accept and install them. As additional funding becomes available and additional monitors are provided for other boards of elections, those boards should also take advantage of this important resource.

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

A. CIS, in collaboration with state and local elections officials, technologists, vendors, and other elections community stakeholders, has produced a useful checklist designed to assist elections administrators with addressing threats. Each board of elections must carefully review the full report and identify where it can make improvements in its IT administration infrastructure and practices using the CIS checklist as a guide.

---

[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.

The board of elections must create an Elections Infrastructure Security Assessment (EISA), akin to the Election Administration Plans (EAP) that your board creates for other aspects of elections administration identifying actionable tasks that the board has taken, is taking, or plans to take in response to each item on the CIS checklist. As with the security section of the EAP, each board should discuss with its legal counsel, the county prosecuting attorney, which aspects of the EISA are exempt from disclosure as a public record under the public safety and public office security exceptions to Ohio's public records laws.[4] Each board of elections must provide a copy of its EISA to the Secretary of State's Office no later than October 15, 2018. Instructions for submission will be sent under a separate cover.

i. Boards of elections should make best efforts to address action items labeled as "High Priority" prior to the November 6, 2018 General Election.

ii. Action items labeled as "Medium" must be addressed as soon as reasonably practicable.

Boards of elections must also review and incorporate information and recommendations from the excellent *State and Local Election Cybersecurity Playbook*,[5] and the *Election Cyber Incident Communications Coordination Guide*[6] and related template[7] published by the Belfer Center for Science and International Affairs at Harvard's Kennedy School for Government.

B. Reimbursement for Consulting Services / "Pathfinders" – The Secretary of State's Office understands that each county board of elections has employees or access to other county personnel with varying degrees of experience, training, and comfort with complex information technology systems. To that end, the Secretary of State intends to use a portion of the HAVA II funds to allow individual boards of elections to engage a consultant to serve as a "Pathfinder" to advise and assist the board in fulfilling the mandatory portions of this Directive, with particular attention to the requirements contained in Section III. Additional information for securing grant funding for Pathfinder services will be provided at a later date.

IV. SECURING ONLINE CAPABILITIES

TLS/SSL – Counties that have not already done so must utilize TLS/SSL[8] certificates for any publicly facing or internal web-based applications (e.g., the county board of elections' website). Doing so is very inexpensive and will increase the security of data being transferred between a user and the website and reduce the risk of the website being flagged

[4] R.C. 149.433.
[5] https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook.
[6] https://www.belfercenter.org/publication/election-cyber-incident-communications-coordination-guide.
[7] https://www.belfercenter.org/publication/election-cyber-incident-communications-plan-template.
[8] TLS/SSL: "transport layer security" formerly commonly known as "secure socket layer" for use with online communications through secure hypertext transfer protocol, or https

as not secure.[9] Given that most boards of elections have already made this upgrade on their own or through their vendor, state reimbursement will not be made available for this requirement. Boards of elections must confirm with the Secretary of State's Office no later than September 1, 2018 that the appropriate certificate is in place. An Elect Collect survey for this purpose will be provided at a later date.

V. PUBLICLY AVAILABLE RESOURCES FOR ELECTION OFFICIALS

A. Cloudflare Athenian Project – Cloudflare is providing a suite of services to elections officials for free. These services, collectively the Athenian Project, include DDoS 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. Boards are permitted to enroll and are 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/.

B. Google Project Shield – Google is offering a DDoS protection service, Project Shield, to elections officials for free. Project Shield provides advanced DDoS protection by filtering harmful traffic and absorbing traffic through caching. Boards are permitted to enroll and encouraged to use Google's Project Shield. Additional information and an enrollment form are available at https://projectshield.withgoogle.com/public/.

VI. WHAT IS THE STATE DOING?

A. New PCs and Windows 10 – The Secretary of State is purchasing new PCs with Windows 10 as the installed operating system (OS) to be deployed at each board of elections for use only on the dedicated state fiber network. As an OS, Windows 10 has numerous inherent security features that are improved over previous versions and will provide increased security to the SWVRD and counties using the state PC with regularity for local administrative purposes. These new systems will replace the current PC supplied by the Secretary of State.

B. SWVRD Database Modernization – The Secretary of State is in the process of modernizing the software that serves as the backbone of the SWVRD to further enhance the security of the system. This will not require you to change your county voter registration system (CVRS) vendor.

C. Multi-Factor Authentication (MFA) – The Secretary of State is in the process of implementing MFA for all of its web-based applications available to election officials. MFA will be user-specific (i.e., board of elections employees will not be able to share access rights). Boards of elections should discuss with their

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

CVRS vendor when the vendor plans to implement MFA at the CVRS local application-level or whether the CVRS can leverage the secretary of state's MFA solution. More information about the Secretary of State's deployment of MFA will be available prior to launch.

D. Pilot E-mail Support – The Secretary of State's Office recently migrated to Outlook 365 for its email solution, which provides a number of protections against cybersecurity vulnerabilities, including spear phishing email attempts. Most county boards of elections receive email support from the county's IT department, local internet service provider, or common carrier (e.g., Gmail, Yahoo!, or Hotmail). As an alternative, the Secretary of State is prepared to conduct a pilot program with county boards of elections that are interested in maintaining a form of a local email domain name but relying on the Secretary of State's IT department and Outlook 365 contract for its email service. If you are interested in discussing participation in a pilot program with the Secretary of State's Office for email service, please contact the Secretary of State's regional liaison.

E. Pilot IT Support – In response to inquiries from several, primarily medium to smaller, county boards of elections, the Secretary of State's Office is prepared to conduct a pilot program with a limited number of county boards of elections that are interested in having the Secretary of State's Office serve as its IT department. Under this arrangement, the board of elections would still select its CVRS system and own the CVRS-related hardware, and be responsible for all functions related to its voting system; but, the Secretary of State's Office would become the local network and internet service provider. Networked board of elections' IT functions would sit behind the Secretary of State's firewalls and other cybersecurity systems and monitors. The board of elections would retain ownership of its local workstations, but employees and authorized users would be required to comply with the Secretary of State's Information Technology Resource Usage policy. Additionally, each workstation would be required to meet ongoing standards established by the Secretary of State's Office. No more than 10 counties, depending on the size of the county, will be permitted to participate in this pilot program in 2018. If you are interested in discussing participation in a pilot program with the Secretary of State's Office for IT support, please contact the Secretary of State's regional liaison.

If you have any questions regarding this Directive, please contact the Secretary of State's elections counsel assigned to your county at (614) 466-2585.

Sincerely,

Jon Husted

Jon Husted