Voluntary Voter Registration System Guidelines

VVRSG V0.9

February 27, 2026

U.S. Election Assistance Commission

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

NOTE: This copy and version of VVRSG is subject to change and edits deemed necessary and appropriate by the U.S. Election Assistance Commission (EAC) Election Supporting Technology Evaluation Program (ESTEP).

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. Specifically, HAVA addresses voter registration systems in Section 245, parts F and H, in which it describes the necessity for the EAC to study the "implementation cost of an online voter registration system..." and the means by which to ensure and achieve equal access online voter registration systems and "address the fairness of such systems to all citizens." (HAVA, sec. 245) 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 guidelines is to provide a set of specifications against which voter registration systems can be tested to determine if they meet baseline standards for accuracy, functionality, security, and accessibility. This document, the Voluntary Voter Registration System Guidelines (herein referred to as the Guidelines or VVRSG), is the first iteration of Voter Registration System standards that have been released at the federal level.

This document 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 confidence in the elections.

EAC staff must periodically review the VVRSG 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.

Table of Contents

Introduction

This document outlines voluntary federal-level functional, security, and accessibility standards for voter registration systems. It was developed by the EAC to specifically address the various processes of voter registration activities within a set software system format, herein referred to as **Voter Registration Systems** (VRS). Adherence to these requirements is governed by state and territory-specific laws and procedures.

Audience

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

Scope

This document focuses solely on Voter Registration Systems (VRS) acquired and/or developed by commercial or in-house manufacturers and evaluated by the EAC. The National Voter Registration Act of 1993 (NVRA) sets forth certain federal requirements for voter registration, including that: states should offer voter registration opportunities through state motor vehicle agencies, by mail-in application, and through state and local offices. It also discusses the need for management of state voter rolls, all of which can be conducted through a VR system. The Help America Vote Act (HAVA) requires that chief state election officials must implement a single, uniform, official, centralized, interactive computerized statewide voter registration list defined, maintained, and administered at the State level that contains the name and registration information of every legally registered voter in the State and the computerized lists shall be coordinated with other agency databases within the State. Voter registration systems shall ensure that voter registration records are accurate and updated regularly, and that safeguards are implemented to ensure that eligible voters are not removed in error from the official list of eligible voters.

VR systems are defined as:

A combination of either compatible hardware, software, or firmware, materials, and documentation used to automate the process of voter registration and secure voter information within a county, state, or election jurisdiction by election administrators. Voter registration systems are connected to a private network, administered through state or local jurisdictions, and hold the capability of administrative functions to aid in the voting process on Election Day.

Voter registration systems are used in an elections office to assist election officials in registering new voters, updating existing voter registrations, updating voter signatures, ensuring voter registration eligibility, and other relevant election activities. Additionally, voter registration systems also have administrative functions that allow them to pair with a number of election-

supporting technologies such as electronic poll books (EPB) to capture voter-check ins at the polls. Per suggestions of the Carter-Baker Commission of 2005, Voter registration systems should strive towards a certain level of interoperability, to encourage use of these systems for better accuracy, security, and voter list maintenance activities. Voter registration systems should have robust and adequate technological security measures to prevent unauthorized access to the computerized voter registration list at the state or local level.

Election administrators are the primary users. Unlike voters, they are trained in how to use the voter registration system effectively to administer various election processes cited throughout this document. Unlike voting machines, voter registration systems house personally identifiable voter information (PII), and should not be accessible to the general public. Only authorized users should be given special administrative access to the voter registration system, that is accompanied by a two-factor authentication process. The tasks conducted in the voter registration system by the user are often done independently and without multiple users accessing the same log-in. Every process that is utilized in the voter registration system should log the users' credentials for auditing purposes.

Voter registration systems often come in the form of a software application that can be accessed on a tablet, laptop, or PC. They should:

- Produce simple visual interfaces with the user.
- Be connected to a secure network that complies with local jurisdictional guidelines.
- Operate under a standard operating systems format.

There may be guidelines for actions by election administrators that affect the fundamental nature of the task. These actions may include:

- Reviewing of comparing a voter's signature to the image of one on file,
- Reading information on a voter's identification (ID) card,
- Reading and manually inputting information from a paper voter registration into the electronic voter registration system, and
- Handling an ID card or a scanner to read the voter information into the system or a printed voter authorization form to be given to the voter.

These guidelines are meant to serve as a **baseline** for voter registration system functionality, security, and accessibility. While some jurisdictions may integrate additional tools within their voter registration systems, such features fall **outside the scope** of these requirements. The VVRSG only covers the minimum test guidelines 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 Voter Registration Systems can use the material presented in this document to verify conformance with the requirements specified herein. Adherence to the Voluntary Voter Registration System Guidelines (VVRSG) signifies that a VR 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 guidelines:** guidelines 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 VR systems, including public-facing websites and web portals, to state and local jurisdictions.
- **In-House Manufacturer or Developer:** A manufacturer, typically a state or local jurisdiction, which owns, develops, and maintains its own VR system, including public-facing websites and/or web portals.
- **Documentation guidelines:** guidelines marked with a badge labeled "Documentation Required" indicate that the evaluation must include a technical documentation review.
- **"If Applicable" Guidelines:** guidelines marked with a badge labeled "If Applicable" are not required for conformance but must be evaluated if the VR system supports or markets the functionality.

Voluntary Voter Registration System Requirements

Section 1 – Functionality and Interoperability

Voter registration systems (VRS) typically have various functionalities and customizability to adhere to jurisdictional requirements and best practices for elections as a whole. Despite the wide range of options for design, creation, and implementation of VRS functionality, VRS should at least adhere to a basic level of functionality outlined in the following requirements.

This area of testing will target the specific functionality claimed by the manufacturer 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 VRS.

Functionality requirements are organized based on the following categories:

1. Jurisdictional Customization
2. Usability Features
3. Functional Configuration
4. Compatibility
5. Telecommunications
6. System Maintenance and Troubleshooting

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

Section 1.1 – Jurisdictional Customization

In the United States, 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 VRS be customizable and adaptable to meet the specific needs of each jurisdiction.

This section outlines the fundamental criteria governing VRS 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 – Software Package Format

DOCUMENTATION REQUIRED

The VRS must adhere to a customizable software package format, in which the VRS is accessible via a web portal, cloud-based service, or private and secured network. The format of this software package will adhere to the legal mandates of the specific jurisdiction in which it will be utilized and follow strict security requirements as outlined in this document. The VRS software package will be able to be accessed on a tablet, laptop, or PC, and the software package format

must hold the ability to be customized per the specific direction of jurisdictions or states, within the confines of contractual agreements between manufacturers of the VRS and those states/jurisdictions. This can include customized:

1. Portals, log-in pages, public facing interfaces,
2. System modules and task pages,
3. System reports,
4. User roles,
5. Any other components deemed necessary for VRS functionality as outlined in these requirements

Section 1.2 – Usability Features

All features of the VRS must be clearly documented so that the system can be effectively used by election workers. VRS manufacturers must:

1. Demonstrate that the VRS was developed using a user-centered design process
2. Clearly document instructions for election administrators
3. Provide instructions written in plain language
4. Submit a VRS for usability testing with election workers
5. Design the VRS so that it is capable of producing auditable records in English
6. Demonstrate that the VRS is able to maintain data for the EAVS Survey

1.2.1 – User-Centered Design Process

DOCUMENTATION REQUIRED

The manufacturer must submit a report providing documentation that the VRS was developed following a user-centered design process.

The report must include, at a minimum:

1. A listing of user-centered design methods used,
2. The types of election workers included in those methods,
3. How those methods were integrated into the overall implementation process, and
4. How the results of those methods contributed to developing the final features and design.

1.2.2 – Instructions for Election Administrators

DOCUMENTATION REQUIRED

The VRS Manufacturer must provide clear, complete, and detailed instructions and messages for the set-up, use and management, and log-in and shutdown of the entire system for appropriate users.

1. The documentation must be:

a. Presented at a beginner to intermediate level expertise (as outlined in section 1.2.3) for election administrators who are not experts in voter registration systems and computer technology, and
b. Provided in either electronic PDF or Microsoft Word document format for use by an election administrator in a typical voter registration office, with the capability for printing to be used to in in-person format.

2. Procedural instructions and trainings must enable the election administrator to verify that the VRS:
    a. Has obtained a successful log-in credential, and
    b. Is in correct working order to engage with voter registration materials and processes as intended by the manufacturer and jurisdictional oversight.

1.2.3 – Plain Language

DOCUMENTATION REQUIRED

Information and instructions for election administrators must be written clearly, following the best practices for plain language. This includes messages generated by the VRS for election administrators in support of the operation, maintenance, or safety of the system.

1.2.4 – Usability Testing with Election Administrators

DOCUMENTATION REQUIRED **IF APPLICABLE**

The manufacturer may conduct usability tests of the VRS setup, operation, and shutdown as documented by the manufacturer, with representative election administrators, to demonstrate that election administrators can learn, understand, and perform these tasks successfully. The results of these usability tests, along with all relevant documentation, must be included in the technical documentation package (TDP).

The test must include handling all variations in voter registration activities, including:

1. General security best practices as outlined in this document,
2. Operation of the system from log-in to log-out,
3. Use of assistive technology or language options that are part of the VRS, and
4. Specific voter registration activities, including but not limited to:
    a. Processing voter registrations,
    b. Processing candidate filings,
    c. Processing requests from outside agencies,
    d. Engaging in the absentee process,
    e. Performing election results activities,
    f. Voter List Maintenance activities, and
    g. Other activities deemed necessary for system functionality by the jurisdiction in which the system operates.

5. The test participants must include election workers representing a range of experience.

1.2.5 – Audit Records

DOCUMENTATION REQUIRED

All records produced by the VRS must have the information required to support auditing by election officials and others who can only read English. This must include reports/records generated by the system related to;

1. user management and role-based access (see section 2.1.1 and 2.1.3) and,
2. reports/records generated by the system showing data related to activities in section 1.3 of this document.

1.2.6 - Election Administration and Voting Survey (EAVS) Data Management

The VRS must be able to produce and submit data requested by the U.S. Election Assistance Commission (EAC) for the purposes of answering all survey inquiries on the Election Administration and Voting Survey (EAVS) in accordance with federal law. The data points are as follows:

1. Total number of registered and eligible people: active and inactive.

2. Total number of same-day voter registrations.

3. Total registration transactions processed in current EAVS Survey data year.

4. Total confirmation notices sent to voters in current EAVS Survey data year.

5. Reasons for sending confirmation notices to voters.

6. Total voters removed from the registration rolls in current EAVS Survey data year.

7. Voter registration records merged or linked in current EAVS Survey data year.

This data must be able to be produced by the system via either a data table or report, in a commonly available and well-known format such as PDF, CSV, XLS, JSON, XML, or another format specified by the system's assigned jurisdiction.

Discussion:

EAVS is a survey of all 50 U.S. states and territories on various topics related to federal elections. Topics covered throughout EAVS data collection and that are relevant to this guideline may include; voter registration and list maintenance data, voting practices data for overseas citizens and members of the armed forces serving away from home, voting machine and e-poll book information from specific jurisdictions, and other important issues related to voting and election administration.

Section 1.3 – Functional Configuration

The VRS must be configured to perform basic tasks during use throughout election and non-election years. These tasks include:

1. Handling specific types of voter registration data,
2. Process, update, and maintain voter registration records,
3. Process absentee/Mail-In requests and records,
4. Record and display election information, and
5. Create and maintain various election and absentee-based reports.
6. Voter List Maintenance (VLM) Activities.
7. The creation and maintenance of petitions.
8. The management of Election Workers and Poll Workers.
9. The use of an internal check for duplicate records process.

Discussion:

For the purposes of these guidelines, it can be assumed that any reference to "registration" activities applies to both same day registration and non-same day registration voter registration systems.

1.3.1 – Voter Registration Data

The VRS must hold the functionality of handling the entry, processing, and disbursement of voter registration data and information to all voters, poll workers, and election administrators within the jurisdiction in which it will be utilized. This must include:

1. Voter registration requests,
2. Voter registration records,
3. Ballot requests,
4. Voter history information,
5. Voter list maintenance, communications, and mailings data

1.3.2 – Process New Voter Registration Applications

The VRS must hold the functionality of processing new voter registration applications. This should include applications submitted by paper or electronic delivery, and must be able to process the following information:

1. Voter Name (first, last, and MI)
2. Voter date of birth
3. Voter ID (If applicable)
4. Voter Address
5. Voter Signature
6. Pre-Registration Status (for potential voters who are age 16, 17, or 18 on or before election day). (If applicable)
7. Other relevant voter information provided on the voter registration application, possibly subject to jurisdictional and state guidelines

1.3.3 - Update an Existing Voter Registration Record with New Information

The VRS must be capable of updating existing and active voter registration records with new information, such as:

1. name changes
2. address changes
3. signature changes
4. Political party changes (if applicable)

1.3.4 - Changing Voter Status

The VRS must hold the functionality of changing a voter status, which can include:

1. Active status
2. Inactive status
3. Pending status
4. Canceled status (can also mean or show as deceased status)
5. Suspended status (can also mean or show as felony status) (if applicable)

1.3.5 - Transmitting and Receipt of Voter Registration Records and Information

The VRS must hold the functionality of transmitting voter registration records information to vital stakeholders including:

1. Other Voter Registration Systems
2. Outside state systems (if applicable) as outlined later in this document

Discussion:

This guideline also applies to VRS types that are considered within the same “bottom-up” formatted state.

1.3.6 - Back Up, Restore, or Export Voter Registration Records

The VRS must hold the functionality of providing backups, restoring, and exporting voter registration records. Records must be in the approved file formats listed in this document.

1.3.7 - Display of Voter Registration Records and Record History

The VRS must have the functionality of displaying voter registration records and history of said record for use by an election administrator.

1.3.8 - Conduct Voter Research

The VRS must hold the functionality of looking up and researching a voter by various voter data points including;

1. Name,
2. Date of birth,
3. Address, or
4. Identification numbers, including drivers license numbers (DLN) and/or full/partial social security numbers (SSN) (if applicable).

1.3.9 – Process New Absentee/Mail-In Requests

The VRS must enable users to process new absentee requests, by processing the following absentee data:

1. First and Last name of Absentee Voter
2. Absentee Voter Address
3. Absentee Voter Date of Birth (DOB)
4. Absentee Voter ID (if applicable)
5. Absentee Voter party selection (if applicable)
6. Absentee Voter reason for ballot request (if applicable)

1.3.10 – Update Current Absentee/Mail-In Requests

The VRS must enable users to update current absentee requests with various statuses within the absentee process. This can include:

1. Active
2. Inactive
3. Unsent

4. Sent
5. Pending
6. Accepted
7. Rejected
8. Cured
9. Cure Needed
10. Any other absentee status required under local jurisdictional laws and regulations

1.3.11 – Display Absentee/Mail-In Records and History

The VRS must enable users to display absentee records and history for voters for use by an election administrator.

1.3.12 – Absentee/Mail-In Voter Research

The VRS must enable users to look up and research absentee voters by various data points including:

1. First and Last Name
2. Date of Birth
3. Address
4. Precinct or Ballot Style
5. Voter ID Number (if applicable)

1.3.13 – Record and Display Election Information

The VRS must be able to record and display various data points related to current and past elections occurring within the jurisdiction said system operates within. These can include:

1. Name and type of the election:
    a. Primary,
    b. General,
    c. Municipal,
    d. Special, or
    e. Referendum;
2. Date of the election:
    a. Day,
    b. Month, and
    c. Year,
3. Appropriate office and office parameters for offices up for election and from past elections,
4. Candidates for current and past elections,
5. Major and Minor party selection by candidate for election, and

6. Information for offices and candidates regarding special elections within a specific jurisdiction.

1.3.14 – Create and Maintain Election and Absentee/Mail-In Reports

DOCUMENTATION REQUIRED

The VRS must be able to produce reports regarding all election and absentee activities in section 1.3 of this document that occur within the system, in a commonly available and well-known format such as PDF, CSV, XLS/XLSX or XLS(X), JSON, XML, or another format specified by the system's assigned jurisdiction. These reports must meet the accessibility requirements as outlined in Section 3 of this document.

1.3.15 - Voter List Maintenance and Accuracy (VLM) Activities

The VRS must enable users to conduct Voter List Maintenance (VLM) activities required by law via the National Voter Registration Act (NVRA) of 1993 and the Help America Vote Act (HAVA) of 2002. The system must allow users to maintain voter registration lists and coordinate with necessary state agencies (see section 1.5.3, 1.5.4 of this document) to keep voter records current, and see that only voters who are not registered or who are not eligible to vote are removed from the computerized list, based on jurisdictional rules and regulations. This includes the management of voters with the following statuses:

1. Deceased voter
2. Non-citizen
3. Voter with address change
4. Voters who have not responded to a notice, and have not voted in two consecutive general elections for federal office
5. Felony conviction
6. Declaration of Mental Incapacitation

Per the National Voter Registration Act (NVRA) of 1993, no otherwise eligible registrant may be removed solely by reason of failure to vote. The Voter List Maintenance functionality in the system must additionally enable users to manually perform comparison checks of voter registration records, in which users can easily differentiate records that have to following issues:

1. Missing or mismatched signature
2. Inaccurate PII
3. Misspellings and typographical errors
4. Invalid or wrongly placed addresses or precincts
5. Duplicate records

Discussion:

For best practices regarding Voter List Maintenance activities, it is recommended that Voter Registration Systems users participate in the National Change of Address (NCOA) product, conduct regular and official election mailings, and stringently review duplicate records and records belonging to voters over the age of 100 years old. If allowed by jurisdictional law, it is also recommended that Voter Registration Systems users use 3rd party data for list maintenance, if applicable.

1.3.16 – Petitions

IF APPLICABLE

The VRS must enable users to have the functionality of creating, maintaining, and editing petitions and petition signatures for candidates and referendums, in accordance with the requirements found in section 1.3.13 of this document.

1.3.17 – Election Worker and Poll Worker Tracking

IF APPLICABLE

The VRS must enable the user to add, edit, and track the work history and the status option of "election worker" or "poll worker" to a voter record, clarifying that that voter either has requested to be an election or poll worker.

The VRS must also enable users to add "election workers" or "poll workers" who are not registered voters to be tracked within the system in the same manner as above.

1.3.18 - Internal Check for Duplicates and Accuracy Standards

The VRS must automatically flag registration records that produce duplicate records, specifically. It must allow users to reject or approve records based on the duplicate notification and subsequent process outlined in section 1.3.15 of this document.

The VRS must include functionality to apply defined accuracy standards through an integrated software solution or module. This functionality should support process such as percentage-based record matching, voter identification verification, data accuracy validation, and signature validation.

1.3.19 – Address and District Management

The VRS must hold the capability of performing address and district management activities. This must include;

1. Adding or removing address points from a particular district

2. Creating new districts related to specific office types

3. removing old districts from specific office types

4. Creating, removing, or editing districts types and addresses via a GIS solution

Section 1.4 – Compatibility

The VRS must be compatible with the minimum list of approved devices in this section, necessary to perform and execute basic functions of the system. These include various hardware devices and software systems that integrate or work with the VRS to perform voter registration activities deemed necessary by the jurisdiction in which the system operates.

1.4.1 - Compatibility with Hardware

The VRS must be compatible with hardware attached to the system, or as identified as supported by the VRS, such as:

1. Bar code capturing devices,
2. Printing devices, and
3. Laptops, tablets, or desktop devices.

1.4.2 – Compatibility with Software

The VRS must have the ability to interface with software systems used to complete various voter registration activities deemed necessary by the jurisdiction in which the system operates. This must include, specifically, software systems that aid the VRS in accessing necessary Geographic Information Systems (GIS) data for the purposes of voter registration, and software systems used to complete signature verification processes.

Section 1.5 – Telecommunications

When applicable, the VRS must have the capability to transmit and receive data from:

1. Other voter registration systems,
2. E-poll books,
3. In-State Government portals/agencies,
4. Out-of-State Government portals/agencies, and
5. Communicate with Third Party/Non-Government Entities.

1.5.1 – Communication with Other Voter Registration Systems

The VRS must have the ability to securely, accurately, and efficiently transmit and receive data electronically and communicate with other VRS in different jurisdictions.

1.5.2 – Communication with E-Poll Books

The VRS must have the ability to securely, accurately, and efficiently transmit and receive data electronically and communicate with e-poll books, typically through a secured web services framework designed by the manufacturer.

1.5.3 – Communication with In-State Government Portals/Agencies

The VRS must have the ability to securely, accurately, and efficiently transmit and receive data electronically and communicate with various in-state government portals and agencies, specifically within the jurisdiction in which it operates.

It will be able to hold inter-communication abilities with other government agencies as needed, such as, The Department of Motor Vehicles, Social Security Agency (SSA), The Department of Health or Bureau of Vital Statistics, courts or state prison/corrections agencies, or various other state agencies that may not be listed.

1.5.4 – Communication with Out-Of-State Government Portals/Agencies

The VRS must have the ability to securely, accurately, and efficiently transmit and receive data electronically and communicate with various out-of-state government portals and agencies, specifically within the jurisdiction in which it operates.

It will be able to hold inter-communication abilities with other out-of-state government agencies as needed, such as, The Social Security Agency (SSA), The United States Postal Service National Change of Address Program, and the Centers for Disease Control & Prevention's National Center of Health Statistics, or various other out-of-state government agencies that may not be listed.

1.5.5 - Communication with Third Party/Non-Government Entities

The VRS must have the ability to securely, accurately, and efficiently transmit and receive data electronically and communicate with various third party or non-government portals and entities, specifically within the jurisdiction in which it operates.

This communication must occur via a digital upload, with eligibility to be determined by the user.

Third party and Non-government entities must also be blocked from accessing data in the VRS, via the security guidelines in sections 2.1.3, 2.1.6, 2.2.3, and 2.3.3 in this document, respectively.

Discussion:

These entities referenced above may include non-profits that hold voter registration drives or other groups that seek to coordinate or expand voter registration efforts.

Section 1.6 – System Maintenance and Troubleshooting

DOCUMENTATION REQUIRED

A VRS must contain information in its documentation pertaining to maintenance and troubleshooting procedures for:

1. Loss of Connectivity
2. System Response Time
3. System-Related Errors
4. System Failure
5. Warnings, Alerts, and Instructions
6. Icon Labels

1.6.1 – Loss of Connectivity

DOCUMENTATION REQUIRED

In the event of a network failure or other interruption, documentation should outline how the VRS must:

1. Captures and saves Election Administrator activity, including:
    a. New Registrations,
    b. Voter Record Updates,
    c. Signature Updates,
    d. Absentee Updates, and
    e. Vote History Updates;
2. Reconnects with any hardware, including:
    a. Digital signature capturing devices,
    b. Bar code capturing devices,
    c. Printing devices,
    d. Network devices (i.e. routers),
    e. E-Poll Books (If applicable),
    f. Laptops, tablets, or desktop devices.

In addition to the steps above, documentation must also include any troubleshooting steps an Election Administrator may take to verify the outage isn't localized to their local network or devices.

1.6.2 – System Response Time

The VRS must complete a visual response or display in no more than 2-3 seconds or display an indicator that a response is still being prepared.

Discussion:

This is to allow the user to quickly perceive that an action has been detected by the VRS and is being processed. The user should never get the sense of dealing with an unresponsive or "dead" system.

1.6.3 – System Related Errors

The VRS must allow election administrators to complete their duties accurately and effectively, ensuring that the design or features of the system do not lead to election administrators making errors. Specifically, the system shows this by adhering to requirements outlined in sections 1.1.1, 1.2.1, 1.2.2, and 1.2.3 of this document.

1.6.4 – System Failure

DOCUMENTATION REQUIRED

The VRS should contain documentation regarding procedures to resolve a system failure, which is defined as a problem either with hardware or operating system software that causes the system to perform abnormally.

1.6.5 – Warnings, Alerts, and Instructions

Warning, alerts, and instructions issued by the VRS must be distinguishable from other information.

1. Warnings and alerts must clearly state, in plain language:
    a. The nature of the issue or problem,
    b. whether the Election Administrator has performed or attempted an invalid operation or whether the VRS itself has malfunctioned in some way, and
    c. the responses available to the election administrator.
2. Each step in an instruction or item in a list of instructions must be separated:
    a. Spatially in visual formats, and
    b. with a noticeable pause in audio formats (if applicable).

1.6.6 – Icon Labels

When an icon label is used in the electronic interface to convey information, indicate an action, or prompt a response, it must be accompanied by a corresponding label that uses text.

Section 1.7 – Common Data Format

Voter Registration Systems (VRS) must hold the capability of importing and exporting various voter registration data points in and out of the system. In particular, the system must hold the capability of performing the interoperable task of importing and exporting specific voter registration data found on the National Mail Voter Registration Form and Federal Post Card Application (FPCA), required by the National Voter Registration Act (NVRA), or state voter registration forms with additional state-specific information being clarified by local Election Officials. In communicating this specific information, the VRS can do so across a myriad of election technology platforms, including e-poll books, other voter registration systems, and e-ballot delivery systems.

To clearly and effectively communicate voter registration data, it is recommended that a VRS follow the below requirements for utilizing a Common Data Format (CDF) to transmit data effectively and accurately to best serve voting populations amongst various election technology systems.

The purpose of this section is to provide clear data interchangeable formats for voter records requests and responses so as to assist election officials and VRS manufacturers to implement and support the development of voter records within states and allow for their systems to perform in an interoperable manner across states and jurisdictions when needed.

A VRS manufacturer aiming to meet the required CDF requirements outlined in VVRSR must comply with standards generally outlined in NIST SP 1500-102 v .1.0, “Voter Records Interchange Common Data Format Specification”. This encompasses various components, including but not limited to:

1. eXtensible Markup Language (XML) Format
2. JavaScript Object Notation (JSON) Format

A VRS manufacturer aiming to meet the required CDF requirements outlined in VVRSR must show the ability to process commonly accepted points of information and voter data, found on the NVRA and FPCA documentation submitted by a voter. The VRS manufacturer must also show the ability to process the specific use cases, listed in section 1.7.4 of this document.

1.7.1 – eXtensible Markup Language (XML) Format

The Voter Registration System must be capable of importing and exporting various voter registration record data points, highlighted in section 1.7.4, via eXtensible Markup Language (XML) Format. Specifically, the use of XML format should be used to transmit address data

points via the U.S. Thoroughfare, Landmark, and Postal Address Standard as issued by the Federal Geographic Data Committee (FGDC).

1.7.2 – JavaScript Object Notation (JSON) Format

The Voter Registration System must be capable of importing and exporting various voter registration record data points, highlighted in section 1.7.4, via JavaScript Object Notation (JSON) Format.

1.7.3 – NVRA and FPCA Data Points

The Voter Registration System must be capable of importing and exporting various voter registration record data points, via CDF format listed above, found on the NVRA and FPCA submissions by voters. These data points must include:

1. First and last name
2. Date of Birth
3. Address
4. Telephone number
5. ID Number
6. Choice of Party
7. Race or Ethnic group
8. Signature image

1.7.4 - Specific Use Cases

The Voter Registration System must be capable of importing and exporting specific data use cases, listed below and found in NIST SP 1500-102 v .1.0, “Voter Records Interchange Common Data Format Specification”.:

1. Class AdditionalInfo
2. Class BallotRequest
3. Class BallotStyle
4. Class ContactMethod
5. Class Election
6. Class ElectionAdministration
7. Class ElectionBasedBallotRequest
8. Class Error
9. Class ExternalIdentifier
10. Class File
11. Class Image
12. Class LatLng
13. Class Location
14. Class Name

15. Class Party
16. Class PermanentBallotRequest
17. Class PhoneContactMethod
18. Class ReportingUnit
19. Class RequestAcknowledgement
20. Class RequestHelper
21. Class RequestProxy
22. Class RequestRejection
23. Class RequestSuccess
24. Class Signature
25. Class TemporalBallotRequest
26. Class Voter
27. Class VoterClassification
28. Class VoterID
29. Class VoterParticipation
30. Class VoterRecord
31. Class VoterRecordResults
32. Class VoterRecordsRequest
33. Class VoterRecordsResponse
34. Enumeration AssertionValue
35. Enumeration BallotReceiptMethod
36. Enumeration ContactMethodType
37. Enumeration IdentifierType
38. Enumeration PhoneCapability
39. Enumeration ReportingUnitType
40. Enumeration RequestError
41. Enumeration RequestForm
42. Enumeration RequestMethod
43. Enumeration RequestProxyType
44. Enumeration SignatureSource
45. Enumeration SignatureType
46. Enumeration SuccessAction
47. Enumeration VoterClassificationType
48. Enumeration VoterHelperType
49. Enumeration VoterIDType
50. Enumeration VoterRequestType
51. Enumeration VoterStatus

Section 2 – Security

Voter Registration Systems (VRS) in the United States are hosted in one of two ways, in the cloud or locally (by the state or local jurisdiction). While there will be some requirements specific to the method used by each VR system, overlap can occur between the two options as well.

This area of testing will target the specific security claimed by the manufacturer to ensure the system is secured as documented and expected. This testing will use both positive and negative test data to assess the security of the VRS.

Security requirements are organized based on the following categories:

1. Access Control
2. System Integrity
3. Network/Telecommunications Security
4. Software Design/Architecture Standards
5. Database Security Requirements (Cloud/Locally Hosted)
6. Portals and Website Security
7. Data Recovery and Resiliency

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

Section 2.1 – Access Control

Access to both physical and digital spaces containing VRS, voter information, and voter registration equipment must be strictly controlled during the entire VRS lifecycle from development to end-of-life disposal of the information and equipment to detect and prevent supply chain attacks.

VRS manufacturers must establish procedures and technical controls that reflect applicable federal and state laws, regulations, directives, policies, standards, and guidance to control access to physical sites and networks containing VRS and related equipment. Access control systems should be automated when possible.

A VRS must be configured to:

1. Implement account management,
2. Follow established account management procedures and processes,
3. Implement and enforce role-based access,
4. Implement and support multi-factor authentication,
5. Implement and enforce separation of duties,
6. Implement and enforce principles of least privilege,
7. Implement and enforce session termination, device lock, and reauthentication,

8. Record Unsuccessful logon attempts, and
9. Implement system use notification.

2.1.1 – Account Management

VRS must authenticate each user with access to the system using an automated account management system. If available, the device's operating system can be used for automated account management. Regardless of the method employed, the account management system must enforce the use of codewords or passwords for each user. VRS must require their users to develop a password based on NIST SP 800-63-3 guidelines.

2.1.2 – Access Control Policies and Procedures

DOCUMENTATION REQUIRED

The VRS must have documentation for access control policies and procedures describing how the requirements in Section 2 are implemented.

2.1.3 – Role-Based Access

The VRS must implement access control to assign roles and permissions based on job responsibilities (e.g., system administrator, election administrator).

Additionally, documentation must include details on creating, modifying, and revoking roles.

Finally, VRS must hold to role Based Access Control Standards as outlined in ANSI INCITS 359-2004.

2.1.4 – Multi-Factor Authentication

The VRS shall enforce multi-factor authentication (MFA) for all privileged operations.

Discussion:

Privileged operations can include account creation, deletion, permission modification, or when directly updating external databases. Additionally, multi-factor authentication does not mean having multiple passwords.

2.1.5 – Separation of Duties

The VRS must be configurable to enforce separation of duties as defined by the jurisdiction.

Discussion:

For example, changes to voter information or system configurations may need to be authorized by two or more personnel to mitigate insider threats, depending on the jurisdictional requirements.

2.1.6 – Least Privilege

The VRS must enforce the concept of least privilege for accounts to restrict both privileged and non-privileged accounts to only permissions required to carry out the role assigned to the account.

For example, election administrators may have preferred roles for certain members of staff, versus themselves, that require different roles to be assigned to the individual's account.

2.1.7 – Session Termination

The VRS must include a configurable mechanism to automatically terminate a user session after a defined period of inactivity and lock the device, which can be defined and implemented by those assigned an Administrator Role.

2.1.8 - Device Lock

The VRS must include a user-initiated or time-configurable automatic lockout when a user is away from the system, which can be defined and implemented by the jurisdiction and/or those assigned an Administrator Role, and the account lockout must include a standard or configurable screen when the system is locked to obscure any data presented on the screen when terminated.

2.1.9 - Reauthentication

The VRS must include the ability to require reauthentication of the authorized user(s) after the session is terminated and the device locked.

2.1.10 – Unsuccessful Logon Attempts

The VRS must be configured to lock after a configurable number of login attempts and remain locked until an administrator or technician can unlock the account.

2.1.11 – System Use Notification

The VRS must include a configurable logon banner or system use notification for the user to accept upon logon.

Section 2.2 – System Integrity

The VRS must implement security measures to prevent malicious activity and protect the integrity, confidentiality, and availability of data. The VRS must be configured to:

1. Support an endpoint detection and response (EDR) tool (If Applicable)
2. Support an antivirus tool to detect and alert on malicious code (If Applicable)
3. Support file integrity checking to monitor file changes
4. Support verification of voter information

2.2.1 – Endpoint Detection and Response (EDR) Tool

IF APPLICABLE

Most VRS require connection to a network during operation, and as such, the system must support an EDR tool to prevent, detect, and respond to attempts to manipulate the system.

2.2.2 – Antivirus Tool

IF APPLICABLE

The VRS must implement an antivirus tool to detect and alert users to malicious code.

2.2.3 – Authentication to Access Configuration File

The VRS must allow only authenticated system administrators to access and modify system configuration files.

2.2.4 – Verification of Voter Information

Verifying voter information is an essential defense-in-depth measure aimed at safeguarding against accidental errors or malicious incidents involving altered or false voter data.

Therefore, VRS must:

1. cryptographically verify the integrity and authenticity of all voter data.
2. immediately log any verification error; and
3. immediately present on-screen any verification errors.

Section 2.3 – Network/Telecommunications Security

The VRS must be configured to:

1. Implement FIPS 140 approved encryption for the transfer of data
2. Disallow connections to unapproved external networks
3. Disallow connections to unapproved external devices
4. Implement network firewall settings for approved communication (network connected devices only)
5. Documentation of the network and communications architecture

2.3.1 – Network Encryption

The VRS must be configured to utilize, at minimum, FIPS 140-2 approved network encryption for the transfer of data for active and historic statuses. The VRS should utilize FIPS 140-3, once available.

2.3.2 – Disallow Connections to Unapproved External Networks

The VRS must be configured to disallow connections to unapproved external networks. This may be accomplished through IP or MAC address allow/whitelisting or other configurations where external network access is explicitly granted.

2.3.3 – Disallow Connections to Unapproved External Devices

The VRS must be configured to disallow connections to unapproved external devices.

This requirement applies to devices that can be recognized as approved, such as only allowing connections to managed devices. Security documentation must be clear on how this requirement is satisfied.

2.3.4 – Network Firewall

As the VRS requires connection to a network during voter registration activities, the VRS must implement a firewall configured to only allow approved communication with each device within the system.

2.3.5 – Documentation of the Network and Communications Architecture

DOCUMENTATION REQUIRED

The VRS documentation must include the network and communications architecture of any network used by any portion of the system.

Documentation can assist with data flow analysis, proper network configuration, and architecture to properly support the system.

Documentation must clearly indicate what types of network access the VRS supports.

2.3.6 - Device Access Control

DOCUMENTATION REQUIRED

The VRS documentation must include examples of valid and trusted machine certification allowing said device to join the election system network. The documentation must highlight the process of assigning, updating, and revoking machine certificates, and how those certified machines are assigned MAC/IP addresses pairings.

Section 2.4 – Software Design/Architecture Standards

The VRS or its documentation must:

1. Execute on a supported operating system
2. Support updates and patching
3. Utilize recognized software standard(s)
4. Generally operate within a layered, two front-end database system (internal and external)

2.4.1 – Execute on a Supported Operating System

The VRS software must execute on an operating system that is currently supported with updates and/or patches.

2.4.2 – Support Updates and Patching

The VRS applications must have the ability to be updated and/or patched.

2.4.3 – Utilize Recognized Software Standards

Application logic must adhere to a published, credible set of coding rules, conventions, or standards (coding conventions) that enhance the workmanship, security, integrity, testability, and maintainability of applications.

Coding conventions may be specified by the EAC in conjunction with voting system test labs and the VRS manufacturer must include information on coding conventions used in their VRS as part of their TDP submission.

Discussion:

The guidelines to follow coding conventions serve two purposes. First, by requiring specific risk factors to be mitigated, coding conventions support the integrity and maintainability of voting system logic. Second, by making the logic more transparent to a reviewer, coding conventions facilitate test lab evaluation of the logic's correctness to a level of assurance beyond that provided by operational testing.

2.4.4 - Database Dual Frontend System Format

DOCUMENTATION REQUIRED **IF APPLICABLE**

The VRS application must operate, generally, with a database that falls under a dual frontend system format. The database will be presented between two frontend systems, one internal and one external. A typical implementation may likely include several different internally and externally facing user interface systems, but should at minimum be illustrated via the two-frontend systems format, which shall include:

1. Internal database frontend
    a. This database is the primary interface used by election officials, and should be designed so that the election official can perform all required actions as set forth within their jurisdiction.
    b. This database should have higher functionality than the external database frontend, and require various security standards outlined in Section 2.5 of this document.
2. External database frontend
    a. This database allows for several use cases, in particular, a public voter portal in which the public, via an internet connection, can register to vote, check their registration status, or verify polling locations.
    b. This database should have reduced functionality, with multiple safeguards in place before reaching the internal database frontend, as outlined in sections 2.5 and 2.6 of this document.

Section 2.5 – Database Security Requirements (Cloud/Locally hosted)

The following security requirements are specific to Voter Registration Systems utilizing Cloud Service Providers (CSP) or Locally Hosted Databases to host voter registration information.

2.5.1 – Cloud Service Providers – FedRAMP Compliance

DOCUMENTATION REQUIRED **IF APPLICABLE**

All VRS utilizing cloud-based services must be compliant with the security requirements outlined in the Federal Risk and Authorization Management Program (**FedRAMP**). Specifically, VRS must adhere to the FedRAMP **Baseline: High** and align with Cloud Service Offering (CSO) **Impact Level 4**. These standards ensure robust security controls while accommodating the operational needs of state and local-level administrators.

2.5.2 – Cloud Service Providers – SOC 2 Compliance

DOCUMENTATION REQUIRED **IF APPLICABLE**

In addition to FedRAMP compliance, if the VRS is a CSP, it must provide comprehensive documentation demonstrating their adherence to SOC 2 Type I guidelines or certification. Current SOC 2 3rd party reports provided by the CSP will satisfy this requirement.

2.5.3 – Locally Hosted Databases – NIST SP 800-95 Compliance

DOCUMENTATION REQUIRED **IF APPLICABLE**

The VRS, if locally hosted, must be installed and configured in accordance with NIST SP 800-95. Specifically, the accompanying documentation should provide explicit details on how the VRS implements the following security mechanisms for web services:

1. Authentication,
2. Authorization,
3. Confidentiality, and
4. Integrity.

2.5.4 – Locally Hosted Databases – NIST SP 800-44 Compliance

DOCUMENTATION REQUIRED **IF APPLICABLE**

The VRS, if locally hosted, must be installed and configured in accordance with NIST SP 800-44. The accompanying documentation should provide explicit details on how the VRS adheres to the following principles from NIST SP 800-44:

1. Web Server Configuration,
2. Operating System Security,
3. Network Protection,
4. Information Handling, and
5. Ongoing Maintenance.

Section 2.6 – Portals and Website Security

VRS often access or are in direct connection with a public facing website or portal, for means of public access to the process of voter registration, specific to jurisdictional requirements in which the system operates within. The following requirements outline standards a VRS must adhere to for portal and website security. This includes:

1. Web Application Firewall,
2. Website/Portal Encryption, and
3. Valid HTTPS/SSL Certificate.

2.6.1 – Web Application Firewall

The VRS must incorporate a Web Application Firewall (WAF), which is configured to address OWASP's Top 10 weaknesses. Specifically, the WAF must protect against:

1. Broken Access Control,
2. Cryptographic Failures,
3. Injection Attacks,
4. Security Misconfiguration,
5. Vulnerable and Outdated Components,
6. Identification and Authentication Failures,
7. Security Logging and Monitoring Failures, and
8. Server-Side Request Forgery.

2.6.2 – Website/Portal Encryption

The VRS must encrypt traffic using Hypertext Transfer Protocol Secure (HTTPS), supporting Transport Layer Security (TLS) version 1.3.

2.6.3 – Valid HTTPS/SSL Certificate

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

Section 2.7 – Data Recovery and Resiliency

VRS store and exchange several important data points relevant to voter registration processes of the jurisdiction in which it operates in. This data must be available to be recovered and protected via various backups, including:

1. Regular Automated Backups,
2. Complete System Backups,
3. Offline Backups, and
4. Data Verification Package.

2.7.1 – Regular Automated Backups

The VRS must perform automatic backups regularly with a backup schedule that can be adjusted by the jurisdiction. It should implement an Automated File Integrity Checking Service, in which the file integrity system can continuously scan for unauthorized changes, and can be reported to the election official utilizing the VRS.

2.7.2 – Complete System Backups

Automated backups of the VRS must be a complete backup of the jurisdiction's data, which includes, but is not limited to:

1. Election Information,
2. Voter Registration Record Information,
3. Absentee Information, and
4. Incoming Voter Registration Data.

2.7.3 - Offline Backups

IF APPLICABLE **DOCUMENTATION REQUIRED**

The VRS must be able to conduct offline backups of the jurisdiction's data, which includes, but is not limited to:

1. Election Information,
2. Voter Registration Record Information,
3. Absentee Information, and
4. Incoming Voter Registration Data.

NOTE: This requirement is only applicable to submitted Voter Registration Systems that are locally hosted in some capacity.

2.7.4 - Data Verification Package

DOCUMENTATION REQUIRED

The VRS must be able to conduct and show a data verification package, showing time, date, and contents of data included in the package. The VRS data verification package must include any and all data for its specific jurisdiction.

Section 3 - Accessibility

Voter Registration Systems (VRS) are essential to the elections process across the country, and not widely used by the public except in certain instances where a VRS has a public portal piece that communicates voter registration information to the system. These public portals typically are in the format of a publicly accessible website domain, that act as a means for the public to engage with various voter registration and absentee activities. Activities may include registering to vote, checking one's voter registration status, or applying for an absentee ballot, amongst many others.

This section discusses both required accessibility standards for public facing portions of VRS, and optional accessibility standards for private or back-end use portions of VRS.

Section 3.1 – Baseline Accessibility

3.1.1 – Federal Requirements for Accessibility – Public Facing VRS Portions

A VRS manufacturer aiming to meet the required accessibility requirements outlined in VVRSG, must comply with WCAG 2.1 Level AA Standards for all public-facing portions of the VRS. This encompasses various components, including but not limited to:

1. Portal Login Page,
2. Splash page and static icons,
3. Instructions displayed on the screen,
4. Higher contrast viewing options, and
5. Well-defined skip links, landmarks, and headings to aid site navigation
6. Any other components deemed necessary for VRS functionality as outlined in these requirements.

3.1.2 – Federal Requirements for Accessibility – Back-End/User-Facing VRS Portions

A VRS manufacturer aiming to meet the required accessibility requirements outlined in VVRSG, must comply with WCAG 2.1 Level AA Standards for all back end and administrative users.

Section 3.2 – Additional Languages

IF APPLICABLE **DOCUMENTATION REQUIRED**

3.2.1 – Languages

The Voter Registration system must be capable of displaying and printing all the information contained in the VRS instructions and on the public-facing VRS webpage in all languages the manufacturer has declared the system supports.

Appendix A: References

Reference	Citation
HAVA2002	Help America Vote Act of 2002 (HAVA), Pub. L. No. 107–252, 116 Stat. 1666 (2002).
CIS2018	Center for Internet Security (CIS). A Handbook for Election Infrastructure Security, Version 1.0. February 2018.
NIST800-63	National Institute of Standards and Technology (NIST). Digital Identity Guidelines, NIST Special Publication 800-63-3.
NIST800-53	National Institute of Standards and Technology (NIST). Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53 Rev. 5.
NIST800-44	National Institute of Standards and Technology (NIST). Guidelines on Securing Public Web Servers, NIST Special Publication 800-44 Version 2.
NIST800-95	National Institute of Standards and Technology (NIST). Guide to Secure Web Services, NIST Special Publication 800-95.
NIST1500-102	National Institute of Standards and Technology (NIST). Voter Records Interchange Common Data Format Specification, NIST Special Publication 1500-102 Version 1.0.
MITRE2024	MITRE Corporation. Recommended Security Controls for Voter Registration Systems.
FedRAMP	Federal Risk and Authorization Management Program (FedRAMP). FedRAMP Security Controls Baseline: High.
SOC2	American Institute of Certified Public Accountants (AICPA). SOC 2® Trust Services Criteria.
OWASPTop10	OWASP Foundation. OWASP Top 10 Web Application Security Risks.
WCAG21	World Wide Web Consortium (W3C). Web Content Accessibility Guidelines (WCAG) 2.1.
Section508	U.S. General Services Administration. Section 508 Standards.
EAVS	U.S. Election Assistance Commission. Election Administration and Voting Survey (EAVS).
NCSL2022	Draeger, Saige. The What, Why, and How of Voter List Maintenance. National Conference of State Legislatures, March 23, 2022.