Frank LaRose
Ohio Secretary of State

Chapter 3: SECURITY

Directive 2022-07

Section 3.01 Security

SECURITY OF THE BOARD OFFICE

Each board of elections is required to adopt a policy regarding the overall security of its office. When adopting its security policy, a board must consider, at minimum, the following:

1. How it can best prevent unauthorized access to the board office;
2. How board staff will register and supervise visitors;
3. How the board can restrict access to those areas of its office that house voting equipment, election materials, and its tabulation and voter registration servers, networks, and computers;
4. How will the board regularly audit its records and procedures to ensure they are being followed; and
5. If there is a violation of the security policy, what is the reporting process?

SECURE AND PROPER STORAGE OF VOTING EQUIPMENT

In addition to adopting a policy to address the overall security of the board office, each board of elections must adhere to the following guidelines in storing voting equipment at its office or other designated site whenever the equipment is not in use.

1. To prevent damage and maintain the integrity of the equipment, each board of elections must store its voting equipment properly in a secure, clean, and climate-controlled area.
2. Physical security of voting equipment in the storage area must be maintained at all times. Access to the equipment should be limited to the least number of board personnel as possible.

3. If the board office is not equipped with a monitored security system, the room(s) used to store the voting equipment, tabulation and voter registration servers and networking equipment must have a monitored security system that will detect and alarm on unauthorized access.
4. When an alarm is signaled by the security system at the board office or room(s) used to store the voting equipment, tabulation and voter registration servers, and networking equipment, at a minimum the director and deputy director must be notified. The director or deputy director must notify the Secretary of State office as described in Directive 2019-07 (Reporting of Security Events).
5. All equipment, along with the cases, cabinets, and/or shelving units that house the equipment, must be locked under a dual-control lock system, such that any access to the equipment requires a bipartisan team. The director or designee of the same political affiliation must hold one key or lock combination and the deputy director or designee of the same political affiliation must hold the other key or lock combination.
6. The identification of any visitor, vendor, or maintenance personnel must be verified before they may be granted access to the equipment storage area. The board must keep a log of the name of each visitor, vendor, or maintenance person who enters the area, along with the date and time of their entry and exit. Visitors should be monitored at all times. The best method for access control is one that uniquely identifies the person, authorizes entry, and logs the date and time of access (i.e., badges, door entry access devices, and video monitoring system).
7. The storage area must be equipped with a monitored, alarmed smoke detection system and the proper fire extinguisher(s) or suppression system, so, if a fire occurs, it may be detected, extinguished, or suppressed as quickly as possible. Board personnel must be trained on how to respond to a fire in the storage area.
8. All voting equipment must be stored properly. Each board must contact the manufacturer of its voting equipment and request and review the voting equipment or system manual for instruction on the proper storage of the equipment. Please note that improper storage of the equipment may affect the voting system maintenance agreement and/or the equipment's warranty.
9. The storage area must be clean and free of excess dust, debris, and pests. The board should routinely inspect and clean the area. Voting equipment must not be stored on the ground in an area prone to flooding or in any area where liquid accumulates.

TAKING OF VOTING EQUIPMENT OFF-SITE

A board of elections may on occasion take voting equipment off-site for demonstrations, to raise public awareness of the voting process, or in case of relocation due to an emergency situation. Such events encourage civic engagement and build public trust in the election process. To maintain that public trust, the board must always ensure the security of voting equipment.

Bipartisan control of the voting equipment must be maintained at all times including during transportation and the demonstration. The only exception to this requirement is when a private company is contracted by the board to deliver equipment. In either case, to ensure the security of the voting equipment, the board must follow all procedures outlined in Chapter 9, section 1.01 of this document including the use of tamper evident seals. If a member of the bipartisan team must leave the area for an extended period of time such as for a lunch break, a person of the same party who meets the requirements must relieve the team member. Usage and custody of the voting equipment must be recorded according to the board's inventory control process.

INVENTORY OF VOTING EQUIPMENT

The board must inventory all of its voting equipment and maintain a list of each item of equipment and its corresponding serial number. Additionally, for each piece of equipment, the board must retain the following:

1. Invoice, purchase order, or other documentation of the purchase of the equipment;
2. Chain of Custody Log for at least 90 days following every election;
3. Record of the equipment's usage (i.e., the date and location of use and the individual(s) using the equipment);
4. A report of any damage to or unauthorized handling of the equipment; and
5. Any repair history (when, where, by whom, for what purpose, and the outcome) and documentation of the repair.

The inventory list must be maintained and reviewed on a regular basis by the board's director and deputy director.

SECURE AND PROPER STORAGE OF BALLOTS AND ELECTION DATA MEDIA

For purposes of this section, ballots and election data media includes, but is not limited to the following:

1. Optical scan ballots prepared by a vendor or printed in house by the board for use in an upcoming or previous election;
2. Blank ballot stock for a ballot printer;
3. All memory cards;
4. CDs or USB drives that house election results;
5. VVPATs; and
6. Ballot initiation or access devices (e.g., Personal Electronic Ballot cartridges, access cards, eCM tokens).

When not in use, all ballots and election data media also must be stored properly in a clean and climate-controlled environment that is equipped with a secured, monitored, alarmed smoke detection system, and the proper fire extinguisher(s) or suppression system following the guidance provided above for the storage voting equipment. These items must not be stored on the ground in an area prone to flooding or in any area where liquid accumulates. Food and beverages should never be stored or consumed within the storage area.

Access to ballots and election data media must be restricted to authorized personnel only. These items should be segregated and stored in a separate, locked room or storage unit (e.g., cabinet) designated for that purpose. As with voting equipment, ballots and election data media must be locked under a dual-control lock system. An explanation of a dual-control lock system is provided under "Secure and Proper Storage of Voting Equipment."

Ballots must be stored as recommended by the printer (or, if storing blank ballot stock, as recommended by the manufacturer of the blank ballot stock). They must be stored in protective cases, containers, or if recommended by the printer or manufacturer, in their original packaging.

Election data media should be stored in a sleeve or case and should be marked so that each item is easily identifiable.

INVENTORY OF BALLOTS

The board must inventory all ballots by implementing the following procedures:

1. If optical scan ballots are printed by an outside source, the board must maintain a list of the ballot styles and the number of ballots for each style that are delivered to the board by the printer. The board must document any discrepancy between what was ordered and what was received and the steps taken to rectify the discrepancy. The board must also maintain a list of the sequence numbers of the ballots received, the number and sequence number range of the ballots that will

be provided to each precinct, and number and sequence number range of the ballots for absentee and provisional voting. The board must document the disposition of each ballot (i.e., voted, unvoted, or spoiled).

2. If optical scan ballots are printed in house via a BOD printer, the board must document the use of each sheet of blank ballot stock.[1]

A Chain of Custody Log must be used to document the delivery of optical scan ballots to each precinct.

SECURITY OF VOTING SYSTEM AND TABULATION PROGRAMS/SOFTWARE

No voting machine[2] or component of a voting system may be connected to the internet. A voting system includes the total combination of mechanical, electromechanical, and electric equipment, including software or firmware required to program, control, and support the equipment that is used to: set up elections, define ballots cast, receive voting data from polling locations, count votes, report or display election results, and maintain and produce any audit trail information. The board's voter registration server is not considered a voting machine or component of a voting system for purposes of this section.

Voting machines or components of a voting system may only be connected via a local computer network cable to the central tabulating system (a closed local network) for the purpose of creating or uploading memory cards, ballots definitions, precinct results, and other required tasks. Additionally, voting machines in a polling location may be connected to a closed local network.

Election results, ballot definitions, or other similar information must never be transferred to a voting system via the internet (except that blank ballots may be transmitted to a UOCAVA voter via the internet or facsimile).

No one may download or install software or firmware on a voting machine or components of a voting system without prior approval from the Secretary of State's Office.

PASSWORDS

In order to maintain the proper security of the voting equipment and central tabulating system the following password protocols must be used:

A BIOS password shall be required for all vote tabulation sever systems, forcing users to enter a correct BIOS password in order to boot the machine.

[1] No board of elections shall use a ballot-on-demand system unless each ballot printed by the system includes a tracking number. R.C. 3506.20(B).
[2] R.C. 3506.22.

All central tabulating systems must be password protected. At a minimum the passwords must be composed as follows:

- ☐ The password must be split with authorized Republican personnel possessing half of the password and authorized Democratic personnel possessing the other half of the password;
- ☐ The entire password must be at least 15 characters or the minimum number that the system will accommodate, whichever is greater;
- ☐ Each half of the password must have a number included in it;
- ☐ Each half of the password must include one non-alphanumeric character;
- ☐ Each half of the password must include mixed-case letters; and
- ☐ The entire password must have no more than two consecutively repeating characters.
- ☐ Simple letter substitution is NOT considered acceptable. (Example – D1ct10n4ry is NOT a secure password.)

Both the BIOS and central tabulating system software passwords must be changed prior to every election.

Both the BIOS and central tabulating system software passwords must require 10 unique passwords prior to reuse of a prior password.

Both the BIOS and central tabulating system passwords shall be distributed to only authorized users. This means that the posting of the either half of a password on a monitor or keyboard is strictly prohibited.

The system shall log out users after five minutes of inactivity.

USER ACCOUNT MANAGEMENT

For all IT systems containing voter information and central tabulating systems, boards of elections must require every user to have a single unique user ID and a personal password unique to that user. This ID and password must be required for multi-user access to computers and networks.

All users of boards of elections systems, email, and official social media accounts must utilize the following controls:

- Each user must have a unique username and password/passphrase.
- Users are strictly prohibited from sharing passwords/passphrases or multi-factor authentication devices.

- Passwords/passphrases must be complex and comply with the following complexity requirements:
    - Be at least 15 characters in length.
    - Contain three out of the following four items:
        - Number
        - Lower-case letter
        - Upper-case letter
        - Symbol
    - Not contain the user's name or username.
    - Avoid using simple dictionary words without proper lengths or complexity. Passwords/passphrases should be generated from pass phrases or uncommon word associations.
        - Example: Buckeys79!AreBlah
    - Simple letter substitution is NOT considered acceptable. (Example – D1ct10n4ry is NOT a secure password.)
- Passwords/passphrases shall not be re-used across different applications. For example, your personal email account and your board of elections email account passwords cannot match. Your LinkedIn password/passphrase should not match your Twitter password/passphrase. This reduces the effectiveness of a popular threat called "credential stuffing."
- Passwords/Passphrases must be encrypted while stored in a format prescribed under NIST 800-53.

Multifactor authentication must be used for all accounts accessing or modifying voter registration data and election systems, email, system administrator access and remote access sessions. Any multifactor solution must follow NIST 800-63b standards, and can be achieved by using smart cards, certificates, one-time use password tokens, or biometrics. Boards of elections that utilize social media are strongly encouraged to ensure that accounts are secured using multi-factor authentication.

ACCESS LOG

Directors and deputy directors shall regularly monitor the access logs maintained by their election management systems voting system servers, voter registration servers, computers, firewall, and networking devices. When checking these logs, directors and deputy directors should look for any unusual or suspicious access or activity on the system. Examples of this kind of activity would be accessing the systems at unusual

hours and with unusual frequency.

These logs must be stored, where possible, on a dedicated system to ensure that the logs can be securely maintained. All access logs and events collected must be kept for 90 days.

Electronic logs must not be disabled.

THIRD PARTY ACCESS TO VOTING SYSTEM

Board policies on voting system server security must prohibit individuals who are not employees, contractors, or consultants of the board of elections or the Secretary of State's Office from being granted a user ID or otherwise be given privileges to access any network or component of the election system within the board offices or at a satellite location, unless the written approval of both the board's chairman and director have been obtained.

Any remote access to board of elections systems or networks must use secure remote access technologies such as Transport Layer Security (TLS v1.2 or higher) or IPSEC. Multifactor is required and must comply with the User Account Management section of this chapter. Any remote access solution being utilized must:

- All remote access solutions must use Virtual Private Network ("VPN") with Multifactor Authentication ("MFA")
- All remote access traffic must be encrypted pursuant to the state of Ohio's data encryption standards and policies. These policies can be found at: https://das.ohio.gov/Divisions/Information-Technology/State-of-Ohio-IT-Policies
- All encryption systems must comply with National Institute of Science and Technology ("NIST") Federal Information Processing Standard ("FIPS") 140-2.
- All remote access sessions must be logged and stored as described in the access log section of this chapter.

Before providing to any third party access to any network or component of the election system within the board's offices or at a satellite location, written documentation defining the following shall be executed: the scope of work and authorization for access to any network or component of the election system within the board offices or at a satellite location; relevant terms, including the name of a responsible manager at the third party organization; and the timeframe, with starting and ending dates and times, if applicable, for access.

Section 3.02 Information Technology Security

All network connected systems, including but limited to, voter registration server(s), workstations, networking and firewall devices must follow all items outlined in Directive 2019-08.

VULNERABILITY MANAGEMENT

Each board of elections must continue to utilize the following Department of Homeland Security ("DHS") services:

- 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.
- 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.

On a weekly basis, all board of elections systems must be scanned on the internal network using a Security Content Automation Protocol ("SCAP") compliant vulnerability scanner. A list of critical and high vulnerabilities must be provided to the system administrators, technical point-of-contact, or providers for remediation.

Critical and high vulnerabilities in internet-accessible systems must be remediated in a timely manner:

- Critical vulnerabilities must be remediated within 15 calendar days of initial detection.
- All remaining high vulnerabilities must be remediated within 31 calendar days of initial detection.

Evidence that these scans were completed and acted upon must be kept in accordance with a retention schedule and for at least one year.

EMAIL AND WEBSITE SECURITY

Each board of elections email address and website must end in .gov domain names.

Board of elections email messages cannot be forwarded to personal email accounts such as Gmail.com, Hotmail.com and Yahoo.com.

All county boards of elections email accounts must utilize Domain-based Message Authentication, Reporting and Conformance ("DMARC") services. DMARC gives email owners the ability to protect their email from unauthorized use by verifying authenticity. A key component of DMARC is Domain Keys Identified Mail ("DKIM"). The purpose of implementing DMARC and DKIM is to protect a domain from being used in business email compromise attacks, phishing emails, email scams and other cyber threat activities. Additional information regarding DMARC can be found at:

https://cyber.dhs.gov/bod/18-01/#introduction-to-email-authentication

Boards of elections email must utilize Sender Policy Framework ("SPF"). SPF has the ability to tell mail servers to reject mail not coming from the correct source.

All county board of elections email accounts must be using multifactor authentication ("MFA").

Each permanent employee and board of elections member who need email access must have an individual email address that meets these requirements.

NETWORK SECURITY

All boards of elections must ensure that the network being used is configured in a secure method as described in the Technical Security Document attached as part of Directive 2019-08, specifically covering topics of network protection, network scanning, segmentation, device whitelisting, wireless, and access control.

VOTER REGISTRATION AND ELECTION MANAGEMENT SYSTEM DATA

The board of elections voter registration server and any data processed by the board of elections must be backed up on a daily basis. These backups must be encrypted following National Institute Science and Technology ("NIST") Federal Processing Standard ("FIPS") 140-2. Additional details on encryption requirements can be found in the Technical Security Document attached as part of Directive 2019-08.

A copy of this backup must be stored in a secure off-site location at least once per week. This backup will need to be used should anything happen to the backup stored locally at the board of elections.

At a minimum, the board of elections must annually test the backup ensure that the voter registration server can be fully restored using the off-site backup.

Section 3.03 Security

As election officials, it is our duty to protect the security and integrity of Ohio's elections. Each county board of elections is required to take the actions outlined in this Section to enhance its overall election security and protect its information technology (IT) systems.

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.

The EI-ISAC is an elections specific sub-component of the Multi-State Information Sharing and Analysis Center (MS-ISAC) and is supported by the U.S. Department of Homeland Security (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.[3] 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

[3] https://www.dhs.gov/topic/election-security#.

participants to reduce their exposure to exploitable vulnerabilities." This service must be utilized **weekly** by each county board of elections.

CENTER FOR INTERNET SECURITY (CIS) ELECTIONS INFRASTRUCTURE PLAYBOOK[4]

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 this duty, 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 were still a number of "High Priority" items that boards of elections had not addressed. Each board of elections was then **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 accompanied Directive 2019-08, contains additional details regarding these items that each board must review thoroughly.

SECURING ONLINE CAPABILITIES – TLS/SSL,[5] CLOUDFLARE, 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.[6] 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/.

[4] https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf.
[5] TLS/SSL: "transport layer security" formerly commonly known as "secure socket layer" for use with online communications through secure hypertext transfer protocol, or https.
[6] https://security.googleblog.com/2018/02/a-secure-web-is-here-to-stay.html.

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/.

All board of elections websites must utilize either Cloudflare or Google Project shield services to protect the board of elections websites.

The Technical Security Document and Ohio Mandatory Security Measures Checklist accompanying Directive 2019-08 provide additional details regarding the requirements contained within this Section. 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 Section.

ADDITIONAL SERVICES FROM DHS[7] & TABLETOP EXERCISE ("TTX")

Each board of elections is **required** to utilize the following additional services from DHS at no additional cost prior to each general election in even-numbered years. Election officials can contact DHS to obtain information on these resources and services at NCCICCustomerservice@hq.dhs.gov.

1. 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.
2. 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.
3. 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.

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

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

If critical vulnerabilities are identified based on these services, the board must immediately remediate no later than 30 days after they have been identified.

USE OF .GOV DOMAIN NAME

Each board of elections must use a domain name ending in ".gov" for its board of elections' website. All email addresses used to conduct board of elections official business must end in ".gov". 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.

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 that accompanied Directive 2019-08. 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 complete a DHS physical security assessment, which is offered at no cost. 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, identifies security gaps, and recommends improvements. The board of elections should carefully review the DHS assessment report and consider the recommendations for improved security.

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.

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 (1) require access to customer/consumer/agency employee information, (2) relate to the board of elections or Secretary of State's computer networks, information systems, databases or secure

facilities under circumstances that would permit modifications to such systems, or (3) involve unsupervised access to secure facilities.

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.

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.

DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING & CONFERENCE ("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. DMARC must be configured to either require the rejection or quarantine of any messages that fail DMARC.

Additional information on using DMARC is available here: https://cyber.dhs.gov/bod/18-01/#introduction-to-email-authentication.

Section 3.04 Security Reporting

Over the last several years, local, state, and federal partners have worked diligently to enhance the security of Ohio's election infrastructure. Despite this community's vigilance, "security events" (a broad term that can encompass everything from a pulled fire alarm at a school, a vehicular accident that takes out an electric pole and electricity to a polling location, to severe weather events, and more) can still occur.

The purpose of this section is to define the types of "security events" that must be reported to the Secretary of State's Office and to provide a streamlined reporting mechanism for doing so.

TECHNICAL POINT OF CONTACT

Each board of elections must identify a Technical Point of Contact ("TPOC"). This TPOC can be an employee of the board of elections, or if the board of elections contracts for external IT support services provided either by the county or a third party, an employee of that contracted organization. The board must notify the Secretary of States' office anytime there is a change in the board's TPOC including to any of the TPOC's contact information.

REPORTING

If a security event occurs in your county, you must immediately notify the Secretary of State's Office. This notification must occur as soon possible even if the event occurs outside of normal business days or hours. In order to streamline the reporting of any security events, you must use the email address contained in Directive 2019-07 to relay the relevant information. If you are unable to relay the information via email, you must follow the instructions outlined in Directive 2019-07. Even if local law enforcement or other first responders are aware of your security event, it is the responsibility of the local election officials to report the nature of the event to our office using this email address anytime that a security event occurs. This reporting requirement applies year-round.

TYPES OF EVENTS

The following is a list of possible "security events" that must be reported to our office; this list is not exhaustive. If you do not know whether an event is required to be reported, it is best to report it.

1. Unauthorized entry or attempts to gain unauthorized access to storage facilities, polling location, early vote centers, and/or offices of the board of elections (regardless of whether on private or public property that is used by the board of elections).
2. Incidents of phishing,[8] including spear-phishing,[9] or attempts to hack county voter registration systems or websites, including similar efforts against seemingly unrelated county government entities.
3. Attempts to access, alter, or destroy systems used to qualify candidates; produce

[8] *Phishing* is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.
[9] *Spear-phishing* is the fraudulent practice of sending emails ostensibly from a known or trusted sender in order to induce targeted individuals to reveal confidential information.

and deliver ballots; procure, manage and prepare voting equipment; process request for absentee ballots; and store and manage administration process and procedure documentation.

4. Unauthorized access or attempts to access, or unexplained inaccessibility or unavailability of, IT infrastructure or systems used to manage elections, including systems that count, audit, or display election results on election night and systems used to certify and validate post-election results.
5. Attempts to hack, phish, or compromise personal or professional email accounts and social media accounts of elections officials, staff, and precinct election officials.
6. Hacking attempts or successful hacks into political party or candidate headquarters or IT systems, including email.
7. Attempts to access, hack, alter, or disrupt infrastructure to receive and process absentee ballots through tabulations centers, web portals, email, fax machines; attempts to interfere with votes sent through the U.S. Postal Service.
8. Compromises of any networks and/or systems, including hardware and/or software, to include tactics, techniques, procedures and impact observed on election-related networks and systems; evidence of interference detected on county networks or systems for cyber security indicators of compromise.
9. Attempts to persuade an elections official to engage in illegal activity or deviate from established practices in an effort to impact the administration of the election.
10. Instances of any unexplained disruption at a polling location or training location for precinct election officials, including early voting locations, which block or inhibit voter participation. Disruptions may include social media posts or robo-calls or texts reporting closed or changed polling locations, or physical incidents at polling locations, including distribution of false information.
11. Disinformation efforts to alter or shutdown government web sites to foment social unrest or alter voter participation (including via social media or other electronic means).
12. Unauthorized entry of centralized vote counting/tabulation locations or electronic systems or networks used by board of elections to count voted ballots.
13. Impacts to critical infrastructure that limit access to polling locations or information from elections officials, such as power, natural gas, water, internet, telephone (including cellular), and transportation (including traffic controls) outages.