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 2018-09
April 11, 2018

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

Re: Reminder of Important Security Precautions and Practices

SUMMARY

Prior to the November 2016 Presidential Election and the 2017 General Election, my office issued guidance to boards of elections regarding security best practices and precautions. Because cybersecurity threats are an ongoing concern, this Directive is to underscore the importance of these security practices and precautions and ensure that they are being routinely exercised.

In addition to reviewing this Directive, each board of elections must review the guidance and instructions on security provided in Chapter 2 of the Election Official Manual. This Directive is intended to serve as a supplement to the security requirements outlined in Chapters 2, 7, and 10 of the Election Official Manual.

INSTRUCTIONS

I. EMAIL

Directors and deputy directors must remind all staff who have access to a computer within the board of elections' office to exercise caution when opening emails. When using a computer within the board of elections' office, an email user should not open any email that appears to be spam or suspicious or that is unsolicited and contains an attachment. Because email phishing scams are constantly evolving, it is imperative that board of elections' staff know how to recognize and how to handle a suspicious email. A suspicious email might be any email:

- With an uncommon domain name (the domain name is the portion of the email address that follows the "@" symbol) or with a domain name that contains numbers inside of brackets – i.e., @[3456];
- That is sent from someone unknown to the recipient and contains an attachment or a link within the body of the message;
- That is sent from someone known to the recipient (i.e., vendors and elections organizations) but is unsolicited or unexpected and contains an attachment or link within the body of the email;
- That requests personal information (e.g., credit card numbers, user names/passwords, etc.) or money; or

- That appears to have been sent from a well-known company or organization but contains spelling errors, poor grammar, or threats (e.g., "if you do not respond to this email, your account will be closed");

A recipient should never open, respond, reply to, or forward a suspicious email.[1] A recipient should not open or download any files attached to a suspicious email or click on any links within the body of the email. Instead, the recipient should notify the designated contact person within the board or county that a suspicious email has been received.

Directors and deputy directors also must instruct all staff who have access to a computer within the board of elections' office on how to handle suspicious emails. Each board should discuss safe email practices with its or the county's IT personnel or the county's data processing center board administrator and establish a procedure for notifying the appropriate IT personnel of a suspicious email.

Additional information on types of suspicious emails and phishing attempts – and on how to identify and report suspicious emails to several common email account providers – may be found by using the following links:

Microsoft:https://www.microsoft.com/en-us/safety/online-privacy/phishing-symptoms.aspx
Google: https://support.google.com/mail/answer/8253?hl=en
Yahoo: https://safety.yahoo.com/Security/PHISHING-SITE.html
AT&T: https://www.att.com/esupport/article.html#!/email-support/KM1010551

Boards should conduct phishing awareness campaigns to ensure staff are properly trained in identifying and reacting to a suspicious email. An available resource to boards is the spear-phishing campaign assessment the Department of Homeland Security offers to entities deemed critical infrastructure.[2]

II. WEBSITE, SYSTEM, AND DATA SECURITY

Each board of elections must take every precaution available to ensure the security of its website, systems, and data. A board, if it has not already, should discuss what security precautions are in place with its voting system, voter registration, and website vendors.

[1] Often, the most effective phishing emails may appear to come from known email addresses and will contain ordinary subject lines. Phishing emails can often be identified as malicious by looking for misspellings, errors/changes in the email address, and requests for information that would not normally be requested by email. Furthermore, when responding to emails from unknown or suspicious senders (if necessary), it is better to use the "forwarding" function rather than "replying" as forwarding it requires the user to physically re-enter the sender's email address, allowing the user to identify unknown or suspicious email addresses. Finally, phishing emails should be provided to local IT personnel to enhance situational awareness.

[2] DHS Election Infrastructure Security Resource Guide" for additional information on the spear-phishing campaign assessment: https://www.dhs.gov/sites/default/files/publications/election-resource-guide-03162018-508v2.pdf.

A board also should apply the following best practices:

- Confirm that search fields on its website are locked in such a way as to limit the risks of SQL injection attacks.
- Implement and utilize allowable firewalls, anti-virus software, and anti-spyware software – and keep the software up-to-date –to protect against unauthorized access.
- Move websites to Hypertext Transfer Protocol Secure (HTTPS) for added website security.
- Ensure that all ports in the board's voter registration server (except the port for the Statewide Voter Registration Database connection) are locked and routinely monitored.
- Limit access to systems and data only to those agents and employees who require access. A board should know when, and for what purpose, anyone – even an authorized user – is accessing any aspect of the board's voter registration or election management system. To that end, the board should utilize the systems' auditing and intrusion detection capabilities and monitor the systems to determine whether any unauthorized access or attempted access has occurred.
- Do not connect the voter registration database or election management system to any other system that is not required for their use.
- Wherever permitted (i.e., not with your central tabulating system that requires federal certification of material changes), be sure to use current versions (with relevant security updates) of operating systems, software, and web content management programs (e.g., WordPress, etc.). Using the current versions helps protect the board's systems against known vulnerabilities.
- Limit access to any network (wired or wireless) to authorized users who have been provided with the necessary network credentials, security key, and/or access code for connection. A board should consider the following safeguards for networked communication:
    - Secure any router according to industry standards for security.
    - Utilize non-broadcasting Service Set Identifier (SSID) to make the access point invisible on most wireless and mobile devices.
- Take advantage of the cyber hygiene and risk and vulnerability assessment services offered by the U.S. Department of Homeland Security. For details on available services, please email the State, Local, Tribal, and Territorial Government Coordinating Council at nccicustomerservice@hq.dhs.gov.[3]
- Use strong passwords and encryption on a removable media device (i.e., USB stick, thumb drive, flash drive, etc.) to protect the data that is contained on the device.[4]

[3] For a full catalog of services provided by the Department of Homeland Security visit: https://www.dhs.gov/topic/election-security.

[4] See "Protecting Portable Devices: Data Security" for additional guidance and suggestions: https://www.us-cert.gov/ncas/tips/ST04-020.

- Enable two-factor authentication on all website and social media accounts maintained by the board of elections. Ensure that passwords are unique, complex and different for every site accessed, and are not shared to prevent unwanted access to the applications. Board officials and staff should also ensure that strong security practices are applied to personal email and social media accounts to deter unauthorized access and the possible communication of false election-related information to the public.
- Ensure that all website software is routinely patched and maintained to prevent distributed denial of service attacks and or the posting of false information on an official site.
- Determine which individuals have the ability to update the board's website and know who is responsible for the hosting of the website in the event a situation occurs and requires attention of web-service providers. Review the website and official social media accounts frequently to prevent the posting of fake or false content.

III. USE OF REMOVABLE MEDIA DEVICES

Board of elections' staff must exercise caution when using removable media with board of elections' servers and computers. Attackers can install malware or malicious code onto a removable media device. If the infected device is inserted into a computer, that malware or malicious code can infect the computer. The U.S. Computer Emergency Readiness Team (CERT) recommends several best practices to follow when using removable media.[5]

Board of elections' staff should never use a personal removable media device to save information from a board of elections' server or computer or transfer files from one board of elections' server or computer to another. Only removable media purchased and maintained by the county board of elections should be used for this purpose. Moreover, a removable media device that is purchased and maintained by the board of elections for use within the board of elections' office should never be inserted into a personal computer or laptop.

Board of elections' staff must never use or insert an unknown removable media device into a board of elections' server or computer. If the board of elections discovers an unknown device, it should provide the device to the appropriate county IT personnel for inspection and investigation.

Each board of election should disable "Autorun" on its servers and computers. Disabling this feature prevents a server or computer from automatically opening and running the contents of a removable media device.

To preserve an "air gap" between systems connected to the internet or other unknown systems, each board must maintain a single-use policy when transferring election results from the EMS to the system utilized to transmit election results. A media device, such as a USB stick, used to transfer election results must never be inserted into the EMS after being inserted on another device.

[5] https://www.us-cert.gov/ncas/tips/ST08-001.

Boards need to be vigilant and ensure that third-party vendors who use, for instance, removable media to program voting systems and election management systems (EMS) are not reusing that same media. Also, ensure they are taking the proper steps to isolate the central processing unit (CPU) used to program ballots.

IV. BACKUP OF VOTER REGISTRATION AND ELECTION MANAGEMENT SYSTEM DATA

The board's voter registration data should be backed up on a daily basis.[6] If unwanted modifications to the data occur, or a situation requires recovery of data, the database can be restored to its last known state. If the board's voter registration system vendor needs remote access to the system to perform backups, the board should ensure that this access is password protected and consider implementing two-factor authentication as well. A board may want to consider locking vendor access except for pre-determined timeframes or require pre-authorization prior to remote access of the server.

The board's election definition data from its central tabulation system should be backed up after the board has completed its programming for the election and after any change is made to backup data available on the system. It also should be backed up after any change is made to the board's election definitions, so that, if unauthorized modifications occur, the data can be restored.

The medium containing the backup data from both the board's voter registration and election management systems should be stored in a secure, offsite location at least once per week, and the board should utilize encryption to protect any data containing confidential or personal information.[7]

Backups of data should be tested regularly by taking backup files and loading them to ensure the data is accessible and can be restored from the backup. Further, ensure that antivirus and patches are up to date and confirm that there is no malware present on the backup device. Each board should work with its voter registration vendor and county IT personnel to determine how to test an existing backup and perform a complete restoral from the backed-up data.

V. PROHIBITION ON INTERNET CONNECTION

No part of a voting system, including the system's tabulation server, may be connected to the internet.[8]

VI. PROTECTION OF CERTAIN PERSONAL INFORMATION

Each board is reminded that a voter's driver's license or state identification card number must never be disclosed, appear on the board's website, or be accessible to precinct election officials

[6] See "Ransomware and What To Do About It" for additional information: https://www.eac.gov/documents/2016/9/16/ransomware-and-what-to-do-about-itpdf/.
[7] It is considered a best practice to use the "3-2-1" method: three copies, two different devices, one in a separate location.
[8] R.C. 3506.23.

on a signature pollbook or electronic pollbook. A board is encouraged to consult with its legal counsel, the county prosecuting attorney, regarding what information must be disclosed and what information must not be disclosed in response to a public records' request.

VII. RE-REVIEW OF CHAPTER 2 OF THE ELECTION OFFICIAL MANUAL

Each board of elections must re-review the Security section of Chapter 2 of the Election Official Manual to refresh recollection on the guidance and instructions provided on the following topics:

- Security of the Board Office;
- Secure and Proper Storage of Voting Equipment;
- Inventory of Voting Equipment;
- Secure and Proper Storage of Ballots and Election Data Media;
- Inventory of Ballots;
- Security of Voting System and Tabulation Programs/Software;
- Passwords;[9]
- User Account Management; and
- Access Log; and Third Party Access to Voting System.

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

Sincerely,

Jon Husted

[9] Passwords to any system or service accessed frequently or at regular intervals should generally be changed every 90 days. It is recommended that passwords for voting systems and services be reset before each election whenever practicable. The U.S. Department of Homeland Security has information on passwords at https://www.dhs.gov/blog/2013/05/08/protecting-your-personal-information-secure-passwords and https://www.dhs.gov/sites/default/files/publications/Best%20Practices%20for%20Creating%20a%20Password.pdf.