

Chapter 15: MISCELLANEOUS DUTIES

Directive 2019-33

SECTION 1.01 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.¹ Election officials can obtain information on these resources and services by contacting DHS at NCCICCustomerService@hq.dhs.gov.

¹ <https://www.dhs.gov/publication/election-security-resources>



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.

CENTER FOR INTERNET SECURITY (CIS) ELECTIONS INFRASTRUCTURE PLAYBOOK²

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 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 accompanied [Directive 2019-08](#), contains additional details regarding these items that each board must review thoroughly.

SECURING ONLINE CAPABILITIES – TLS/SSL,³ 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.⁴ Each county board of elections **must** continue to utilize TLS/SSL certificates for any publicly facing or internal web-

² <https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf>

³ TLS/SSL: “transport layer security” formerly commonly known as “secure socket layer” for use with online communications through secure hypertext transfer protocol, or https

⁴ <https://security.googleblog.com/2018/02/a-secure-web-is-here-to-stay.html>



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/>.

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 DHS⁵ & 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.

- A. Risk and Vulnerability Assessment. This onsite assessment gathers data and "combines it with national threat and vulnerability information" to detect

⁵ The CISA Election Infrastructure Security Resource Guide sets forth these resources and provides additional information regarding them.



- 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.

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”. Boards of elections continuing to use a “.us” domain or email address must have a written transition plan on file with the Secretary of State’s office to transition both the email and the website address to a “.gov” address no later than July 1, 2020. 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 (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.

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.

Each board of elections is required to begin utilizing 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>.

SECTION 1.02 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 place, 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 places, 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 phishing⁶, including spear-phishing⁷, 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 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.

⁶ *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.

⁷ *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.



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 place 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 places, or physical incidents at polling places, 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 places or information from elections officials, such as power, natural gas, water, internet, telephone (including cellular), and transportation (including traffic controls) outages.

Section 1.03 Vacancy in Elective Office

A vacancy in a public elective office can be caused by the death, resignation, suspension, or removal of the holder of the office before the current term has expired. The vacancy usually is filled initially by appointment in accordance with the relevant legal provisions. The vacancy in office also may require the holding of an election for the remainder of the unexpired term, depending on: 1) the particular office in which the vacancy has occurred, and 2) when the vacancy occurred.

Various provisions of the United States Constitution, Ohio Constitution, Ohio Revised Code, and home rule charters set forth procedures for filling a vacancy in a particular office by appointment, either for the remainder of the term or until an election is held to select someone to serve for the remainder of the unexpired term.

When a vacancy occurs in a county office, the board's director provides notice of the party's right to make an appointment to fill the vacancy to the central committee of the political party with which the outgoing office holder is affiliated.



A board may use Secretary of State [Form 292](#) (Certification by Director of Board of Elections as to Political Party Affiliation of the Last Occupant of a County Office) to do so.

APPOINTING AUTHORITY'S DUTY

1. Generally

It is the duty of the entity entitled to appoint a person to a vacancy in office to determine what legal provisions apply to the appointment and to take the appropriate action. Examples of entities that have appointing authority under state law include, but are not limited to, a legislative authority of a municipal corporation, a village mayor, a board of township trustees, the county central committee of a political party, a school board, etc.

2. Notice of Appointment to Election Officials

When an elective office becomes vacant and is filled by appointment, the appointing authority shall immediately, but no later than seven days after making the appointment, certify it both to the board of elections and the Secretary of State.

The Secretary of State has prescribed a form, Certification by Party Central Committee to Fill a Vacancy in County Office or City Office ([Form 291](#)) that the appropriate committee of a political party may use to give notice to election officials that a vacancy in city or county office has been filled by appointment.

Other appointing authorities must prepare a written notice of an appointment and certify that notice to the board of elections.⁸

BOARD OF ELECTIONS POST-APPOINTMENT DUTIES

1. Issue Certificates of Appointments

The board of elections (or, in the case of an appointment to a statewide office, the Secretary of State) must issue a certificate of appointment to the appointee. Certificates of appointment shall be in the form prescribed by the Secretary of State, using [Form 155-B](#) (Certificate of Appointment to Fill Vacancy in Elective Office).⁹

⁸ [R.C. 302\(B\)](#).

⁹ [R.C. 302\(B\)](#).



2. Submit Documents and Fee for Governor's Commission

Persons appointed to any county office or to a judgeship also must receive a governor's commission before entering upon the duties of the office.¹⁰

The board of elections must collect from any person appointed to one of those offices the commission fee mandated by [R.C. 107.06](#). The fee for the commission is \$5, except in the case of county court judges¹¹ for whom it is \$2.

Note: "County court" is defined in [R.C. 1907.01](#). A court of common pleas is not the same as a "county court;" therefore, a judge of a court of common pleas pays the \$5 commission fee.

The board then sends to the Elections Division of the Office of the Secretary of State the following materials:

- the appropriate commission fee collected from the appointee, (checks are acceptable as long as the check is not issued to or signed by a board of elections' employee)
- the notice of appointment executed by the appointing authority,
- the certificate of appointment executed by the board of elections, and
- any other necessary documentation (for example, [Form 292](#), Certification by Director of Board of Elections as to Political Party Affiliation of the Last Occupant of a County Office, if applicable).

The Secretary of State's office will obtain a governor's commission for the appointee and mail it to the clerk of the court of common pleas in the county where the appointee lives. The clerk will deliver the commission to the appointee.¹²

Section 1.04 Recall or Removal from Office

Recall is the procedure that allows voters to decide whether to remove (recall) a municipal official holding elective office. The use of recall is significantly limited. First, it is available only in a municipality whose voters have adopted both 1) a form of limited home rule – that is, a charter or one of the plans of government outlined in [Chapter 705 of the Revised Code](#) – and 2) the recall process as part of that home rule government.¹³

¹⁰ [R.C. 107.05](#).

¹¹ [R.C. 1907.01](#).

¹² [R.C. 107.07](#).

¹³ *Lockhart v. Boberek* (1976), 45 Ohio St.2d 292; [R.C. 705.91-92](#).



Note: Recall is not available in a statutory municipality or in a limited home rule municipality that has not adopted the recall process. Additionally, recall is not available for state, township or district offices, or for county offices, except in a county that has adopted a limited home rule charter that specifically provides for the recall.

Additional details on the recall process may be found in the [Ohio Ballot Questions & Issues Handbook](#).

REMOVAL – ALL PUBLIC OFFICES

The General Provisions of the Revised Code provide that any person holding a public office in this state, or in any municipal corporation, county, or subdivision thereof, coming within the official classification in [Section 38 of Article II of the Ohio Constitution](#) may be removed by judicial action for good cause shown. In order to be removed from office, a public officer must be found guilty by a court of competent jurisdiction of misconduct in office for one or more of the following reasons:

- Willfully and flagrantly exercising authority or power not authorized by law.
- Refusing or willfully neglecting to enforce the law or to perform any official duty imposed upon the public officer by law.
- Gross neglect of duty.
- Gross immorality.
- Drunkenness.
- Misfeasance.
- Malfeasance.
- Nonfeasance.¹⁴

Additional details on initiating a judicial action for removal may be found in the [Ohio Ballot Questions & Issues Handbook](#).

¹⁴ [R.C. 3.07](#).



REMOVAL – PUBLIC OFFICIALS WITH FISCAL DUTIES

There are also provisions in Ohio law that provide for the removal of a person who holds a public office with fiscal duties. These public offices include: county auditors, county treasurers, township fiscal officers, village fiscal officers, village-clerk treasurers, village clerks, city auditors, city treasurers, and fiscal officers of chartered municipalities who have duties and functions similar to the city or village fiscal officers of statutory municipalities.¹⁵ A person holding one of these offices may be removed for:

1. Purposely, knowingly, or recklessly failing to perform a fiscal duty expressly imposed by law with respect to the fiscal duties of the office; or
2. Purposely, knowingly, or recklessly committing any act expressly prohibited by law with respect to the fiscal duties of the office.¹⁶

This type of removal is initiated by the filing of a sworn affidavit and evidence with the Auditor of State by a person or persons authorized by law to file such an affidavit and evidence. The person or persons authorized by law to file an affidavit and evidence are:

- The county treasurer or county commissioner against the county auditor;¹⁷
- A county commissioner or county auditor against the county treasurer;¹⁸
- Four residents of a township against a township fiscal officer;¹⁹ and
- A member of the legislative authority of a municipality against a village or city fiscal officer.²⁰

An individual with questions regarding this removal process might want to consult with private legal counsel, the county prosecuting attorney (for county and township officials), legal counsel for the municipality (for municipal officials), or the Office of the Auditor of State.

REMOVAL – MUNICIPAL OFFICER

Additionally, a judicial complaint can be filed against a municipal officer pursuant to [R.C. 733.72](#). This method for removal is available only when the municipal officer is receiving illegal compensation for services, has a private interest in a city contract, or is guilty of misfeasance or malfeasance in office.

¹⁵ [R.C. 319.26](#); [R.C. 321.37](#); [R.C. 507.13](#); [R.C. 733.78](#).

¹⁶ [R.C. 319.26\(A\)](#); [R.C. 321.37\(A\)](#); [R.C. 507.13\(A\)](#); [R.C. 733.78\(B\)](#).

¹⁷ [R.C. 319.26\(A\)](#).

¹⁸ [R.C. 321.37\(A\)](#).

¹⁹ [R.C. 507.13\(A\)](#).

²⁰ [R.C. 733.78\(B\)](#).



The complaint is filed with the probate judge of the county in which the municipality or the larger portion the municipality is located.

An individual with questions on removing a municipal officer under [R.C. 733.72](#) might want to consult with private legal counsel.

Section 1.05 Advisory Elections

An advisory election is a non-binding election on a question that municipal officials submit to the electorate to gauge voter attitudes on a particular topic. An advisory election is not intended as a substitute for the election on a municipal ordinance, resolution, charter amendment, or other measure. Rather, the advisory election only tests the appeal of the proposed legislation, with a second election on the legislation itself to follow, if municipal officials so choose.²¹

Please note that only a municipality may conduct an advisory election; an advisory election may not be held by any other political subdivision (e.g., state, county, township, school district, etc.).

When municipal officials certify an advisory question to the board of elections, the board should review the municipality's charter, if it has one, to determine whether the charter prohibits an advisory election. If the charter does not specifically prohibit an advisory election, the board should proceed with the election. If the charter appears to prohibit the advisory election, the board should consult with its legal counsel, the county prosecuting attorney.

The heading "Advisory Election" must be placed on the ballot for an advisory election.

Section 1.06 Voter File for Commissioner of Juries

On the date ordered by the common pleas court, the director of the board of elections shall prepare the current voter file for the county and file it with the commissioner of jurors.

The file compiled by the board of elections must include all electors registered in that county for the most recent general election regardless of active status (i.e., include voters in both active-active and active-confirmation status), except that the board of elections must remove from the file any elector who has not voted in at least one election during the preceding four calendar years. In addition, the list may not include any elector who has a confidential voter record under the Safe At Home program.²² The file layout must include only full name, registration address, and date of birth, unless

²¹ In *State ex rel. Bedford v. Cuyahoga Co. Board of Elections* (1991), 62 Ohio St.3d 17, the Court held that [Article XVIII, Section 3 of the Ohio Constitution](#) (commonly referred to as the "home rule" provision) grants a municipality the authority to hold an advisory election, absent a specific prohibition against holding such an election in the municipality's charter, the Ohio Revised Code, or the Ohio Constitution.

²² [R.C. 2313.06\(A\)\(1\)\(b\)](#); [R.C. 111.44](#).



additional information is specifically requested. The file should be transferred in as secure a manner as possible.

In the event that a board does not have a standard report that meets these statutory requirements, it must contact your county voter registration system vendor to create one.

Section 1.07 Precinct Election Official Evaluations

To ensure that the performance of precinct election officials (PEOs) can be fairly and consistently assessed, all boards of elections must adopt local performance standards along with uniform and non-discriminatory evaluation methods for their precinct election officials. Following are the minimum standards a board must use for monitoring and assessing the performance of their precinct election officials as a means to ensure the public that the precinct election officials have met the board's minimum standards in performing their duties for the public. These minimum standards also apply to those elections officials conducting in-person absentee voting.

OPENING AND CLOSING OF POLLING PLACES

- Did the polling location open and close on time;
- Did the PEOs print and appropriately sign a zero tape(s) and summary report(s);
- Did the PEOs sign the oath; and
- Did the PEOs open and close correctly the voting machines?

SELF-REPORTING OF PROBLEMS

- Did the PEOs follow required procedures for reporting any voting machine/device issues to the board, and
- Did the PEOs follow required procedures for reporting if/when the ballot supply ran low to the board?

HANDLING OF PROVISIONAL BALLOTS

- Did the PEOs issue properly provisional ballots to voters, including directing wrong-polling location voters to the correct location?

RECONCILIATION AFTER POLLS ARE CLOSED

- Did the PEOs complete their reconciliation duties, and
- Did the PEOs sign the reconciliation certification document?



Section 1.08 Election Administration Plans

Each board of elections is required to create an Election Administration Plan (EAP) prior to each even-numbered year general election and prior to each presidential primary election. The Secretary of State's office is providing an EAP template for use by each board of elections. To promote consistency in plan content and format among all 88 county boards of elections, each board **MUST** use this template when drafting its plan. Additional information beyond the categories in the template is acceptable, so long as the additional information is provided as an addendum and not commingled with the response to the template categories.

Detailed election administration planning is something that each board of elections should do prior to any election, not just federal elections. The EAP template pinpoints the most important election administration action-items for the board's consideration as it builds its plan to execute the election. The board should look at the EAP process not just as critical planning exercise, but also as an opportunity for continuous process improvements.

Each board must submit an EAP to the Secretary of State's office 60 days before each statewide presidential primary election and 120 days before each statewide general election in even-numbered years.

Below is an outline of the template that each board of elections must use when drafting its EAP. Adhering to the substance and format of this template ensures that counties are well-prepared to execute their elections administration duties.

The EAP must contain thirteen sections, organized as follows:

1. Precinct Election Official Recruitment, Training, and Accountability,
2. Resource Allocation,
3. Pre-Election Day and Election Day Communication Plan,
4. Materials,
5. Contingencies and Continuity Planning,
6. Security,
7. Voter Registration,
8. Absentee Ballots,
9. Polling Places and Accessibility,
10. Ballot Preparation,
11. Pre-Election Testing,



12. Reconciliation and Audits, and
13. Master Calendar.

Each board must submit this completed template as its EAP. A submission may include additional content, but must, at a minimum, include the items designated in the template. The response “not applicable” is unacceptable for any portion of the template.

The EAP must be signed by the board members, director, and deputy director and submitted to the Secretary of State’s office no later than 60 days before each statewide presidential primary election and 120 before each statewide general election in even-numbered years. The template containing an outline of the required content of the EAP will be provided to county boards of elections via email not later than 60 days prior to the deadline for submission to the Secretary of State’s office.

In order to assist this office with the processing of public records requests, each county must submit its EAP electronically, as one unrestricted PDF file. Additionally, each county must submit a second electronic file of the same document, also as an unrestricted PDF, with specified portions redacted as may be permitted under Ohio’s public records laws. Each redaction must cite to the relevant legal authority and be reviewed and approved by your county prosecuting attorney. This office will use the second, redacted electronic file to respond to public records requests for copies of an EAP.

Each county must send its EAP by email to elections@OhioSOS.gov.

Section 1.09 Voter Access to Public Information²³

Each board of elections must offer the following minimum look-up tools on its website:

VOTER REGISTRATION STATUS

This functionality must allow a voter to identify the address within the county at which the voter is registered to vote. A successful search result must offer a link to the Secretary of State’s Online Voter Registration System in the event the voter must update the voter’s registration address. An unsuccessful search (i.e., the voter cannot be found in the county’s voter file) must offer a link both to the voter registration form and the Secretary of State’s Online Voter Registration System. This search functionality must be available to voters throughout the year. Boards of elections must continue to ensure that registration updates made in the county voter registration system (e.g., new registrations, changes of name, changes of address, etc.) are promptly sent to the Statewide Voter Registration Database.

²³ The confidential voter record of a Safe at Home participant is not public record and may not be included in this lookup function. [R.C. 149.43\(A\)\(1\)\(ee\)](#).



ABSENTEE BALLOT STATUS

This functionality must allow all absentee voters in the county to identify the status of their absentee ballot from the date of application to the date the ballot was accepted for counting. Specifically, a successful search result must provide the voter with the following information:

- The date the voter's absentee application was approved;
- The date the voter's approved absentee application was processed by the board of elections (i.e., the date the board of elections mailed the ballot or otherwise issued it);
- The date the voter's voted absentee ballot was received by the board of elections; and
- The date the voter's voted absentee ballot was accepted for counting (or, if not accepted for counting, the reason it was determined to be ineligible for counting and the deadline by which the voter may correct any deficiency).

This search functionality must be available to voters beginning at least the 46th day before an election through the 35th day after that same election.

POLLING PLACE LOOKUP

This functionality must allow a voter to identify the correct polling location assigned to the voter based upon the address at which the voter is registered to vote. Optional functionality may offer a link to online directions (e.g., Google, MapQuest, etc.) from the voter's registration address to the address of the correct polling location assigned to the voter. This search functionality must be available to voters throughout the year. Boards of elections must continue to ensure that registration updates made in the county voter registration system (e.g., changes to precinct assignments or changes to polling location locations, addresses, names, etc.) are promptly sent to the Statewide Voter Registration Database.

SAMPLE BALLOT

This functionality must allow a voter to view and print the correct sample ballot assigned to the voter for the upcoming election based upon the address at which the voter is registered to vote. This search functionality must be available to voters beginning the 46th day before the election.

ADDITIONAL REQUIREMENTS

Because election information changes from time to time, it important that each board establish regular intervals by which the information necessary to populate the lookup



tools established above is updated. Any change to a voter's registration information or absentee ballot status must be reflected in the lookup tool each business day. Any changes to the location of a polling location or to a sample ballot must be reflected promptly in the lookup tool.

Boards of elections must make the necessary arrangements to ensure that the IT infrastructure supporting its website and these lookup tools, as well as the internet "path" to them, are sufficiently robust and stable to support the traffic during peak election periods. Boards of elections should procure the appropriate personnel and resources (e.g., county Automatic Data Processing board personnel and other county or elections IT staff, county voter registration system vendor, local internet service provider personnel, etc.) to ensure that the board's online presence is scaled and supported appropriately to meet presidential-year activity levels.

The voter information discussed here is derived from public records as defined in state law. However, each board of elections must take all necessary steps to ensure that industry-standard security protocols for its website and lookup tools are implemented and followed. Boards should procure the appropriate resources (see above) to do so.

Each board of elections' website must have these baseline online voter information access tools with the end user – the voter – in mind. Each board needs to evaluate the following:

- Are users easily able to find the correct site when using online search engines (e.g., Google, Yahoo!, etc.);
- Are users easily able to navigate within the board of elections' own website (e.g., are links clearly labeled, is the content organized, and does it use plain language whenever possible); and
- Is the information easily displayed using various platforms (i.e., PC vs. mobile; iPhone vs. Android; Internet Explorer vs. Chrome)?

Boards of elections must work to ensure that its website and these baseline online voter information access tools can be accessed effectively and used by voters with disabilities.