Voluntary Electronic Ballot Delivery Requirements VEBDR v0.9

June 3rd, 2025

U.S. Election Assistance Commission

Prepared by the ***Election Supporting Technology Evaluation Program***

Executive Summary

The United States Congress passed the Help America Vote Act of 2002 (HAVA) [HAVA02] to modernize the administration of federal elections and to establish the U.S. Election Assistance Commission (EAC) to provide guidance to the states in their efforts to comply with the HAVA administrative requirements. Under the authority of HAVA, the EAC developed the Election Supporting Technology Evaluation Program (ESTEP) in 2022, which is responsible for the evaluation of election technologies not covered under the Voluntary Voting System Guidelines (VVSG).

The purpose of these requirements is to provide a set of specifications against which electronic ballot delivery systems can be tested to determine if they meet baseline standards for functionality, security, and accessibility. This document, the Voluntary Electronic Ballot Delivery Requirements (herein referred to as the Requirements or VEBDR), is the first iteration of Electronic Ballot Delivery standards that have been released at the federal level.

This version of the Voluntary Electronic Ballot Delivery Requirements (VEBDR) was produced by ESTEP, working in conjunction with stakeholders, manufacturers, and the National Institute of Standards and Technology (NIST), to aid in the process of requirements development. The process of developing standardized election requirements is paramount to ensuring that elections are secure and accessible, as well as providing the public with confidence in elections.

These standards will assist stakeholders in better serving their election jurisdictions by guiding the development of their election systems.

EAC staff must periodically review the VEBDR for proposed revisions, considering both internal and external feedback. Determinations must be sent to the EAC’s Executive Director (or a person operating in that capacity) to begin the review process required to ensure the timely adoption of revisions. Under the direction of the Executive Director, EAC staff, in consultation with NIST staff, may make minor technical changes to the requirements in a timely manner. EAC staff is responsible for updating the test assertions and issuing responses to requests for interpretation or notices of clarification, as needed, to ensure efficiency in the process.

Table of Contents

Introduction

This document outlines federal-level functional, security, and accessibility standards for electronic ballot delivery. It was developed by the EAC to specifically address the delivery of blank electronic ballots, herein referred to as **Electronic Ballot Delivery (EBD)**. Adherence to these requirements is governed by state and territory-specific laws and procedures.

Audience

This document will be used primarily by electronic ballot delivery system developers and manufacturers and Voting System Test Laboratories (VSTLs) as a baseline set of requirements for functionality, security, and accessibility to which states or territories may add their specific requirements, as necessary.

Scope

This document focuses solely on **electronic ballot delivery systems (EBD Systems)** acquired or developed in-house by election officials and evaluated by the EAC. EBD Systems are defined in this document as:

Systems in which blank ballots and voter information packets are delivered to a voter electronically over the internet. These systems use a combination of software and hardware, which may or may not reside onsite or in the cloud, and can be accessed from a voter's personal device (e.g., computer, cell phone, tablet, etc.).

The federal Military and Overseas Voter Empowerment (MOVE) Act requires each state to provide for the electronic delivery (via fax, email, or an Internet-supported application) of ballots and related information from the local or state election office to any registered Uniformed and Overseas Civilian voters covered by the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA Voters). Some jurisdictions also offer electronic ballot delivery to voters with disabilities, voters who have been displaced, or individuals living within the election jurisdiction in unique situations. However, the specifics of system usage and eligibility for electronic ballot delivery depend on the jurisdiction in which the voter is registered.

These requirements are meant to serve as a **baseline** for EBD system functionality, security, and accessibility. While some jurisdictions may integrate additional tools within their EBD portals or links (such as voter registration portals or electronic ballot return), such features fall **outside the scope** of these requirements.

The **Voluntary Electronic Ballot Delivery Requirements (VEBDR)** only covers the standard test requirements for federal certification, and any expectations beyond this baseline will be at the discretion of state, local, or territorial rules or statutes.

Conformance Information

This section outlines how manufacturers of EBD Systems can use the material presented in this document to verify conformance with the requirements specified herein. Adherence to the VEBDR signifies that an EBD System has met the stipulated standards. However, this conformance should not be construed as certification under the EAC's Election Supporting Technology Evaluation Program.

- **Identifying Requirements:** Requirements are indicated by the presence of a unique number in the left margin, followed by a descriptive title.
- **Discussion Fields:** Requirements that have a "Discussion" field are intended to aid readers in their understanding of the requirement. Information presented in this field does not constitute a requirement.
- **Commercial Manufacturer:** A manufacturer engaged in the commercial activities of selling, renting, leasing, or supplying EBD systems, including public-facing websites and web portals, to state and local jurisdictions.
- **In-House Manufacturer:** A manufacturer, typically a state or local jurisdiction, which owns, develops, and maintains its own EBD system, including public-facing websites and/or web portals.
- **Documentation Requirements:** Requirements marked with a badge labeled "Documentation Required" indicate that the evaluation must include a technical documentation review.
- **"If Applicable" Requirements:** Requirements marked with a badge labeled "If Applicable" are not required for conformance but must be evaluated if required by a jurisdiction or if the EBD system supports or markets the functionality.

Guidance for Documentation Requirements

Prior to submitting an EBD system for evaluation, the EAC requires a comprehensive set of technical documentation to be included as part of a complete Application Package.

Note: Manufacturers must submit all technical documentation requirements outlined in the Election Supporting Technology Evaluation Program Manual.

Manufacturers must clearly mark any documentation they request to be treated as confidential and proprietary before providing it to the EAC and its designated test laboratory for evaluation. Marking the entire package as confidential and/or proprietary is insufficient. All pages of the documentation that contain information the manufacturer considers confidential and/or proprietary information must be clearly marked as such.

Disclaimer: All requirements labeled as "documentation required" may require further testing or review to ensure conformance. The EAC and test laboratories have the discretion to request further documentation or testing to ensure that the EBD system has met the minimum requirements.

Responsibilities of the Election Official

While these requirements are designed to help focus the efforts of manufacturers and developers in creating EBD systems that are safe, secure, and accessible, election officials also play a vital role.

The following considerations related to electronic ballot delivery are especially important to emphasize:

- Voter Education
- Secure PDF Ballot Transmission
- .Gov Domains for Websites and Emails
- Ensuring Security

Voter Education

Voters must have clear and accessible information about their state or local jurisdiction's EBD system or process. Key details include:

1. **Eligibility**: Voters should be given clear, written guidance to determine whether they qualify for an electronic ballot.
2. **Request Process**: Voters should be given clear, written instructions regarding the process to request an electronic ballot.
3. **Voting Period**: Voters should be given clear and written communications regarding the timeframes when they can request, access, vote, and return an electronically delivered ballot.

Whether through a fact sheet, distributed materials, or information on an official state or municipal jurisdiction website, election officials are responsible for providing clear information to voters about the process of requesting and using an electronic ballot before, or on, election day or associated deadlines.

Secure PDF Ballot Transmission

Depending on the needs and resources available to states, localities, and territories, not every election jurisdiction will choose to utilize an EBD system. Reasons for this can include budgetary restrictions, the number of voters eligible for an electronic ballot, and/or the number of voters historically requesting an electronic ballot within the jurisdiction. In any case, a portable document format (PDF) transmission of a ballot has been successfully used in the past. While it is an option available to election jurisdictions, it is far from the most secure. Some points to keep in mind when considering this alternative include:

- **Attachment vs Link**: If a PDF is sent to the voter, will it be accessed via an attachment or link to a secure document-sharing platform?

- **Password Protection**: Does state statute or procedural rules require that the electronic ballot PDF be encrypted or protected by passwords, codes, or multi-factor authentication? If so, will any other actions be restricted, such as editing or marking? Additionally, how will the authentication mechanism be provided to the intended voter?

.Gov Domains for Websites and Emails

The importance of clearly identifying official channels for election information and materials cannot be understated in today's age of artificial intelligence (AI), disinformation, and cyber threats. Election Officials should consider using a .gov address for all official election information or material. Using a .gov address is the single most effective way to let voters know that they are accessing or receiving official government information or documents.

More information can be found here: https://get.gov/domains/.

Ensuring Security

The EAC, NIST, CISA, and FBI have identified inherent risks commonly associated with electronic ballot delivery, similar to those found in other internet-connected applications. However, these risks can be effectively mitigated through the implementation of appropriate security measures.

As such, we encourage EOs using or considering whether to use electronic ballot delivery to take appropriate steps to address these security risks. For further information about the risks of electronic ballot delivery, marking, and return please reference this document produced by the EAC, CISA, NIST, and the FBI:

Risk Management for Electronic Ballot Delivery, Marking, and Return

Voluntary Electronic Ballot Delivery Requirements

Section 1 – Functionality and Interoperability

This area of testing will target the specific functionality claimed by the manufacturer or developer to ensure the system functions as documented and expected. This testing will use both positive and negative test data to assess the functionality of the EBD System.

For instance, a successful positive test outcome would involve the seamless upload of ballot data into the system. Conversely, a successful negative test outcome would involve rejecting multiple selections for a single-choice contest when digitally marking a ballot.

Functionality and Interoperability requirements are organized based on the following categories:

1. Jurisdictional Customization
2. Election Data Imports
3. Voter Authentication
4. Ballot Marking Online
5. Reports

Each numbered section below contains a brief explanatory description followed by the requirements.

Section 1.1 – Jurisdictional Customization

In the United States, states and local jurisdictions have the autonomy to conduct elections based on their respective state statutes and jurisdictional rules. Achieving a one-size-fits-all system can be challenging due to variability across different regions. Therefore, it is crucial that any EBD system be customizable and adaptable to meet the specific needs of each jurisdiction.

This section outlines the fundamental criteria governing EBD customization. It is important to note that these requirements represent the minimum standards and are not exhaustive. Jurisdictions may augment or tailor these provisions as necessary to meet their specific needs.

1.1.1 – Active Voting Period

The duration permitted for voters to access an electronic ballot must be adjustable to align with the timeframes established by the jurisdiction.

Discussion: Active Voting Period

Whether ballot access is facilitated through email, a web portal, or a hyperlink, the period during which a ballot remains accessible must be adaptable to comply with the legal mandates of the specific jurisdiction in which it will be utilized, i.e., 45 days to comply with the MOVE Act.

1.1.2 – Ballot Format

The EBD system must offer the ability to customize the format of the ballot to best adhere to state or jurisdictional requirements.

Discussion: Ballot Format

Not only does the ability to customize an electronic ballot contribute to consistency, but in some cases, it is legally mandated by state statutes. When attempting to meet jurisdictional requirements effectively, consider the following customizable formatting options:

- Election title, date, and jurisdiction information
- Instructions on how to vote the ballot
- Contest names, candidate names, measure text, and voting options
- Order in which measures, races, and candidates appear on the ballot

1.1.3 – Ballot Packet/Supplemental Documents

The EBD system must have the ability to include supplemental documents, which will print or display as part of a complete ballot packet.

Discussion: Ballot Packets and Supplemental Documents

A Ballot Packet is the collection of documents required to mark and cast an absentee ballot which can include but is not limited to the ballot, a voter affidavit, and any supplemental documents required by the jurisdiction or election, such as return instructions, or a ballot cover sheet.

Section 1.2 – Election Data Imports

This section will cover an EBD system's ability to import voter registration information, ballot data, and election data files to ensure the accurate distribution of electronic ballots to eligible voters.

1.2.1 – Voter Registration Import

The EBD system must support importing voter registration information in at least one commonly available and well-known format, such as CSV, XLS, JSON, XML, or as specified by the jurisdiction.

Discussion: Common Data Format

Ensuring interoperability across different election technologies is crucial for effective election administration and auditing. While not a requirement, adopting the Common Data Format

(CDF) as an import/export option in EBD Systems offers significant benefits and aligns with best practices in data management.

By incorporating CDF, election technologies can improve compatibility with other systems and enhance the reliability and transparency of election data handling. For more information on this use case, refer to NIST SP 1500-102 Voter Records Interchange (VRI) CDF.

1.2.2 – Eligible Voters

Once voter registration information has been uploaded to the EBD system, administrators must have a method to review and verify that the imported records meet the eligibility criteria for EBD.

Discussion: Verifying Eligible Voters

This verification process can be as straightforward as providing a way to review uploaded voter data and may also include the ability to filter that data based on additional information (i.e. ballot delivery preferences or whether the voter is a UOCAVA voter). Overall, the aim of this requirement is to prevent the accidental inclusion of unqualified voters.

1.2.3 – EBD Record Management

The EBD system must provide a mechanism for administrators to remove or deactivate voter records that do not meet the eligibility requirements for electronic ballot delivery.

Discussion: Removal of Ineligible Voters

As with Requirement 1.2.2, this requirement aims to prevent the accidental inclusion of ineligible voters in the EBD system. If an ineligible voter record is accidentally uploaded into the EBD system, the system must provide a mechanism to ensure that only qualified voters receive electronic ballots. This safeguard helps maintain the integrity of the EBD process.

1.2.4 – Ballot Data/Election Definition Imports

The EBD system must support the import and parsing of ballot data/election definition exports. File format will vary from one jurisdiction to another; therefore, the EBD system must, at the very least, accept ballot data/election definition imports formatted as TXT, CSV, JSON, or XML.

Discussion: Ballot Data

Modern election management/ballot design software allows the export of ballot data which typically contains:

- Election title, date, and jurisdiction information;
- Districts included in the election;
- Precincts/precinct splits and associated ballot styles for the election;
- Contest names and measure text;
- Contest choice options;

- Contest and Candidate ordering information Precinct/precinct split and/or districts to contest relationships;
- And political party affiliation or ballot preference if applicable.

Allowing the import and parsing of ballot data will both streamline and ensure accuracy when configuring an election in the EBD system.

1.2.5 – Ballot Image Import

In addition to ballot data/election definition imports, the EBD system must also allow the import of blank ballot images in PDF.

Section 1.3 – Voter Authentication

This section will cover the EBD systems' ability to customize the voter authentication or login methods as set by the jurisdiction, as well as outline some guidelines for basic functionality.

1.3.1 – Voter Authentication

An EBD system must provide a portal login for voters to securely access blank ballots.

1.3.2 – Login Requirements

Login requirements for voter access must be customizable by the jurisdiction, based on the requirements set in state statutes or regulations. However, an EBD system must offer a login system that relies on two or more of the following options:

1. Unique username
2. Password
3. Login PIN
4. Name
5. DOB
6. State-issued driver's License or ID Card
7. Or other accepted forms of ID approved by the jurisdiction, such as a state's unique identifying number.

1.3.3 Inactivity Alert

If the voter has not interacted with the EBD system within a jurisdiction-defined timeframe, but no less than 5 minutes, the system must issue an inactivity alert to notify the voter.

1.3.4 Inactivity Reset

When an inactivity alert is issued, the system must provide the voter with an option to extend their session.

1.3.5 Inactivity Logout

If the voter does not respond to the alert within a jurisdiction-defined timeframe, but no less than 5 minutes after the alert, the EBD system must automatically log the voter out of their session.

Section 1.4 – Ballot Marking Online

While not universally available in all jurisdictions, online ballot marking can play a role in providing voters access to a ballot. Although specific voting methods and rules will vary based on the jurisdiction, certain fundamental functions remain the same.

1.4.1 – Ballot Access

The EBD system must provide a distinct and unambiguous indication when a voter is about to access their blank ballot. Whether the subsequent action involves printing out a blank ballot packet or marking their ballot online, any icons, buttons, or messages related to accessing the ballot or ballot packet must clearly convey the intended next step.

Discussion: Notification of Ballot Access

In some jurisdictions voters are limited to one ballot instance per request and any subsequent replacements must be requested in person, over the phone, or via email. Therefore, the EBD system must present a clear and explicit warning when the voter initiates access to their ballot or ballot packet.

This can be as simple as a notification or on-screen alert informing the voter that they are about to access a ballot and any steps they may need to take if a replacement is needed.

1.4.2 – Ballot Marking Accuracy

IF APPLICABLE

When marking a ballot online, if a voter selects, de-selects, or changes their choice/selection, the EBD system will respond with a clear audio and/or visual indication that a choice has been made. This requirement includes the following:

1. In a vote-for-N-of-M contest, the system must not deselect any candidate automatically.
2. In a vote-for-N-of-M contest, the system must inform the voter that they have attempted to make too many selections and offer an opportunity to change their selections.
3. Ballot options intended to select a group of candidates, such as straight-party voting, must provide clear feedback on the result of the action of selecting this option.
4. Ballots with preferential or ranking voting methods must not re-order candidates except in response to an explicit voter command.

References: VVSG 2.0 (7.2-C)

1.4.3 – Spoiled Ballot Protection

IF APPLICABLE

An EBD system must be equipped to address common and avoidable voter errors, particularly overvoting. If a voter selects more candidates or responses than allowed in a contest, the EBD system must block or alert the voter that overvoting may invalidate their vote.

1.4.4 – Write-Ins

IF APPLICABLE

The EBD system must be able to accept write-in votes as valid and allow voters to write in their preferred candidate, where appropriate.

1.4.5 – Ballot Review

Once a voter has finished marking their ballot, the EBD system must provide the voter an opportunity to review their selections, including any undervotes and overvotes, and make any necessary changes before confirming their votes and generating a ballot packet.

1.4.6 – Ballot Review Corrections

Instructions on how to correct or modify a selection from ballot review must be clear and written in plain language.

1.4.7 – Voter Privacy

Once a ballot is marked and printed or saved locally, all details regarding the voter's selections must be immediately removed from the system.

1.4.8 – Reinitiating Ballot Marking

IF APPLICABLE

If jurisdictional rules allow it, and if a voter needs to mark their ballot again due to technical issues (such as printer malfunctions or corrupted saves) or any other reason (such as a lost or damaged ballot packet), the EBD system must provide clear instructions on how the voter may request a new ballot or initiate the ballot-marking process again.

Section 1.5 – Reports

The ability to generate reports regarding voter activity, ballot requests, and ballot access is vital in assisting election officials in tracking system usage, reconciling ballot requests, and spotting or reporting errors. This section will cover the basic reports required to perform these functions.

1.5.1 – Ballot Requests Reports

The EBD system must have the capability to generate a comprehensive report on ballot requests made by voters. The information on these reports must at least include the following:

1. Date and time stamps of requests.
2. Voter identifying information (e.g., voter ID, first and last name, etc.).
3. Ballot information (e.g., ballot style, precinct, first issued or replacement, etc.).
4. Ballot status (e.g., sent/request, accessed, suspended, etc.).

Discussion: Ballot Requests

The reconciliation of issued and active ballots (i.e., a valid ballot) plays a critical role in election administration. Reports generated by systems like EBD systems can provide valuable assistance in maintaining an accurate count of ballots requested or issued throughout the election cycle.

It's important to note that reporting ballot requests is solely for achieving an accurate count and overview of electronic ballots sent to voters. This requirement does not require the collection of voter selections or any unnecessary personal information.

1.5.2 – Activated/Accessed Ballots

In addition to ballot requests, the EBD system must also generate reports containing active ballot information or voters who have already accessed a ballot.

Discussion: Reporting Active and Accessed Ballot

The reconciliation of issued and active ballots (i.e., a valid ballot) plays a critical role in the administration of elections. Reports generated by systems like EBD systems can provide valuable assistance when maintaining an accurate count of ballots issued during the election cycle.

It's important to note that reporting active or accessed ballots focuses solely on achieving an accurate count. It does not involve collecting voter selections or personal information.

1.5.3 – Inactive or Invalidated Ballots

IF APPLICABLE

The EBD system must generate reports that will account for any previously invalidated requests. For example, if a voter requests a replacement electronic blank ballot, the report will indicate that the voter had requested two ballots, one inactive/voided ballot, and a replacement.

Section 2 - Security

EBD systems in the US are hosted in one of two ways: in a cloud database or hosted locally (by the state or local jurisdiction). While there will be some requirements specific to the method used by each EBD system, there will be some overlap.

In addition to covering security requirements for both methods of hosting electronic blank ballots, this section will also touch on:

1. Cloud Database Security Requirements
2. Locally Hosted Security Requirements
3. General Database Security Requirements
4. Website and Portal Security Requirements
5. Data Recovery and Resiliency

Discussion: Cloud Hosting Vs Hosting Locally
When deciding between utilizing Cloud Service Providers (CSPs) or local hosting for electronic ballot delivery, several factors come into play. For example, CSPs offer scalability, accessibility, and robust security measures, but will involve ongoing service costs.

On the other hand, local hosting provides direct control (physical and digital) over servers, data privacy, and reduced latency, but requires dedicated maintenance. Ultimately, the choice relies on the organization's laws, priorities, budget, and risk tolerance.

Section 2.1 – Cloud Database Security Requirements

The following security requirements are specific to EBD systems utilizing Cloud Service Providers (CSP) to host electronic blank ballots and differ from those of locally hosted systems.

Section 2.1 does not apply to locally hosted systems.

2.1.1 – FedRAMP Compliant CSP

DOCUMENTATION REQUIRED

All EBD systems utilizing cloud-based services must be compliant with the security requirements outlined in the Federal Risk and Authorization Management Program (**FedRAMP**). Specifically, EBD systems must adhere to the FedRAMP **Baseline: High** and align with Cloud Service Offering (CSO) **Impact Level 4** or an equivalent standard.

Note: To be considered equivalent to FedRAMP **Baseline: High**, the EBD manufacturer or developer must obtain prior authorization from the EAC by providing documentation from their CSP that demonstrates full compliance with the latest FedRAMP high security control baseline through an assessment conducted by a FedRAMP-recognized Third Party Assessment Organization (3PAO).

References: FedRAMP Security Controls Baseline, DoD Cloud Computing Security Requirements Guide V1,R4

2.1.2 – SOC 2 Compliance

DOCUMENTATION REQUIRED

In addition to FedRAMP compliance, CSPs must provide comprehensive documentation demonstrating their adherence to SOC 2 Trust Service Criteria for Security, Availability, Confidentiality, and Privacy—either through certification or a current third-party SOC 2 report covering these criteria. If a CSP does not have a SOC 2 report covering all four criteria, it must provide additional documentation demonstrating how it meets equivalent security and privacy standards.

Section 2.2 – Locally Hosted Security Requirements

Section 2.2 does not apply to cloud-hosted systems.

2.2.1 – Locally Hosted Security Compliance

DOCUMENTATION REQUIRED

The Electronic Ballot Delivery (EBD) system must be installed and configured in accordance with relevant security controls from NIST SP 800-53 to ensure:

- Authentication – Secure user identification and access control.
- Authorization – Role-based access to prevent unauthorized actions.
- Confidentiality – Protection of ballot and voter data from unauthorized access.
- Integrity – Safeguards against unauthorized modifications or tampering.

Therefore, the EBD system provider must submit documentation that:

1. Explain how the system implements each of the above security mechanisms.
2. Identifies the specific NIST SP 800-53 controls applied and how they are addressed.
3. Includes security assessments, configurations, or test results demonstrating compliance.

Reference: NIST SP 800-53 Rev. 5

2.2.2 – Web Server Security (NIST SP 800-44)

DOCUMENTATION REQUIRED

Locally hosted EBD systems must have their web servers securely configured and maintained in accordance with NIST SP 800-44 Version 2 to protect against unauthorized access and attacks.

Therefore, the EBD system provider must submit documentation detailing:

1. Web Server Hardening – Secure configuration, access controls, and disabling unnecessary features.

2. OS and Network Security – Protections for the server's operating system and network traffic.
3. Data Protection – Secure storage and encryption of transmitted data.
4. Maintenance Practices – Logging, monitoring, and regular security updates.

Documentation must reference specific NIST SP 800-44 checklist items and include relevant security policies, configurations, or test results.

Reference: NIST SP 800-44 Ver.2

2.2.3 – Access Controls

The EBD system must implement role-based access control to assign roles and permissions based on job responsibilities.

Reference: NIST SP 800-53 Rev. 5

2.2.4 – Access Control Documentation

DOCUMENTATION REQUIRED

In addition to requirement 2.2.3, the EBD system must include documentation with clear guidance on creating, modifying, and revoking roles.

Section 2.3 – General Database Security Requirements

2.3.1 – Encryption

Data at rest and stored within the EBD system must be encrypted using the industry-standard encryption algorithm AES-256.

Reference: NIST FIPS 197-upd1

2.3.2 – Principle of Least Privilege

The EBD system must follow the Principle of Least Privilege (PoLP) to ensure that users are granted access only to the data and functions directly related to their assigned roles.

Reference: NIST SP 800-53 Rev.5

2.3.3 – Principle of Least Privilege Documentation

DOCUMENTATION REQUIRED

Documentation provided regarding PoLP must provide clear instructions on creating, modifying, and revoking roles.

2.3.4 – Administrative Access

The EBD system must ensure that all users with administrative access to the system or election management functions authenticate using unique login credentials. This requirement may be satisfied by either:

1. The EBD system issuing unique credentials, or
2. The EBD system integrating with a third-party identity provider (e.g., Microsoft Entra ID, Okta) that enforces strong authentication controls.

Reference: NIST SP 800-53 Rev.5

2.3.5 – Multi-Factor Authentication

The EBD system must utilize Multi-Factor Authentication (MFA) when users with administrative permissions access the system. This requirement may be satisfied through integration with a third-party identity provider that enforces MFA.

Reference: NIST SP 800-53 Rev.5

2.3.6 – Vendor Access Controls

DOCUMENTATION REQUIRED

The EBD system must list clear and specific guidelines on how and when a manufacturer may access the system, e.g., for system setup, system training, troubleshooting, updates, etc.

2.3.7 – Audit Logs and Reports

In addition to reports regarding voter activity, the EBD system must have the ability to generate reports about access and modifications to the EBD database. These reports must include date and timestamps, as well as tailored to include at least the following information:

1. Admin and vendor database access
2. Access attempts
3. Modifications to the database
4. System Logs

Section 2.4 – Website and Portal Security Requirements

2.4.1 – Web Application Firewall

The EBD system must incorporate a Web Application Firewall (WAF).

2.4.2 – Web Application Security Protections

DOCUMENTATION REQUIRED

The EBD system must be configured to mitigate OWASP's Top 10 weaknesses. This includes leveraging a Web Application Firewall (WAF) where applicable, alongside secure coding practices, proper authentication mechanisms, and system hardening measures.

Reference: OWASP Top 10

2.4.3 – Website/Portal Encryption

The EBD system must encrypt traffic using Hypertext Transfer Protocol Secure (HTTPS), supporting Transport Layer Security (TLS) version 1.3 or later, as newer secure versions become available.

Reference: NIST SP 800-52 Rev.2

2.4.4 – Valid HTTPS/SSL Certificate

DOCUMENTATION REQUIRED

In addition to employing HTTPS and TLS, the EBD system must possess a valid HTTPS/SSL Certificate from a reputable Certificate Authority or provide documentation outlining its SSL certificate acquisition and renewal process.

Section 2.5 – Data Recovery and Resiliency

2.5.1 – Automated Backups

The EBD system must perform automatic backups regularly with a backup schedule that can be adjusted by the jurisdiction.

2.5.2 – Complete System Backups

Automated backups of the EBD system must be a complete backup of the jurisdiction's data, which includes:

1. Election Information
2. Voter Registration Information Import
3. Ballot Data/Definition Import
4. Ballot Images
5. Audit Logs

2.5.3 – Backup Data Verification and System Recovery

DOCUMENTATION REQUIRED

Documentation packaged with the EBD system must provide instructions on how to verify the integrity of backed-up data and perform a complete system recovery in case of emergency.

2.5.4 – Offline Backup

The EBD system must support offline backups in the event of hardware failure on locally hosted systems.

For cloud-based EBD systems, backups must be stored in a geographically separate region from the primary system to ensure disaster recovery capabilities.

Section 3 – Accessibility

Electronic ballot delivery offers a significant benefit: tailoring ballots to meet the accessibility needs of voters who cannot physically visit an in-person voting location. While the ballot itself may not be explicitly "customized" for each voter, its digital format allows it to adapt to the individual's accessibility settings on their device—whether it's a PC, mobile device, or tablet.

This section discusses the fundamental aspects required of accessibility within EBD systems.

Section 3.1 – Baseline Accessibility

3.1.1 – Federal Requirements for Accessibility

Any webpage provided by the EBD system developer, aiming to meet the accessibility requirements outlined in the VEBDR, must comply with **WCAG 2.1 Level AA standards**. This encompasses various components, including but not limited to:

- Portal Login Page
- Splash Page and Static Icons
- Ballot Access
- Online Ballot Marking Pages
- Ballot Review
- Instructions displayed on the screen.

A helpful rule of thumb for any system aiming to meet these accessibility requirements is: If the voter will be the primary user of a webpage or portal, it must be designed to adhere to WCAG 2.1 Level AA compliance.

Discussion: Section 508 vs WCAG 2.1 AA compliance

Section 508, a component of the Rehabilitation Act of 1973, is widely recognized as a mandatory requirement in federal guidelines. It stipulates that federal electronic and communication technology must be accessible to people with disabilities.

While, on the other hand, WCAG (The Web Content Accessibility Guidelines) was developed in 1999 by the World Wide Web Consortium (W3C) to ensure an accessible web experience for all users and was once considered a separate guideline from those in Section 508.

However, in a significant development, the U.S. Access Board merged WCAG into Section 508 in 2018, effectively aligning the two. As a result of the merger compliance with WCAG 2.1 at Level AA now inherently fulfills the EBD system's obligations under Section 508. Therefore, we don't explicitly mandate Section 508 compliance here, as adherence to WCAG already covers the necessary accessibility requirements when it comes to EBD systems.

Appendix A: Glossary (Alphabetized)

- **Active Voting Period** – Time during which a voter can access and use their electronic ballot.
- **Administrative Access** – A level of permissions granted to users based on their roles and responsibilities within a system. These permissions allow users to perform administrative tasks such as managing system settings, user accounts, and security configurations. Administrative access is typically restricted to ensure that only authorized personnel can make critical changes to the system.
- **Audit Logs** – Detailed records that track system activities, including user actions, system events, and other significant occurrences. Information included in an audit log typically includes data such as timestamps, user IDs, IP addresses, and descriptions of the actions performed.
- **Ballot Packet / Supplemental Documents** – Additional materials delivered with a ballot, such as voter affidavits or return instructions.
- **Ballot Style** – A ballot with a specific set of contests and candidates for a particular precinct. Ballot styles vary based on which combination of contests and which party affiliation (in primary elections) voters are eligible to participate in. Ballot style varies based on the contests voters are eligible to vote on and, during primary elections, their party affiliation.
- **Common Data Format (CDF)** - Standard and practice of storing and creating data in a common, described format that can be read by other systems.
- **Federal Risk and Authorization Management Program (FedRAMP)** - A U.S. government program that standardizes the security assessment, authorization, and continuous monitoring of cloud products and services used by federal agencies.
- **Multi-Factor Authentication (MFA)** – Authentication using two or more factors. Factors include something you know (e.g., password/personal identification number); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric).
- **Military and Overseas Voter Empowerment (MOVE) Act** – A federal law requiring states to offer UOCAVA voters the option to receive blank absentee ballots electronically at least 45 days before a federal election.
- **National Institute of Standards and Technology (NIST)** – Federal organization tasked with assisting in the development of voting system standards. NIST develops and maintains standards for a wide array of technologies. NIST scientists assist the U.S Election Assistance Commission in developing testable standards for voting systems.
- **Overvote** – When the number of selections made by a voter in a contest is more than the maximum number allowed.
- **Open Worldwide Application Security Project (OWASP)** – A nonprofit organization dedicated to improving software security through community-led open-source projects, educational

resources, and advocacy. OWASP is well-known for publishing the OWASP Top 10, which highlights the most critical security risks to web applications.

- **Principle of Least Privilege (PoLP)** – A security concept where users, applications, and systems are granted the minimum levels of access, or permissions, necessary to perform their tasks. This principle helps reduce the risk of unauthorized access and potential security breaches.
- **Precinct Split** - A subdivision of a precinct which arises when a precinct is split by two or more election districts that may require different ballot styles.
- **Role-Based Access Control** - A security model that restricts system access based on the roles assigned to users within an organization. Each role is associated with specific permissions and responsibilities, allowing users to perform tasks relevant to their job functions. RBAC helps streamline access management and ensures that users have appropriate access levels based on their roles.
- **Section 508** – A component of the Rehabilitation Act of 1973, which is widely recognized as a mandatory requirement in federal guidelines. It stipulates that federal electronic and communication technology must be accessible to people with disabilities.
- **Spoiled Ballot** – A ballot which has been mistakenly marked or altered by a voter. A spoiled ballot is not cast, and the voter may request a new ballot to mark correctly.
- **Transport Layer Security (TLS)** - A cryptographic protocol designed to provide secure communication over a computer network. TLS ensures the privacy, integrity, and authenticity of data exchanged between applications and users on the internet.
- **Undervote** - Occurs when the number of choices selected by a voter in a contest is less than the maximum number allowed for that contest or when no selection is made for a single-choice contest.
- **Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA)** - UOCAVA citizens are U.S. citizens who are active members of the Uniformed Services, the Merchant Marine, and the commissioned corps of the Public Health Service and the National Oceanic and Atmospheric Administration, their eligible family members, and U.S. citizens residing outside the United States. This Act provides the legal basis for these citizens' absentee voting requirements for federal offices.
- **Voting System Test Laboratory (VSTL)** - VSTLs are privately owned testing laboratories that test voting systems (and other election systems) for conformance to the Voluntary Voting System Guidelines (VVSG) or to other requirements, including individual state requirements. VSTLs are periodically reviewed for conformance to National Voluntary Laboratory Accreditation Program (NVLAP) administered by the National Institute for Standards and Technology.

- **Voluntary Voting System Guidelines (VVSG)** - A set of specifications and requirements against which voting systems can be tested to determine if the systems meet required standards. Under HAVA, the EAC is responsible for developing, maintaining, and approving these standards. Some factors examined under these tests include basic functionality, accessibility, and security capabilities.
- **Web Application Firewall (WAF)** - A security system that monitors, filters, and protects HTTP traffic to and from a web application. WAFs help prevent attacks such as SQL injection, cross-site scripting (XSS), and other common web application vulnerabilities.
- **Web Content Accessibility Guidelines (WCAG)** - A set of guidelines developed by the World Wide Web Consortium (W3C) to make web content more accessible to people with disabilities. WCAG provides a comprehensive framework for improving the accessibility of web content, including text, images, and multimedia, to ensure that all users, regardless of their abilities, can access and interact with digital content effectively.
- **Write-In** – A vote for a candidate that was not listed on the ballot. In some jurisdictions, voters may do this by filling in a write-in space provided on a paper ballot, or they may use a keypad, touch screen, or other electronic means to enter the name on an electronic voting device.

This glossary is not exhaustive but provides clarity for frequently used or potentially unfamiliar terms throughout the VEBDR document.