

## Best Practices for Election Technology



**U.S. Election Assistance Commission**  
 633 3<sup>rd</sup> Street NW, Suite 200 | Washington, DC 20001  
[www.eac.gov](http://www.eac.gov)

## Table of Contents

Table of Contents .....	1
Introduction .....	2
Overview .....	2
Cybersecurity .....	3
Physical Security.....	3
Unintentional Errors .....	4
Pre-Election.....	4
Voter Registration Database.....	4
Election Management System .....	6
In-Person Voting .....	9
Electronic Poll Books.....	9
Ballot Marking Devices & Direct Recording Electronic .....	12
Ballot Printing Systems .....	16
Precinct Count Scanners .....	17
Mailed Ballot & Central Count Tabulation.....	20
Central Count Scanners.....	20
Post-Election .....	23
Election Results Reporting .....	24
Conclusion.....	25
Additional Resources .....	25
Election Technology Security Measures Wheel.....	26
Election Technology Security Measures Chart .....	27



## Introduction

Congress established the U.S. Election Assistance Commission (EAC) through the passage of the Help America Vote Act (HAVA) in 2002. The EAC is an independent, bipartisan commission charged with developing guidance to meet HAVA voting requirements, adopting voluntary voting system guidelines, and serving as a national clearinghouse of information on election administration. The EAC also accredits testing laboratories, certifies voting systems, and audits the use of HAVA funds.

Technology has transformed American elections. Election officials of today act as Information Technology (IT) managers, which requires a unique set of attitudes, knowledge, and skills to plan, direct, and control contemporary election administration. This document provides an overview of best practices election officials use to secure the most common types of election technology before, during, and after elections.

## Overview

Election administration requires careful attention to security to maintain the integrity of the entire voting process. Election officials must develop and follow procedures to ensure the security of all components of the election process—from voter registration through final results certification.

Election technology is a broad term encompassing the databases, systems, and devices that support the ongoing operations of an elections office. This includes supportive technology, such as voter registration databases, e-poll books, and results reporting tools used to display unofficial results on elections websites. Election technology also encompasses voting systems, although voting systems themselves are more narrowly defined.

HAVA defines voting systems as “the total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment) that is used—

- to define ballots
- to cast and count votes
- to report or display election results
- to maintain and produce any audit trail information..."

Voting systems are more than voting machines. A system is a collection of unified components, that consist of subsystems, such as scanners, databases, and equipment necessary to count votes and produce election results. Voting systems may also import or export data from external systems using secured removable media.

Most states require voting systems to be certified. The EAC is responsible for testing and certifying voting systems at the federal level, while many states implement their own additional processes for certification. HAVA mandates that the EAC accredit voting system test laboratories and certify voting equipment. State participation in the EAC’s certification program is voluntary.

Each election jurisdiction is responsible for procuring, maintaining, and using their own election technology. Most jurisdictions rely on some form of paper ballot for voting, but the method used by



election officials to tabulate ballots ranges from a hand count of paper ballots to the use of fully electronic systems that record a vote directly on the device. For more information about election security preparedness, see: <https://www.eac.gov/election-officials/election-security-preparedness>.

## Cybersecurity

The cybersecurity of elections has never been more salient in the minds of election officials and voters. To ensure the integrity of the voting process, election officials develop procedures to monitor, detect, and recover from cyber-security incidents. There is no "one size fits all" for election security. However, election officials often use the following general best practices to enhance the overall security of election and voting system computers and electronic devices:

- Limiting the use of software to the very basic functions required to perform the election system's processes. It is a best practice not to install unauthorized applications or software programs to any component of a voting system, e-poll book, or other election systems.
- Ensuring that all systems are running the approved and correct versions of their software by using third-party tools to validate the hashes of the installed software. (Learn more about what has validations are and why election officials should care about them: <https://www.eac.gov/what-hash-validation-and-why-should-election-officials-care>)
- Periodically reviewing audit log information to track the sequence of events that occur on the system and, to the extent possible, identify the person(s) who initiated the events. This should be performed before, during, and after the election, to the extent possible. Election administrators should familiarize themselves with the process of reviewing audit log activity to identify and detect anomalous events more easily.
- Following proper procedures to ensure that all encryption keys are properly managed, including following all state, manufacturer, or IT department guidance and best practices. Well-defined policies and procedures should be used to control access to the voting system, the circumstances under which users can access the system, and the functions users are allowed to perform. These procedures should specify that all users utilize unique login names and passwords and that they are only authorized to perform the minimum functions required to complete their duties.
- Using a two-person accountability and control system, where possible. Access, control, and custody should involve two or more people, preferably from separate political affiliations.

In February 2021, the EAC adopted Voluntary Voting System Guidelines (VVSG) 2.0 to facilitate the replacement of equipment certified under decades-old standards, improve the voter experience, and provide necessary safeguards to protect the integrity of the voting process. All new voting systems certified to VVSG 2.0 will allow for an improved and consistent voter experience, improved security, increased auditability, and better accessibility features, among other improvements. VVSG 2.0 will ensure improved cryptographic protection of data and that security protections developed by experts over the past decade are built into all new certified voting systems.

## Physical Security

The physical security of elections relies on people, processes, and procedures to protect election and voting systems, related facilities and equipment from natural and environmental hazards, tampering,



vandalism, and theft. Physical security safeguards are required for voting systems while in storage, in transit, in the polling place, during voting, and through the post-election canvass and certification process. This includes maintaining strong chain of custody procedures and documentation, utilizing tamper-evident security seals, and limiting physical access. Election officials implement practical policies like two-person accountability, video monitoring, and access logging to promote the system's security.

Logging of actions taken during the election process, from ballot proofing to post-election audits, is the foundation for security in elections. Elections office staff and poll workers document actions taken throughout the election cycle to form an audit trail for each election. This audit trail serves as evidence that proper procedures were followed and provides important supporting evidence of the integrity of the election.

### Unintentional Errors

Election administration relies on complex manual processing of highly technical procedures, often with the assistance of temporary or voluntary poll workers. As complexity increases, so do the opportunities for administrative errors or mistakes throughout the voting process. Election officials put safeguards and procedures in place to prevent common errors, but occasionally mistakes will happen. When mistakes occur, election officials work to quickly remedy the situation, learn from the experience, and adjust procedures to prevent the same mistakes from occurring again in the future.

Properly communicating errors with the public will help election officials more quickly mitigate logistical issues while also providing voters with the information they need to successfully participate in the election. Communication is a critical piece of overall election security. The charts included throughout the document outline key topics that can be conveyed to the public to explain each security measure in detail.

Additionally, election officials should develop contingency plans, known as Continuity of Operations Plans (COOP), in the event errors or crises occur during an election. Having a contingency plan allows election officials to build resiliency and more quickly recover from emergencies. For more information about developing a COOP, see: <https://www.eac.gov/election-officials/contingency-planning>.

### Pre-Election

Administering an election begins months in advance with budgeting, planning, procurement, and securing of voting system components and other election technology. Election officials should have detailed policies outlining procedures that define who has access to systems and equipment, the roles and responsibilities of office staff, and contingency plans. Securing elections begins with securing the Voter Registration and Election Management databases.





#### Voter Registration Database


Voter Registration refers to the requirement for citizens to register with a state or local elections office to be eligible to receive an official ballot and to participate in certain election-related activities (including but not limited to signing petitions, serving as poll workers, and running for office). Every state and territory, except North Dakota, requires citizens to register if they want to vote.



Voter registration databases are either a distributed or centralized system that permits the collection, storage, editing, deletion, and reporting of voter records. The Help America Vote Act (HAVA) requires each state (with the exception of North Dakota) to have a centralized, statewide voter registration system. Voter registration databases have multiple interfaces and can interact with Department of Motor Vehicle (DMV) systems, election officials, voters, and other stakeholders. A voter registration database may be vendor-provided or “homegrown.” They may be client-server architecture or mainframe based.



**Best Practices for Securing Voter Registration Databases**





Risk	Security Measure	Communication
<p><b>Physical Access</b></p>	<p><b>Access Control</b>                      Physically secure the voter registration server(s) and user terminals within the election facility with log-in access including cameras, security alarms, and key-card locks. Routinely examine access logs and camera footage to ensure no unauthorized access.</p> 	<p><b>Explain</b> who has access</p> <p><b>Explain</b> security measures used to control access</p>
<p><b>Remote Access</b></p>	<p><b>Audit Logs</b>                       Information is recorded during election activities to track activities in the voter registration database. Routinely examine audit logs to ensure no unauthorized access or activities.</p> <p><b>Multi-Factor Authentication</b>                      Require a multi-layered authentication system when logging into the voter registration database. Multi-factor authentication requires a combination of two or more of: something you are (biometrics such as fingerprints or facial recognition), something you have (physical security token, smart card, etc.), and something you know (password/passphrase, PIN, etc.). Care should be taken to ensure that any of the factors are not susceptible to forgery.</p>  <p><b>Network Protections</b>                      Because voter registration databases are often accessed from computers that are connected to public networks, administrators should implement strong security controls such as data encryption, firewalls, intrusion detection, malware detection, regular patches, and other techniques to protect these systems from malicious activity.</p> 	<p><b>Keep</b> a record of audit findings and provide records when necessary</p> <p><b>Describe</b> the general types of systems that are used to monitor and detect unauthorized access</p> <p><b>Note:</b> It is a best practice not to publicly disclose information about the type of network protections used</p>

<p><b>Error Protection</b></p>	<p><b>Data Back-ups</b>                  Ensure that copies of the voter registration databases are routinely created (either automatically or manually) in case the working database is lost or compromised. Backup copies of the database should be stored outside of the system so that a compromise or failure of the system does not compromise the backups. Backups should be regularly tested to ensure that personnel understand how to restore the data, the backup procedure is capturing all necessary data, and that the process works as intended. Election officials also provide manual back-up procedures for loss of critical voting processes, including manually processing of voter registration if access to the database is lost or compromised. Develop Continuity of Operations Plans (COOP), to quickly recover in the event of an emergency.</p> 	<p><b>Provide</b> copies of the COOP upon request.</p>
--------------------------------	--	--





### Election Management System

Election Management Systems (EMS) are software running on Commercial Off-the-Shelf (COTS) computing hardware (desktop, laptop, server) that supports ballot generation and proofing, voting machine memory device programming, defining the parameters of the election, and programming corresponding election equipment. EMS systems may also support results tabulation and reporting, audio preparation for accessible voting, and other voting system functions.

Risk	Security Measure	Communication
<p><b>Physical Access</b></p>	<p><b>Access Control</b>                  Physically secure the EMS server(s) and user terminals within the election facility with log-in access including cameras, security alarms, and key-card locks. Routinely examine access logs and camera footage to ensure no unauthorized access.</p>  <p><b>Certification</b>                  Ensure that only approved, certified software is installed on all voting system components. Installed software that is not part of the certified configuration may cause unintended consequences and negatively impact the system's security.</p> 	<p><b>Explain</b> who has access</p> <p><b>Explain</b> security measures used to control access</p>

	<p><b>Hash Validation</b></p> <p>Hash validation is the process of comparing the original hash value of a piece of software to the current hash value. A hash value is a digital fingerprint created by performing a mathematical operation (a hash function) on the data comprising a computer program or other digital file. Any change in just one byte of the data comprising the computer program or digital file will change the hash value, causing it to fail validation and provide an important indicator that the file or program has been modified or the wrong version is installed.</p>  <p>Election officials can compare the hash values of the voting system software to the original, expected hash value to ensure that no data has been altered. It is important that original hash values are obtained from a trusted source.</p> <p><b>Multi-Factor Authentication</b></p> <p>Require a multi-layered authentication system when logging into the EMS. Multi-factor authentication requires a combination of two or more of: something you are (biometrics such as fingerprints or facial recognition), something you have (physical security token, smart card, etc.), and something you know (password/passphrase, PIN, etc.). Care should be taken to ensure that any of the factors are not susceptible to forgery.</p>  <p><b>Trusted Build</b></p> <p>For a new or updated EMS, ensure the software is loaded from a trusted source. Trusted builds are created by validating the source of each component of the system prior to being bundled together in an installer and ensure authenticity.</p> 	
<p><b>Remote Access</b></p>	<p><b>Air-Gap</b></p> <p>The use of single-use memory devices to transfer election results from the voting system tabulator to EMS and that EMS to the elections office’s website is an example of an air gap. It is important to use removable media from a trusted source to ensure that malware has not been pre-loaded on the device. Additionally, write-once or read-only removable media should be used, where possible, to ensure</p> 	<p><b>Keep</b> a record of audit findings and provide records when necessary</p> <p><b>Describe</b> the general types of systems that are used to monitor and</p>



	<p>that files are not modified. If a USB drive or other piece of writable removable media is inserted into a device that is connected to the internet, another network, or is outside of the voting system, it should not be reused without ensuring that it is free of malware. This procedure ensures the voting system remains disconnected, while allowing results to be displayed online.</p> <p><b>Audit Logs</b> Information is recorded to track activities in the EMS.</p> <p> Routinely examine audit logs to ensure no unauthorized access or actions have taken place.</p> <p><b>No Internet Connection</b> Ensure the EMS is not connected to the Internet or other external networks to avoid the potential for unauthorized access and reduce the threats the system may face.</p> <p></p> <p><b>One-Time Use Media</b> When transferring results from an Election Management System to a computer connected to the internet, election officials should only use write-once media such as a properly formatted CD-ROM or single-use USB drives. Alternatively, officials may employ an intermediary solution that ensures a device is clean before inserting it back into the EMS.</p> <p></p>	<p>detect unauthorized access</p> <p><b>Note:</b> It is a best practice not to publicly disclose information about the type of network protection used</p>
<p><b>Error Protection</b></p>	<p><b>Data Back-ups</b> Ensure that copies of EMS databases are routinely created (either automatically or manually) in case the working database is lost or compromised. Backup copies of the database should be stored outside of the system so that a compromise or failure of the system does not compromise the backups. Backups should be regularly tested to ensure that personnel understand how to restore the data, the backup procedure is capturing all necessary data, and that the process works as intended. Election officials also provide manual back-up procedures for loss of critical voting processes, including manually processing of voter registration if access to the database is lost or compromised. Develop Continuity of Operations Plans (COOP), to quickly recover in the event of an emergency.</p> <p></p>	<p><b>Provide</b> copies of the COOP upon request.</p>

## In-Person Voting

The use of technology in polling places varies widely across and within states. HAVA requires at least one accessible voting device in each voting location for use in federal elections. Most jurisdictions and states use more than one type of electronic equipment for in-person voting.

Each state will have their own laws and procedures for delivering, securing, and monitoring election equipment for in-person voting at polling places or voting locations. Some larger items, such as ballot marking devices, printers, direct electronic recording machines, and scanners may be delivered to polling places or voting locations prior to Election Day. Poll workers may bring some items, such as e-poll books, to and from the polling place or voting location. For each item, chain of custody documentation provides a record that all election procedures were followed and that security was maintained.

In jurisdictions that utilize precinct count scanners, votes are recorded on removable media during the voting period. Election workers secure and transport removable media to a central location for election officials to upload into the vote tabulation system. For more information about securing the chain of custody of election materials to and from voting locations, see:

[https://www.eac.gov/sites/default/files/bestpractices/Chain\\_of\\_Custody\\_Best\\_Practices.pdf](https://www.eac.gov/sites/default/files/bestpractices/Chain_of_Custody_Best_Practices.pdf).

## Electronic Poll Books


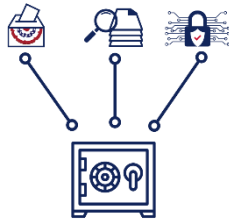


In most polling places, the identity of each voter is checked against voter registration information contained in poll books to ensure voters are registered to vote and did not already cast a ballot during in-person early voting or by using a mailed ballot. Electronic poll books (e-poll books) are devices that partially automate the process of checking in voters, assigning them the correct ballot style, and marking voters who have been issued a ballot. E-poll books may be used in place of a traditional paper poll book. E-poll books can be stand alone at the precinct with a separate copy of the registration list or can be networked into a central voter registration system where they can check and update voter records in real time.





What constitutes an e-poll book varies by jurisdiction. Some e-poll books include peripherals such as signature pads, identification card swipe or barcode scanning of a driver license, state-issued nondriver identification card, or coded voter registration card to facilitate the check-in process, which may require additional security measures beyond the scope of this document.




Since e-poll books range from in-house built to vendor supported systems, the security principals outlined below may not be applicable in all jurisdictions.



Best Practices for Securing E-Poll Books

Risk	Security Measure	Communication
<p><b>Physical Access</b></p>	<p><b>Access Control</b>                      Physically secure the e-poll books, server(s), and user terminals within the election facility with log-in access including cameras, security alarms, and key-card locks. Routinely examine access logs and camera footage to ensure no unauthorized access.</p>  <p><b>Chain of Custody</b>                      Develop controls for ensuring the chain of custody of e-poll books is properly maintained. These controls may include locks, seals, audit logs, witness signatures, or other security measures.</p>  <p><b>Hash Validation</b>                      Hash validation is the process of comparing the original hash value of a piece of software to the current hash value. A hash value is a digital fingerprint created by performing a mathematical operation (a hash function) on the data comprising a computer program or other digital file. Any change in just one byte of the data comprising the computer program or digital file will change the hash value, causing it to fail validation and provide an important indicator that the file or program has been modified or the wrong version is installed.</p>  <p>Election officials can compare the hash values of the e-poll book software to the original, expected hash value to ensure that no data has been altered. It is important that original hash values are obtained from a trusted source.</p> <p><b>Pre-election Testing</b>                      Perform in-depth system readiness tests to detect malfunctioning devices and improper election-specific setup before e-poll books are used in an election. Test the date &amp; time functions, ensuring the date and time are correct, the ability to check in all types of</p> 	<p><b>Explain</b> who has access</p> <p><b>Explain</b> security measures used to control access</p> <p><b>Explain</b> logic &amp; accuracy procedures</p>

	<p>voters, and the ability to issue every ballot style for the voting location, if e-poll books are used to authorize ballot cards. If ballot cards are used, test these cards with a voting device.</p> <p>Conduct tests prior to the start of an election as part of the process of setting up the system and the devices for an election according to jurisdiction practices and conforming to any state laws.</p> <p><b>Tamper-Evident Seals</b> Apply tamper-evident seals that will detect if the e-poll book has been tampered with.</p>  <p><b>Two Person Rule</b> At least two persons (preferably from different parties) work together to program and test e-poll books; reconcile the number of voters checked in; and complete the chain of custody for e-poll books.</p> 	
<p><b>Remote Access</b></p>	<p><b>Audit Logs</b> Information is recorded during election activities to track activities in e-poll books. Examine audit logs as needed to ensure no unauthorized access or unauthorized activities.</p>  <p><b>Multi-Factor Authentication</b> Require a multi-layered authentication system when logging into the e-poll book system. Multi-factor authentication requires a combination of two or more of: something you are (biometrics such as fingerprints or facial recognition), something you have (physical security token, smart card, etc.), and something you know (password/passphrase, PIN, etc.). Care should be taken to ensure that any of the factors are not susceptible to forgery.</p> 	<p><b>Keep</b> a record of audit findings and provide records when necessary</p> <p><b>Describe</b> the general types of systems that are used to monitor and detect unauthorized access</p> <p><b>Note:</b> It is a best practice not to publicly disclose information about the type of network protection used</p>

	<p><b>Network Protections</b></p> <p>Because e-poll books are often accessed from computers that are connected to public networks, administrators should implement strong security controls such as data encryption, firewalls, intrusion detection, malware detection, regular patches, and other techniques to protect these systems from malicious activity.</p> 	
<p><b>Error Protection</b></p>	<p><b>Paper Back-ups</b></p> <p>Ensure that paper copies of poll books are available in case e-poll books are not working properly or are compromised, as authorized by state law. Develop procedures to switch to paper pollbooks if e-poll books are not working properly or become unusable.</p>  <p><b>Train Poll Workers</b></p> <p>Train poll workers on the procedures to switch to paper back-ups, including what circumstances would require using the paper back-up and how to document incidents.</p> 	<p><b>Provide</b> copies of training materials and procedures upon request</p>






### Ballot Marking Devices & Direct Recording Electronic

A ballot marking device (BMD) allows voters to use a touch screen or accessible device to mark their ballot. To begin the voting session, the ballot is “activated” by scanning a barcode, entering a code, inserting a pre-programmed smart card containing the voter’s ballot style information, or inserting an unmarked ballot. The BMD can be programmed to reduce potential voting mistakes, such as voting for more candidates or choices than allowed (overvoting) and can facilitate voting options such as straight party voting. After the voter marks their ballot and confirms their selections, it is printed and placed in a ballot box or precinct count scanner. BMDs do not store or tally votes. Some BMDs print paper ballots containing machine-readable markings such as bar or QR (Quick Response) codes. Others will print full-face ballots identical to hand-marked paper ballots.

Direct Recording Electronic (DRE) voting machines, like BMDs, allow voters to mark their ballot using a touch screen, electronic interface, or accessible device. The primary difference between a DRE and a BMD is that DREs store the vote within the machine on removable memory and tabulate vote totals. Most DREs utilize a Voter Verifiable Paper Audit Trail (VVPAT) that allows voters to confirm their votes and poll workers to audit results without relying solely on the electronically stored results.

A hybrid tabulator combines a BMD with a precinct scanner. Hybrid tabulators may use either blank ballot stock or pre-printed ballots with target areas that are marked during the voting session.

Best Practices for Securing BMDs & DREs

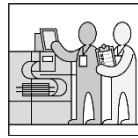
Risk	Security Measure	Communication
<p><b>Physical Access</b></p>	<p><b>Access Control</b>                      Physically secure the facility storing BMDs and DREs with log-in access including cameras, security alarms, and key-card locks. Routinely examine access logs and camera footage to ensure no unauthorized access.</p>  <p><b>Audit Logs</b>                      Information is recorded during voting to track use of BMDs and DREs, including public and private counts of votes cast using the device. Examine audit logs prior to authorizing voting each day and reconcile audits logs at the end of voting each night to ensure no unauthorized access or other abnormalities.</p>  <p><b>Certification</b>                      Ensure that only approved, certified software is installed on all voting system components. Installed software that is not part of the certified configuration may cause unintended consequences and negatively impact the system's security.</p>  <p><b>Chain of Custody</b>                      Develop controls for ensuring the chain of custody of BMDs and DREs are properly maintained. These controls may include locks, seals, audit logs, witness signatures, or other security measures.</p>  <p><b>Hash Validation</b>                      Hash validation is the process of comparing the original hash value of a piece of software to the current hash value. A hash value is a digital fingerprint created by performing a mathematical operation (a hash function) on the data comprising a computer program or other digital file. Any change in just one byte of the data comprising the computer program or digital file will change the hash value,</p> 	<p><b>Explain</b> who has access</p> <p><b>Explain</b> security measures used to control access</p> <p><b>Explain</b> logic &amp; accuracy procedures</p> <p><b>Keep</b> a record of audit logs and provide records when necessary</p>

causing it to fail validation and provide an important indicator that the file or program has been modified or the wrong version is installed.

Election officials can compare the hash values of the voting system software to the original, expected hash value to ensure that no data has been altered. It is important that original hash values are obtained from a trusted source.

### Logic & Accuracy Pre-election Testing

Perform in-depth system readiness tests to detect



malfunctioning devices and improper election-specific setup before BMDs or DREs are used in an election. Test the date & time functions, the ability to vote every ballot style for the voting location, and that votes for every contest tabulate correctly.

### Multi-Factor Authentication

Require a multi-layered authentication system when



accessing administrator functions. Multi-factor authentication requires a combination of two or more of: something you are (biometrics such as fingerprints or facial recognition), something you have (physical security token, smart card, etc.), and something you know (password/passphrase, PIN, etc.). Care should be taken to ensure that any of the factors are not susceptible to forgery.

### Tamper-Evident Seals

Apply tamper-evident seals that will detect if the BMD or DRE has been tampered with, in accordance with state law.







### Two Person Rule

At least two persons (preferably from different parties)



work together to program and test BMDs and DREs; physically transfer, start up, shut down, and store BMDs or DREs; and complete the chain of custody for BMDs or DREs.






<p><b>Remote Access</b></p>	<p><b>Air-Gap</b>                  The use of single-use memory devices to transfer election results from the DREs to the EMS and then from the EMS to the elections office’s website is an example of an air gap. It is important to use removable media from a trusted source to ensure that malware has not been pre-loaded on the device. Additionally, write-once or read-only removable media should be used, where possible, to ensure that files are not modified. If a USB drive or other piece of writable removable media is inserted into a device that is connected to the internet, another network, or is outside of the voting system, it should not be reused without ensuring that it is free of malware. This procedure ensures the voting system remains disconnected, while allowing results to be displayed online.</p>  <p><b>No Internet Connection</b>                  Ensure the BMDs or DREs are not connected to the Internet or other external networks to avoid the potential for unauthorized access and reduce the threats the system may face.</p> 	<p><b>Explain</b> procedures to ensure that BMDs and DREs are not connected to the internet</p>
<p><b>Error Protection</b></p>	<p><b>Paper Back-ups</b>                  Ensure that there are enough paper ballot back-ups in case BMDs or DREs are not working properly or are compromised, as authorized by state law. Develop procedures to switch to paper ballots in the event that BMDs are not working properly or become unusable.</p>  <p><b>Train Poll Workers</b>                  Train poll workers on the procedures to switch to paper ballots, including what circumstances would require using the paper ballots and how to document incidents.</p>  <p>Train poll workers to instruct voters to review printed BMD ballots and DRE VVPAT printouts before casting their ballots. Include how to spoil incorrect ballots and track which device produced the spoiled ballot.</p>	<p><b>Provide</b> copies of training materials and procedures upon request</p> <p><b>Educate</b> voters on the importance of the paper ballot and its accuracy, including that it is the official record of their vote and used in any audits or recounts.</p>





## Ballot Printing Systems

Ballot printers are connected to devices (e.g., desktop computer, laptop, or tablet) that print individual ballots for voters at a voting location and may integrate with e-poll books. These systems are also known as ‘Ballot on Demand’ (BOD).

### Best Practices for Securing Ballot Printing Systems



Risk	Security Measure	Communication
<p><b>Physical Access</b></p>	<p><b>Access Control</b>                      Physically secure the ballot printing systems within the election facility with log-in access including cameras, security alarms, and key-card locks. Routinely examine access logs and camera footage to ensure no unauthorized access.</p>  <p><b>Chain of Custody</b>                      Develop controls for ensuring the chain of custody of ballot printing systems are properly maintained. These controls may include locks, seals, audit logs, witness signatures, or other security measures.</p>  <p><b>Pre-election Testing</b>                      Test each system during the Logic &amp; Accuracy test to detect malfunctioning devices.</p>  <p><b>Tamper-Evident Seals</b>                      Apply tamper-evident seals that will detect if the ballot printing system has been tampered with, in accordance with state law.</p> 	<p><b>Explain</b> who has access</p> <p><b>Explain</b> security measures used to control access</p> <p><b>Explain</b> logic &amp; accuracy procedures</p>
<p><b>Remote Access</b></p>	<p><b>No Internet Connection</b>                      Ensure the ballot printing system is not connected to the Internet or other external networks to avoid the potential for unauthorized access and reduce the threats the system may face.</p> 	<p><b>Explain</b> procedures to ensure that ballot printing systems do not have remote access capabilities</p>

<p><b>Error Protection</b></p>	<p><b>Hand-Marked Paper Back-ups</b>                  Ensure that there are enough pre-printed paper ballot back-ups in case ballot printing systems are not working properly, as authorized by state law. Develop procedures to switch to pre-printed paper ballots if ballot printing systems are not working properly, lose power, or become unusable.</p>  <p><b>Train Poll Workers</b>                  Train poll workers on the procedures to switch to pre-printed paper ballots, including what circumstances would require using the pre-printed paper ballots and how to document incidents.</p> 	<p><b>Provide</b> copies of training materials and procedures upon request</p>
--------------------------------	--	--

### Precinct Count Scanners

Precinct scanners are devices that read individual ballot cards fed one-by-one by voters (or poll workers assisting voters) in a polling place or voting location. In many jurisdictions, the scanners provide feedback to voters about any detected errors on the ballot (overvote, undervote, blank ballot) to allow the voter to make corrections. Most precinct scanners also tabulate votes and store the Cast Vote Records (CVRs) on removable media such as a USB flash drive or Compact Flash card. Ballots are typically dropped into an attached secure ballot box after scanning and tabulation. The scanner may contain a diverter that allows for the separation of ballots into separate compartments for ballots that require further review, such as those containing completed write-in contests.

### Best Practices for Precinct Scanners

Risk	Security Measure	Communication
<p><b>Physical Access</b></p>	<p><b>Access Control</b>                  Physically secure the facility that stores precinct scanners with log-in access including cameras, security alarms, and key-card locks. Routinely examine access logs and camera footage to ensure no unauthorized access.</p>  <p><b>Audit Logs</b>                  Information is recorded during voting to track use of precinct scanners, including public and private counts of ballots cast using the device. Examine audit logs prior to authorizing voting each day and reconcile audits logs at the end of voting each</p> 	<p><b>Explain</b> who has access</p> <p><b>Explain</b> security measures used to control access</p> <p><b>Explain</b> logic &amp; accuracy procedures</p> <p><b>Keep</b> a record of audit logs and</p>

night to ensure no unauthorized access or other abnormalities.

provide records when necessary

**Certification**

Ensure that only approved, certified software is installed on all voting system components. Installed software that is not part of the certified configuration may cause unintended consequences and negatively impact the system’s security.



**Chain of Custody**

Develop controls for ensuring the chain of custody of precinct scanners is properly maintained. These controls may include locks, seals, audit logs, witness signatures, or other security measures.



**Hash Validation**

Hash validation is the process of comparing the original hash value of a piece of software to the current hash value. A hash value is a digital fingerprint created by performing a mathematical operation (a hash function) on the data comprising a computer program or other digital file. Any change in just one byte of the data comprising the computer program or digital file will change the hash value, causing it to fail validation and provide an important indicator that the file or program has been modified or the wrong version is installed.



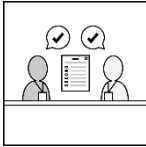






Election officials can compare the hash values of the voting system software to the original, expected hash value to ensure that no data has been altered. It is important that original hash values are obtained from a trusted source.

**Pre-election Testing**

Perform in-depth system readiness tests to detect malfunctioning devices and improper election-specific setup before precinct scanners are used in an election. Test the



	<p>date &amp; time functions, the ability to scan every ballot style and vote position for the voting location.</p> <p><b>Multi-Factor Authentication</b> Require a multi-layered authentication system when accessing administrator functions. Multi-factor authentication requires a combination of two or more of: something you are (biometrics such as fingerprints or facial recognition), something you have (physical security token, smart card, etc.), and something you know (password/passphrase, PIN, etc.). Care should be taken to ensure that any of the factors are not susceptible to forgery.</p>  <p><b>Tamper-Evident Seals</b> Apply tamper-evident seals that will detect if the precinct scanner has been tampered with, in accordance with state law.</p>  <p><b>Two Person Rule</b> At least two persons (preferably from different parties) work together to program and test scanners; physically transfer, start up, shut down, and store scanners; and complete the chain of custody for precinct scanners.</p> 	
<p><b>Remote Access</b></p>	<p><b>Air-Gap</b> The use of single-use memory devices to transfer election results from the voting system tabulator to EMS and that EMS to the elections office's website is an example of an air gap. It is important to use removable media from a trusted source to ensure that malware has not been pre-loaded on the device. Additionally, write-once or read-only removable media should be used, where possible, to ensure that files are not modified. If a USB drive or other piece of writable removable media is inserted into a device that is connected to the internet, another network, or is outside of the voting system, it should not be reused without ensuring that it is free of malware. This procedure ensures the voting system remains disconnected, while allowing results to be displayed online.</p> 	<p><b>Explain</b> procedures to ensure that precinct scanners are not connected to the internet</p>

	<p><b>No Internet Connection</b> Ensure precinct scanners are not connected to the Internet or other external networks to avoid the potential for unauthorized access and reduce the threats the system may face.</p> 	
<b>Error Protection</b>	<p><b>Back-up Secure Ballot Box</b> Ensure that there is a back-up secure ballot box for storing voted ballots in case the precinct scanner is not working properly or is compromised, as authorized by state law. Develop procedures to switch to the back-up secure ballot box in case the precinct scanner is not working properly, loses power, or becomes otherwise unusable.</p>  <p><b>Train Poll Workers</b> Train poll workers on the procedures to switch to a back-up secure ballot box, including what circumstances would require using the back-up secure ballot box and how to document the process.</p> 	<b>Provide</b> copies of training materials and procedures upon request

## Mailed Ballot & Central Count Tabulation





Some jurisdictions tabulate all ballots in a central counting location. At the polling location voters cast their ballots by depositing them into secure ballot boxes, which are then transported to the central counting location to be tabulated.






Ballots cast by mail are typically tabulated using central count scanners, after they have been received, verified as valid, and accepted for counting.



### Central Count Scanners

Most central count scanners read batches of ballots fed in stacks by election workers. Central count scanners often scan at high speed, typically at a rate of 60-400 ballots per minute. Some central count scanners provide a mechanism to physically outstack ballots that require further review (e.g., blank ballots, ballots with write-ins, overvoted ballots, etc.). Others provide digital outstacking that segregates scanned ballot images electronically. Central count scanners can run as stand-alone tabulators that store CVRs and, optionally, ballot images to removable media. More frequently, central count scanners are networked together and store their results in a central location—either on, or accessible by, an associated election management system or a separate tally and reporting system.

Best Practices for Central Count Scanners

Risk	Security Measure	Communication
<p><b>Physical Access</b></p>	<p><b>Access Control</b>                      Physically secure the facility storing central count scanners with log-in access including cameras, security alarms, and key-card locks. Routinely examine access logs and camera footage to ensure no unauthorized access.</p>  <p><b>Audit Logs</b>                      Information about tabulation is recorded and tracked through audit logs when using central count scanners. Routinely examine audit logs to ensure no unauthorized access or other abnormalities.</p>  <p><b>Certification</b>                      Ensure that only approved, certified software is installed on all voting system components. Installed software that is not part of the certified configuration may cause unintended consequences and negatively impact the system's security.</p>  <p><b>Hash Validation</b>                      Hash validation is the process of comparing the original hash value of a piece of software to the current hash value. A hash value is a digital fingerprint created by performing a mathematical operation (a hash function) on the data comprising a computer program or other digital file. Any change in just one byte of the data comprising the computer program or digital file will change the hash value, causing it to fail validation and provide an important indicator that the file or program has been modified or the wrong version is installed.</p>  <p>Election officials can compare the hash values of the voting system software to the original, expected hash value to ensure that no data has been altered. It is important that original hash values are obtained from a trusted source.</p>	<p><b>Explain</b> who has access</p> <p><b>Explain</b> security measures used to control access</p> <p><b>Explain</b> logic &amp; accuracy procedures</p> <p><b>Keep</b> a record of audit logs and provide records when necessary</p>

	<p><b>Pre-election Testing</b>                  Perform in-depth system readiness tests to detect malfunctioning devices and improper election-specific setup before central count scanners are used in an election. Test the ability to scan and tally every ballot style, including the ability to separate and adjudicate ballots with write-ins or other special conditions such as blank ballots or overvotes.</p>  <p><b>Multi-Factor Authentication</b>                  Require a multi-layered authentication system when logging into the central count scanner. Multi-factor authentication requires a combination of two or more of: something you are (biometrics such as fingerprints or facial recognition), something you have (physical security token, smart card, etc.), and something you know (password/passphrase, PIN, etc.). Care should be taken to ensure that any of the factors are not susceptible to forgery.</p>  <p><b>Tamper-Evident Seals</b>                  Apply tamper-evident seals that will detect if the central count scanners have been tampered with, in accordance with state law.</p>  <p><b>Two Person Rule</b>                  At least two persons (preferably from different parties) work together to program, test scanners, start up, scan ballots, shut down, and store scanners.</p> 	
<p><b>Remote Access</b></p>	<p><b>Air-Gap</b>                  The use of single-use memory devices to transfer election results from the voting system tabulator to EMS and that EMS to the elections office's website is an example of an air gap. It is important to use removable media from a trusted source to ensure that malware has not been pre-loaded on the device. Additionally, write-once or read-only removable media should be used, where possible, to</p> 	<p><b>Explain</b> procedures to ensure that central count scanners are not connected to the internet</p>

	<p>ensure that files are not modified. If a USB drive or other piece of writable removable media is inserted into a device that is connected to the internet, another network, or is outside of the voting system, it should not be reused without ensuring that it is free of malware. This procedure ensures the voting system remains disconnected, while allowing results to be displayed online.</p> <p><b>No Internet Connection</b> Ensure the central count scanners are not connected to the</p>  <p>Internet or other external networks to avoid the potential for unauthorized access and reduce the threats the system may face.</p>	
<b>Error Protection</b>	<p><b>Post-Election Audits</b> A post-election tabulation audit involves hand-counting a</p>  <p>sample of votes on paper records, then comparing those counts to the corresponding vote totals originally reported. This type of audit serves as a check on the accuracy of election results, and to detect discrepancies using accurate hand-counts of the paper records as the benchmark.</p> <p>A post-election procedural audit, often referred to as procedural, performance, process, or compliance audits, determines if election procedures were followed. These audits include ensuring that forms were signed, vote tabulation equipment was tested, ballot materials were securely sealed, and the custody of critical election materials was documented.</p>	<b>Explain</b> post-election audit procedures

## Post-Election

An election is not complete after the polls close on Election Day. There are several steps election officials must complete before they certify election results. The method, scope, and timing of post-election activities vary by state. Most states require a canvass, which is the process where election officials reconcile the number of ballots cast with the number of voters and ensure that the final results include every valid vote. The majority of states also require a post-election tabulation audit to verify voting equipment used during an election accurately counted ballots cast. The timing, scope, and associated security measures of post-election activities vary among states. For more information about post-election activities, including audits, the canvass, and certification see:





<https://www.eac.gov/election-officials/election-results-canvass-and-certification>.




## Election Results Reporting

Election results are usually shared with the public through an official website or social media platforms. However, election results are unofficial until certified.

### Best Practices for Securing Election Results Reporting

Risk	Security Measure	Communication
<b>Physical Access</b>	<p><b>Access Control</b> Physically secure the election facility with log-in access including cameras, security alarms, and key-card locks. Routinely examine access logs and camera footage to ensure no unauthorized access. Physical security access should extend to facilities used to host web servers that allow the results to be shared with the public but are not included in the definition of a voting system.</p>  <p><b>Multi-Factor Authentication</b> Require a multi-layered authentication system when logging into the results reporting website and social media platforms. Multi-factor authentication requires a combination of two or more of: something you are (biometrics such as fingerprints or facial recognition), something you have (physical security token, smart card, etc.), and something you know (password/passphrase, PIN, etc.). Care should be taken to ensure that any of the factors are not susceptible to forgery.</p> 	<p><b>Explain</b> who has access</p> <p><b>Explain</b> security measures used to control access</p>
<b>Remote Access</b>	<p><b>Cybersecurity Protections</b> Election officials can use the <a href="#">Checklist for Securing Election Night Results Reporting</a> as a baseline to assess their current Election Night Reporting cybersecurity protocols. Most importantly, any physical media used to transport results from the voting system to the election night results reporting system should either be single-use or sanitized before they are used again within the voting system.</p>  <p><b>Social Media Verification</b> Attain verified status on social media platforms to increase trust that social media accounts are official.</p> 	<p><b>Describe</b> the general types of systems that are used to monitor and detect unauthorized access</p> <p><b>Note:</b> It is a best practice not to publicly disclose information about the type of network protections used</p>

<p><b>Error Protection</b></p>	<p><b>Contingency Planning</b>  Election officials should develop a detailed plan for communicating election night results, detailing how election results will be shared throughout the election, including a timeline of election results updates and which ballots are expected to be included in each report (I.e., early voting, by-mail, and absentee, Election Day provisional, write-in votes, etc.). The plan should include information about how the public can access results if results reporting websites or social media platforms are not operating as expected, or if they are rendered inoperable due to a power outage, cyber incident, or any other technical failure. Contingency plans should identify threats and establish an action plan. Contingency plans can be tested using tabletop or similar exercises.</p> 	<p><b>Provide</b> copies of the COOP upon request.</p>
--------------------------------	---	--

## Conclusion

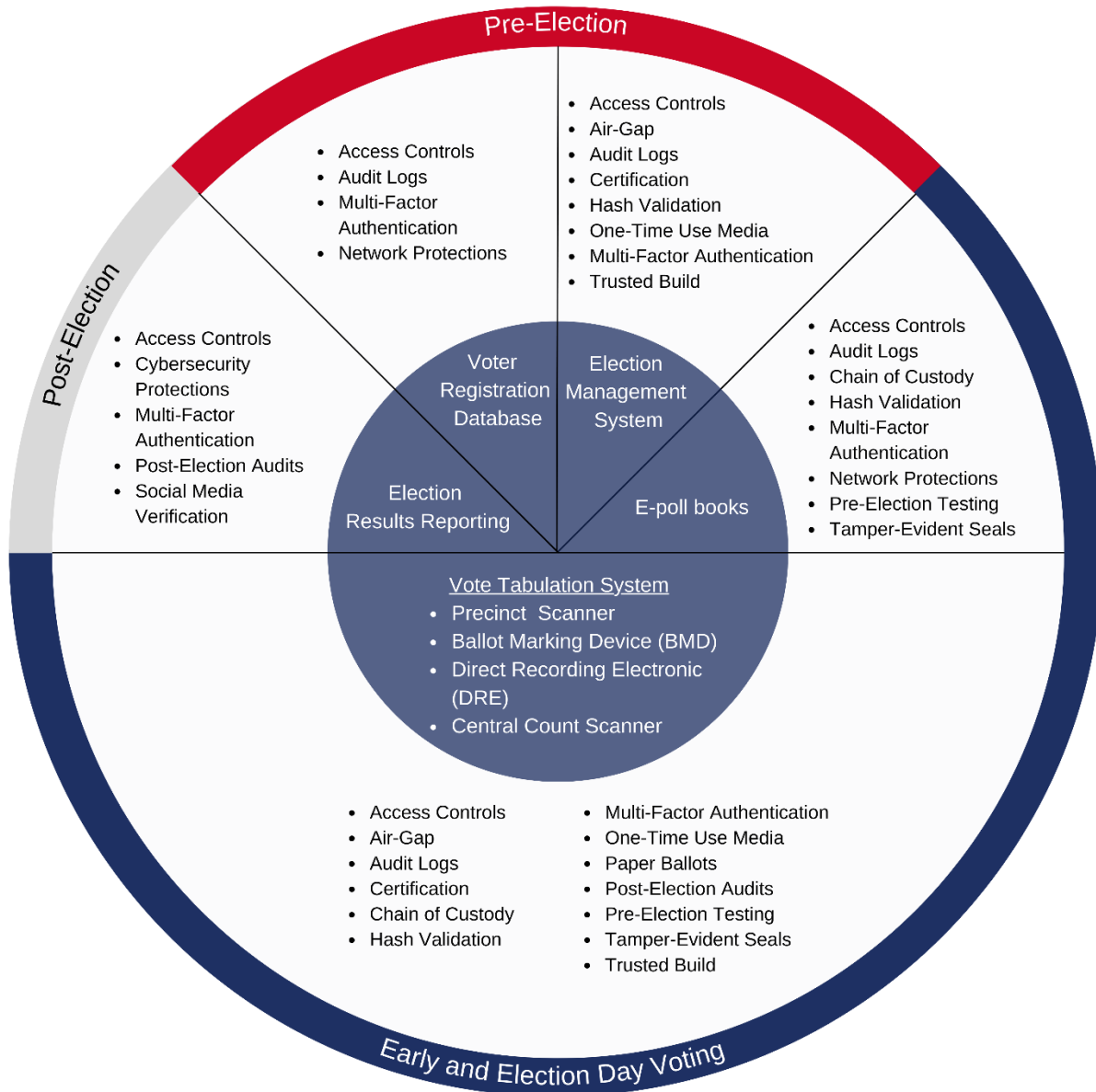
Advances in technology can benefit both election officials and voters. There is a large and growing body of knowledge about emerging trends in election administration and the risks and threats of using technology in elections and voting. Election officials weigh the security, accessibility, auditability, usability, voter convenience, transparency of process, and testing and certification practices to set priorities and to manage risk mitigation.

## Additional Resources

- EAC Chain of Custody Best Practices: <https://www.eac.gov/election-officials/chain-custody-best-practices>
- EAC Security Preparedness Resources: <https://www.eac.gov/election-officials/election-security-preparedness>
- Cybersecurity and Infrastructure Security Agency (CISA) Security Resources for the Election Infrastructure Subsector: [https://www.eac.gov/sites/default/files/electionofficials/security/security\\_resources\\_election\\_subsector\\_508\\_CISA\\_FBI.pdf](https://www.eac.gov/sites/default/files/electionofficials/security/security_resources_election_subsector_508_CISA_FBI.pdf)
- CISA Cybersecurity Toolkit to Protect Elections: <https://www.cisa.gov/cybersecurity-toolkit-protect-elections>
- Center for Internet Security (CIS) Handbook for Election Infrastructure Security: <https://docs.cisecurity.org/en/latest/index.html>
- Department of Homeland Security Resources for Election Security: <https://www.dhs.gov/topics/election-security>



## Election Technology Security Measures Wheel



## Election Technology Security Measures Chart

Type	Tamper Evident Seals/Locks	Air-gap	Hash Validation	Multi-factor authentication	Audit logging	EAC Certification
<b>Voter Registration Database</b>	N/A	No	No	Yes	Yes	No
<b>Election Management System</b>	No	Yes	Yes	Yes	Yes	Yes
<b>E-Poll books</b>	Yes	From Voting System	Mixed	Yes	Yes	Pilot Program
<b>Precinct Scanner</b>	Yes	Yes	Yes	Mixed	Yes	Yes
<b>BMD</b>	Yes	Yes	Yes	Yes	Yes	Yes
<b>DRE</b>	Yes	Yes	Yes	Mixed	Yes	Yes
<b>Central Scanner</b>	No	Yes	Yes	Yes	Yes	Yes

