DISCLAIMER

09-09-2019
Please note that this document, its sectional content, structure, ordering, and requirements are in a draft state and are not yet ready for final posting in their current form. We are also developing and organizing more front-matter at this time. However, this document is provided as is at this time as an up-to-date version of the current requirements. They are provided solely for the purpose of facilitating on-going discussions and do not yet represent the final version.

Voluntary Voting System Guidelines
VVSG 2.0

Draft Recommendations for Requirements for the Voluntary Voting System Guidelines 2.0

September 9, 2019

Prepared for the Election Assistance Commission

At the direction of the Technical Guidelines Development Committee
Acknowledgements

Chair of the TGDC:

Dr. Walter G. Copan
Director of the National Institute of Standards and Technology (NIST)
Gaithersburg, MD

Representing the EAC Standards Board:

Robert Giles
Director
New Jersey Division of Elections
Trenton, NJ

Paul Lux
Supervisor of Elections
Okaloosa County
Crestview, FL

Representing the EAC Board of Advisors:

Neal Kelley
Registrar of Voters
Orange County
Orange County, CA

Linda Lamone
Administrator of Elections
Maryland State Board of Election
Annapolis, MD

Representing the Architectural and Transportation Barrier, and Compliance Board (Access Board):

Marc Guthrie
Public Board Member
Newark, OH

Sachin Pavithran
Public Board Member
Logan, UT

Representing the American National Standards Institute (ANSI):

Mary Saunders
Vice President, Government Relations & Public Policy
American National Standards Institute
Washington, DC
Representing the Institute of Electrical and Electronics Engineers:

Dan Wallach
Professor, Electrical & Engineering Computer Science
Rice University
Houston, TX

Representing the National Association of State Election Directors (NASED):

Lori Augino
Washington State Director of Elections
Washington Secretary of State
Olympia, WA

Judd Choate
State Elections Director
Colorado Secretary of State
Denver, CO

Individuals with technical and scientific expertise relating to voting systems and equipment:

McDermot Coutts
Chief Architect/Director of Technical Development
Unisyn Voting Solutions
Vista, CA

Geoff Hale
Computer Security Expert
Washington, DC

David Wagner
Professor, Electrical & Engineering Computer Science
University of California-Berkeley
Berkeley, CA

Public Working Groups discussed and developed guidance to inform the development of requirements for the VVSG.

- **The Interoperability Working Group** handled voting system interoperability including common data format (CDF) modeling and schema development.
- **The Human Factors Working Group** handled human factors-related issues including accessibility and usability.
- **The Cybersecurity Working Group** handled voting system cybersecurity-related issues include various aspect of security control and auditing capabilities.
- **The Testing Working Group** handled voting system testing-related issues including what portions of the new VVSG need to be tested and how to test them.
Introduction to the VVSG 2.0

Overview

This document, the Voluntary Voting System Guidelines 2.0 (VVSG 2.0), is the third version of national level voting system standards. This version offers a new approach to the organization of the guidelines.

VVSG 2.0 is a recommendation from the Technical Guidelines Development Committee (TGDC) to the Election Assistance Commission (EAC) for a voting system standard written to address the next generation of voting equipment. It is a complete re-write of the Voluntary Voting System Guidelines (VVSG) of 2005 and 2015 and contains new and expanded material in many areas, including reliability and quality, usability and accessibility, security, and testing.

The requirements are more precise, more detailed, and written to be clearer to voting system manufacturers and test laboratories. The language throughout is written to be readable and usable by other audiences as well, including election officials, legislators, voting system procurement officials, various voting interest organizations and researchers, and the public at large.

Purpose

This document will be used primarily by voting system manufacturers and voting system test labs. Manufacturers will refer to the requirements in this document when they design and build new voting systems; the requirements will inform them in how voting systems should perform or be used in certain types of elections and voting environments. Test labs will refer to this document when they develop test plans for verifying whether the voting systems have indeed satisfied the requirements. This document, therefore, serves as a very important, foundational tool for ensuring that the voting systems used in U.S. elections will be secure, reliable, and easier for all voters to use accurately.

Scope

The VVSG is described as “Voluntary” and a “Guideline” because individual states and U.S. territories purchase their own voting systems and use them according to state and territory-specific laws and procedures. The Federal Government cannot dictate how elections are to be run. The majority of states and territories, however, now require that their voting systems conform to the requirements in the VVSG. Therefore, the VVSG can be considered essentially as a mandatory standard.
**Audience**

The VVSG is intended primarily as a critical reference document for:

- Designers and manufacturers of voting systems,
- Test labs performing the analysis and testing of voting systems in support of the national certification process,
- Software repositories designated by the national certification authority or a state, and
- Test labs and consultants performing the state certification of voting systems.

**Structure**

The VVSG contains the following sections:

- **Principles and Guidelines**: 15 principles and related guidelines that form the core of the VVSG
- **Requirements**: Detailed technical requirements that support the principles and guidelines
- **Appendix A, Glossary**: covers terminology used in requirements and informative language
- **Appendix B, List of all Requirements**: a summary listing of the titles of all requirements
- **Appendix C, References**: contains references to documents and on-line document used in the writing of this standard

A separate volume of tests will accompany the VVSG. The VVSG contains descriptions for test methods and general protocols for how requirements are to be tested, but does not contain the actual tests themselves.

Information and requirements for participation in the EAC’s certification program and for the voting system test labs are now located in the certification program manuals.

**Requirements and definitions from the Help America Vote Act**

The Help America Vote Act requires the EAC to develop standards for voting systems.

**Definition of a voting system**

HAVA Section 301 defines a voting system as the total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment), that is used to:

- define ballots;
- cast and count votes;
- report or display election results; and
- maintain and produce any audit trail information.
Functional Requirements from the Help America Vote Act

HAVA Section 301 mandates several requirements to assist voters. Although these requirements may be implemented in a different manner for different types of voting systems, all voting systems must provide these capabilities.

- Permit the voter to verify (in a private and independent manner) their choice before the ballot is cast and counted.
- Provide the voter with the opportunity (in a private and independent manner) to change their choice or correct any error before the ballot is cast and counted.
- Notify the voter if they have selected more than one candidate for a single office, inform the voter of the effect of casting multiple votes for a single office, and provide the voter an opportunity to correct the ballot before it is cast and counted.
- Be accessible for individuals with disabilities in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters.
- Provide alternative language accessibility pursuant to Section 203 of the Voting Rights Act.
# Table of Contents

Acknowledgements.................................................................................................................. 2  
Introduction to the VVSG 2.0................................................................................................... 4  
The VVSG 2.0 - Principles and Guidelines.............................................................................. 8  
What’s New in VVSG 2.0 Requirements ............................................................................... 13  
Using this document ............................................................................................................. 17  
Conformance Clause ............................................................................................................... 19  
Principle 1 High Quality Design............................................................................................. 21  
Principle 2 High Quality Implementation ........................................................................... 69  
Principle 3 Transparent ......................................................................................................... 97  
Principle 4 Interoperable ....................................................................................................... 120  
Principle 5 Equivalent and Consistent ............................................................................... 128  
Principle 6 Voter Privacy ....................................................................................................... 136  
Principle 7 Marked, Verified, and Cast as Intended .......................................................... 141  
Principle 8 Robust, Safe, Usable, and Accessible............................................................... 175  
Principle 9 Auditable ........................................................................................................... 186  
Principle 10 Ballot Secrecy................................................................................................... 201  
Principle 11 Access Control ................................................................................................. 210  
Principle 12 Physical Security ............................................................................................... 225  
Principle 13 Data Protection ................................................................................................ 233  
Principle 14 System Integrity ............................................................................................... 241  
Principle 15 Detection and Monitoring ............................................................................. 254  
Appendix A Glossary of Terms ............................................................................................. 266  
Appendix B Requirements Listing ....................................................................................... 325  
Appendix C References ....................................................................................................... 346
The VVSG 2.0 - Principles and Guidelines

The VVSG 2.0 consists of 15 principles and 63 guidelines. Together these principles and guidelines cover voting system design, development, and operations.

**Principle 1: HIGH QUALITY DESIGN**

The voting system is designed to accurately, completely, and robustly carry out election processes.

1.1 - The voting system is designed using commonly-accepted election process specifications.

1.2 - The voting system is designed to function correctly under real-world operating conditions.

1.3 - Voting system design supports evaluation methods enabling testers to clearly distinguish systems that correctly implement specified properties from those that do not.

**Principle 2: HIGH QUALITY IMPLEMENTATION**

The voting system is implemented using high quality best practices.

2.1 - The voting system software is implemented using trustworthy materials and best practices in software development.

2.2 - The voting system is implemented using best practice user-centered design methods that consider a wide range of representative voters, including those with and without disabilities, and election workers.

2.3 - Voting system logic is clear, meaningful, and well-structured.

2.4 - Voting system structure is modular, scalable, and robust.

2.5 – The voting system supports system processes and data with integrity.

2.6 - The voting system handles errors robustly and gracefully recovers from failure.

2.7 - The voting system performs reliably in anticipated physical environments.

**Principle 3: TRANSPARENT**

The voting system and voting processes are designed to provide transparency.
3.1 - The documentation describing the voting system design, operation, accessibility features, security measures, and other aspects of the voting system can be read and understood.

3.2 - The processes and transactions, both physical and digital, associated with the voting system are readily available for inspection.

3.3 - The public can understand and verify the operations of the voting system throughout the entirety of the election.

Principle 4: INTEROPERABLE
The voting system is designed to support interoperability in its interfaces to external systems, its interfaces to internal components, its data, and its peripherals.

4.1 - Voting system data that is imported, exported, or otherwise reported, is in an interoperable format.

4.2 - Standard, publicly-available formats for other types of data are used, where available.

4.3 - Widely-used hardware interfaces and communications protocols are used.

4.4 - Commercial-off-the-shelf (COTS) devices can be used if they meet applicable VVSG requirements.

Principle 5: EQUIVALENT AND CONSISTENT VOTER ACCESS
All voters can access and use the voting system regardless of their abilities, without discrimination.

5.1 - Voters have a consistent experience throughout the voting process within any method of voting.

5.2 - Voters receive equivalent information and options in all modes of voting.

Principle 6: VOTER PRIVACY
Voters can mark, verify, and cast their ballot privately and independently.

6.1 - The voting process preserves the privacy of the voter's interaction with the ballot, modes of voting, and vote selections.

6.2 - Voters can mark, verify, and cast their ballot or other associated cast vote record, without assistance from others.
Principle 7: MARKED, VERIFIED, AND CAST AS INTENDED
Ballots and vote selections are presented in a perceivable, operable, and understandable way and can be marked, verified, and cast by all voters.

7.1 - The default voting system settings present a ballot usable for the widest range of voters, and voters can adjust settings and preferences to meet their needs.

7.2 - Voters and election workers can use all controls accurately, and voters have direct control of all ballot changes and selections.

7.3 - Voters can understand all information as it is presented, including instructions, messages from the system, and error messages.

Principle 8: ROBUST, SAFE, USABLE, AND ACCESSIBLE
The voting system and voting processes provide a robust, safe, usable, and accessible experience.

8.1 - The voting system’s hardware, software, and accessories are robust and do not expose users to harmful conditions.

8.2 - The voting system meets currently accepted federal standards for accessibility.

8.3 - The voting system is evaluated with a wide range of representative voters, including those with and without disabilities, for effectiveness, efficiency, and satisfaction.

8.4 - The voting system is evaluated for usability by election workers.

Principle 9: AUDITABLE
The voting system is auditable and enables evidence-based elections.

9.1 - An error or fault in the voting system software or hardware cannot cause an undetectable change in election results.

9.2 - The voting system produces readily available records that provide the ability to check whether the election outcome is correct and, to the extent possible, identify the root cause of any irregularities.

9.3 - Voting system records are resilient in the presence of intentional forms of tampering and accidental errors.

9.4 - The voting system supports efficient audits.

Principle 10: BALLOT SECRECY
The voting system protects the secrecy of voters’ ballot selections.
10.1 - Ballot secrecy is maintained throughout the voting process.
10.2 - The voting system does not contain nor produce records, notifications, information about the voter or other election artifacts that can be used to associate the voter’s identity with the voter’s intent, choices, or selections.

Principle 11: ACCESS CONTROL
The voting system authenticates administrators, users, devices, and services before granting access to sensitive functions.

11.1 - The voting system enables logging, monitoring, reviewing, and modifying of access privileges, accounts, activities, and authorizations.

11.2 - The voting system limits the access of users, roles, and processes to the specific functions and data to which each entity holds authorized access.

11.3 - The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations.

11.4 - The voting system’s default access control policies enforce the principles of least privilege and separation of duties.

11.5 - Logical access to voting system assets are revoked when no longer required.

Principle 12: PHYSICAL SECURITY
The voting system prevents or detects attempts to tamper with voting system hardware.

12.1 - The voting system supports mechanisms to detect unauthorized physical access.

12.2 - The voting system only exposes physical ports and access points that are essential to voting operations.

Principle 13: DATA PROTECTION
The voting system protects data from unauthorized access, modification, or deletion.

13.1 - The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records.

13.2 - The source and integrity of electronic tabulation reports are verifiable.

13.3 - All cryptographic algorithms are public, well-vetted, and standardized.

13.4 - The voting system protects the integrity, authenticity, and confidentiality of sensitive data transmitted over all networks.


**Principle 14: SYSTEM INTEGRITY**
The voting system performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

14.1 - The voting system uses multiple layers of controls to provide resiliency against security failures or vulnerabilities.

14.2 - The voting system limits its attack surface by avoiding unnecessary code, data paths, connectivity, and physical ports, and by using other technical controls.

14.3 - The voting system maintains and verifies the integrity of software, firmware, and other critical components.

14.4 - Voting system software updates are authorized by an administrator prior to installation.

**Principle 15: DETECTION AND MONITORING**
The voting system provides mechanisms to detect anomalous or malicious behavior.

15.1 - Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing.

15.2 - The voting system generates, stores, and reports all error messages as they occur.

15.3 - The voting system is designed to protect against malware.

15.4 - A voting system with networking capabilities employs appropriate, well-vetted modern defenses against network-based attacks, commensurate with current best practice.
What’s New in VVSG 2.0 Requirements

There are many new or updated requirements, strengthening the security, interoperability, and usability and accessibility of voting systems:

Principle 1 - High Quality Design
- Functional equipment requirements are organized as phases of running an election:
  - Election and Ballot Definition
  - Pre-election Setup and logic and accuracy (L&A) testing
  - Opening Polls, Casting Ballots
  - Closing Polls, Results Reporting
  - Tabulation, Audit
  - Storage
- Requirements dovetail with cybersecurity in areas including:
  - Pre-election setup
  - Audits of bar codes versus readable content for ballot marking devices (BMDs)
  - Audits of scanned ballot images versus paper ballots
  - Audits of Cast Vote Record (CVR) creation
  - Content of various reports
  - Ability to match a ballot with its corresponding CVR

Principle 2 - High Quality Implementation
- Adds requirement to document and report on user-centered design process by developer to ensures system is designed for a wide range of representative voters, including those with and without disabilities, and election workers (P 2.2)

Principle 3 – Transparent
- Addresses transparency from the point of view of documentation that is necessary and sufficient to understand and perform all operations

Principle 4 - Interoperable
- Ensures that devices are capable of importing and exporting data in common data formats
- Requires manufacturers to provide complete specification of how the format is implemented
- Requires that encoded data uses publicly-available, no-cost method
• Uses common methods (for example, a USB) for all hardware interfaces
• Permits Commercial-off-the-Shelf (COTS) devices as long as relevant requirements are still satisfied

**Principle 5 - Equivalent and Consistent Voter Access**
• Applies to all modes of interaction and presentation throughout the voting session, fully supporting accessibility

**Principle 6 - Voter Privacy**
• Distinguishes voter privacy from ballot secrecy and ensures privacy for marking, verifying, and casting the ballot

**Principle 7 - Marked, Verified, and Cast as Intended**
• Updates voter interface requirements such as font, text size, audio, interaction control and navigation, scrolling, and ballot selections review
• Describes requirements that are voting system specific, but derived from Federal accessibility law

**Principle 8 - Robust, Safe, Usable, and Accessible**
• References Federal accessibility standards, Section 508 and Web Content Accessibility Guidelines 2.0 (WCAG 2.0)
• Updates requirements for reporting developer usability testing with voters and election workers

**Principle 9 - Auditable**
• Focuses on machine support for post-election audits
• Makes software independence mandatory
• Supports paper-based and end-to-end (E2E) systems
• Supports all types of audits, including risk-limiting audits (RLAs), compliance audits, and ballot-level audits

**Principle 10 - Ballot Secrecy**
• Includes a dedicated ballot secrecy section
• Prevents association of a voter identity to ballot selections
Principle 11 - Access Control
- Prevents the ability to disable logging
- Bases access control on voting stage (Pre-voting, Activated, Post-voting)
- Does not require role-based access control (RBAC)
- Requires multi-factor authentication for critical operations:
  - Accessing the admin account
  - Software updates to the certified voting system
  - Aggregating and tabulating
  - Enabling network functions, wireless and use of telecommunications
  - Changing device states, including opening and closing the polls
  - Deleting the audit trail
  - Modifying authentication mechanisms

Principle 12 - Physical Security
- Requires using only those exposed physical ports that are essential to voting operations
- Ensures that physical ports are able to be logically disabled
- Requires that all new connections and disconnections be logged

Principle 13 - Data Protection
- Clarifies that there are no hardware security requirements (for example, TPM (trusted platform module))
- Requires Federal Information Processing Standard (FIPS) 140-2 validated cryptographic modules (except for end-to-end cryptographic functions)
- Requires cryptographic protection of various election artifacts
- Requires digitally signed tabulation reports
- Ensures transmitted data is encrypted with end to end authentication

Principle 14 - System Integrity
- Requires risk assessment and supply chain risk management strategy
- Removes non-essential services
- Secures configurations and system hardening
- Exploit mitigation (for example, address space layout randomization (ASLR) data execution prevention (DEP) and free of known vulnerabilities
- Requires cryptographic boot validation
- Requires authenticated updates
- Ensure sandboxing and runtime integrity
Principle 15 - Detection and Monitoring

- Ensures moderately updated list of log types
- Requires firewalls and Intrusion Detection System for networked systems
- Detection systems must be updateable
- Requires digital signatures or whitelisting for voting systems
- Requires malware detection focusing on backend PCs
- Does not include direct recording electronic voting machines (DREs), Optical scanners (Opscans), or ballot marking devices (BMDs)
Using this document

Organization and Structure of Sections and Requirements

The requirements are organized and numbered according to the principles and guidelines they are most applicable to. They have the following fields:

- Number and title of each requirement
- Normative text of each requirement
- Optional informative discussion field
- Optional informative fields for source and applicability of the requirement

As an example, Requirement 8.1-B contains all four fields:

<table>
<thead>
<tr>
<th>8.1-B – Flashing</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the voting system emits lights in flashes, there must be no more than three flashes in any one-second period.</td>
</tr>
</tbody>
</table>

**Discussion**

This requirement has been updated to meet WCAG 2.0 and Section 508 software design issue standards

- External references: WCAG 2.0/Section 508
- Prior VVSG sources: VVSG 1.1 - 3.2.5.a.i
- Applies to: Electronic interfaces

The **Discussion field** may aid in understanding the requirement but does not itself constitute a requirement.

The optional informative fields show the source of the requirement and to which functions or devices of the voting system it applies:

- **External references**: specifications or laws that are sources for the requirement.
- **Prior VVSG sources**: previous VVSG requirements that the current requirement is updating.
- **Applies to**: indicates the type of voting system function or device to which the requirement applies. This field is used only if the applicability of a requirement is not already clear in the requirement text.
Technical standards used in the requirements

There are a number of technical standards that are incorporated in the Guidelines by reference. These are referred to by title in the body of the document. The full citations for these publications are provided in Appendix B. I

This appendix also includes other references that may be useful for understanding the information.

References in requirements and informative text are linked to Appendix B.

Definitions of terms with special meetings

The requirements contain terms describing function, design, documentation, and testing attributes of voting system hardware, software, and telecommunications. Unless otherwise specified, the intended sense of technical terms is that which is commonly used by the information technology industry. In some cases, terminology is specific to elections or voting systems.

Appendix A contains a glossary of terms. Non-technical terms not listed in Appendix A should be interpreted according to their standard dictionary definitions.

Requirements that use words with special meanings are linked to their definitions in the glossary

Navigating through Requirements

You can navigate through the requirements:

- **From the list of principles and guidelines.** Links in this list go to the requirements that support each principle or guideline.
- **From the list of all requirements in Appendix C.** This list lets you quickly identify requirements in each section. Each title is linked to the requirement text.

In addition, features of the Adobe Acrobat Reader can be useful. More information can be found in Adobe’s help site under *Navigating PDF Pages.*
Conformance Clause

This section provides information and requirements about how manufacturers can use the features of this document to assess whether a voting system conforms to the VVSG Principles and Guidelines. Conformance here means only that the requirements of the VVSG have been met; it does not imply certification according to the EAC’s voting system certification program.

Normative and Informative Language

The text of a requirement is referred to as normative, meaning that the text constitutes the requirement and must be satisfied when implementing and testing the voting device or system. Text in this document that is not part of a requirement is referred to as informative, meaning that it is for informational purposes only and does not contain requirements.

The following keywords are used to convey conformance requirements:

- **Must** indicates a mandatory requirement. Synonymous with "is required to."
- **Must not** also indicates a mandatory requirement, but the requirement is to not do something.
- **May** indicates an optional, permissible action and often suggests one possible way of conforming to a more general requirement.

Requirements are also indicated by the presence of a unique number in the left margin, followed by a descriptive title. Voting systems must meet all requirements to be in conformance with the VVSG Principles and Guidelines.

Informative parts of this document include discussion, examples, extended explanations, and other matters that are necessary to understand the VVSG Principles and Guidelines and how to conform to them. Informative text may serve to clarify requirements, but it is not otherwise applicable to achieving conformance.

Unless otherwise specified, a list of examples should not be interpreted as excluding other possibilities that were not listed.

What is neither required nor prohibited by the language of the requirements is permitted.

Implementation Statement

A voting system conforms to the VVSG Principles and Guidelines if all stated requirements that apply to that voting system and all of its devices are fulfilled. The implementation
statement documents the requirements that have been implemented by the voting system, the optional features and capabilities supported by the voting system, and any extensions (that is, additional functionality) that it implements.

The implementation statement may take the form of a checklist to be completed for each voting system submitted for conformity assessment. It is used by test labs to identify the conformity assessment activities that are applicable.

The implementation statement must include:

- Full product identification of the voting system, including version number or timestamp
- Separate identification of each device that is part of the voting system
- Device capacities and limits
- List of languages supported
- List of accessibility capabilities
- List of voting variations supported
- Devices that support the core functions and how they do it
- List of requirements implemented
- Any extensions also included in the voting system
- Signed document that the information provided accurately characterizes the system submitted for testing

Extensions

Extensions are additional functions, features, or capabilities included in a voting system that are not defined in the requirements. To accommodate the needs of states that may impose additional requirements and to accommodate changes in technology, extensions are permitted. However, an extension is not allowed to contradict or relax requirements that would otherwise apply to the system and its devices.
HIGH QUALITY DESIGN

The voting system is designed to accurately, completely, and robustly carry out election processes.

1.1 - The voting system is designed using commonly-accepted election process specifications.

1.2 - The voting system is designed to function correctly under real-world operating conditions.

1.3 - Voting system design supports evaluation methods enabling testers to clearly distinguish systems that correctly implement specified properties from those that do not.
Principle 1
HIGH QUALITY DESIGN
The voting system is designed to accurately, completely, and robustly carry out election processes.

The requirements for Principle 1 and its guidelines include functional requirements for election definition and preparation through all voting processes concluding with closing of the polls, tabulating, and reporting. The requirements deal with how voting systems are designed to operate during election processes, including limits for stress and volume. Other principles provide more detailed requirements in other areas including accessibility, security, and usability.

The requirements for Guideline 1.1 are arranged into sections by election process with requirements containing the basic core requirements for conducting an election:

1 – Election definition which deals with the capabilities of the voting system to define an election, that is, manage items such as election districts, contests, candidates, and to define ballots for the election that may be specific to various combinations or splits of precincts. Support for the specifications described in the NIST SP 1500-100 common data format (CDF) is required for imports and exports.

2 – Equipment set-up which deals with capabilities of the voting system to configure and verify correctness of devices before opening the polls. Logic and accuracy (L&A) testing is covered here, as well as new requirements to check that cast vote records (CVR) are created properly and that any encoded data such as barcodes is accurately recorded.

3 - Opening the polls which deals with capabilities of the voting system to ensure that the voting system is properly configured so that polls can be opened.

4 - Ballot activation which deals with functions needed to activate the ballot for a voter. If ballot activation occurs on an electronic pollbook, one cannot test and verify whether these requirements are satisfied unless the entire pollbook is also tested.

5 - Casting which deals with the capabilities of the voting system to enable a voter to cast a ballot. The requirements deal with capabilities needed for common vote variations, ballot measures, and write-ins.

6 - Recording voter choices which deals with casting ballots and how equipment will handle ballots as they are cast, including the processes involved in recording votes in cast vote records. It mandates recording the selected contest options, and other information needed for linking the CVR with the device that is creating the CVRs and for auditing.
7 – **Ballot handling for scanners** which deals with functions that scanners will provide, including separating ballots for various reasons, for example, because of write-ins on manually-marked paper ballots and handling mis-fed ballots. It deals with the behavior of batch-fed scanners and voter-facing scanners when scanning ballots that need manual handling or inspection, such as for write-ins or unreadable ballots.

8 – **Closing the polls** which deals with exiting the voting mode (closing the polls), that is, stopping voting and preventing further voting. This applies to those systems located at a remote location such as the polling place.

9 – **Tabulation** which deals with how tabulation processes will handle voting methods, including those methods used most commonly across the United States.

10 – **Reporting results** which deals with the need for the voting system to have the capability to create all required precinct post-election reports. This includes recording ballots such as absentee ballots and Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) ballots.

The requirements for **Guideline 1.2** cover how a voting system is designed to function correctly under real-world operating conditions. They address:

- **Reliability** – the failure rate benchmark for reliability, the need to protect against a single point of failure, and the need for systems to withstand the failure of input and storage devices.
- **Accuracy** – the need to satisfy integrity constraints for accuracy, to achieve the required end-to-end accuracy benchmark, and the ability to reliably detect marks on the ballot.
- **Mid-feed rate** – which treats all misfeeds, such as multiple feeds, jams, and ballot rejections collectively as “misfeeds” and the need to meet the misfeed rate benchmark.
- **Stress** – the ability to respond gracefully to all stresses of the system’s limits.
- **Election volume** – the ability to handle realistic volume of activities in normal use throughout an entire election process.

The requirements for **Guideline 1.3** cover how voting system design supports evaluation methods that enable testers to distinguish system that correctly implement specified properties from those that do not. They include:

- **Identifiability** – so testers can clearly identify the full set of basic and compound elements of the system.
- **System configuration processes** – so testers can understand how particular configurations of process and technology are formed to produce a final working system.
- **Observable configurations** – so testers can detect plausible observational tools and techniques to observe signs of the system configurations.
- **Identifiable resolution limits** – so testers can determine how well the observational tools and techniques can detect and distinguish each type of element in a system configuration.
• **Observational noise and consequences** – so testers can determine what sources of noise will arise from observing a system configuration and be able to map observable signs of those configurations.

• **Performance criteria** – so testers can state criteria that enable them to unambiguously decide whether an observed configuration exhibits intended properties.

• **Evaluation methods** – so testers can derive, construct and execute plausible evaluation methods that can:
  o Observe system configurations using observation tools and techniques
  o Decide whether a configuration has satisfied the performance criteria.
  o Report the findings.
1.1 – The voting system is designed using commonly-accepted election process specifications.

1.1.1 – Election definition

1.1.1-A – Election definition
An election definition must provide the information necessary to hold an election, including accurate information on election districts, contests, candidates, and ballot style information, along with the number of allowable votes for each contest and related rules for voting and tabulating the results.

Discussion
This requirement and its sub-requirements deal with the processes involved in election definition, including ballot definition and layout. It includes capability to:

- import election definition data that can be stored in external databases, and
- export the same data.

It includes the most commonly used voting methods in the United States, including for write-ins, ballot questions, straight party voting, N-of-M contests, cumulative voting contests, proportional voting contests, and ranked choice voting contests.

1.1.1-B – Election definition details
The election definition function must be capable of importing, defining, and maintaining:

1. contests and their associated labels and instructions
2. candidate names and their associated labels
3. ballot measures and their associated text

Discussion
Labels means any headers, footers, or other text that appears on the ballot along with the contest or candidate’s name.

External reference: NIST 1500-100 CDF
Related requirements 1.1.1-Z – Data inputs and outputs
1.1.1-C – Define political geographies
An election definition must clearly describe the political geographies where the list of contests varies between subdivisions. The political geographies include:

1. election districts, including Congressional, state government, and local government that may overlap each other
2. county, city, town and township jurisdictions
3. precincts, splits, and combinations of precincts
4. user-defined geographies

Discussion
User-defined geographies could include non-election districts such as mosquito abatement districts.

1.1.1-D – Serve multiple or split precincts and election districts
An election definition must describe election districts and precincts in such a way that a given polling place may serve:

1. two or more election districts
2. combinations of precincts and split precincts

Discussion
This requirement addresses the capability of precinct devices to be flexible in accommodating multiple ballot styles depending on the political geography being served by a polling place.

1.1.1-E – Identifiers
An election definition must enable election officials (EOs) to associate multiple identifiers that can be cross-referenced with each other for administrative subdivisions, election districts, contests, and candidates, including for:

1. locally-defined identifiers
2. state-wide-defined identifiers
3. Open Civic Data Identifiers (OCD-IDs)

Discussion
This is based on the need to support cross-referencing of statewide identifier schemes or schemes such as OCD-IDs with those used on a more local level.
1.1.1-F – Definition of parties and contests
An election definition must allow for:

1. the definition of political parties and indicate the affiliation or endorsements of each contest option
2. information on both party-specific and non-party-specific contests, with the capability to include both contests on the same ballot
3. contests that include ballot positions with write-in opportunities

1.1.1-G – Voting methods
An election definition must enable election officials to define and identify contests, contest options, candidates, and ballot questions using all voting methods indicated in the manufacturer-provided implementation statement.

1. For N-of-M contests, an election definition must be capable of defining contests where the voter is allowed to choose up to a specified number of contest options from a list of options.

2. For ballot questions, an election definition must include the ability to create ballot questions where the voter is allowed to vote yes or no on a question.

3. For ballot questions, an election definition must include the ability to create ballot questions where the voter is allowed to vote on one or more from a list of possible choices on a question.

4. For the cumulative voting method, an election definition must include the ability to create ballot questions where the voter is allowed to allocate up to a specified number of votes over a list of contest options, possibly giving more than one vote to a given option.

5. For the proportional voting method, an election definition must include the ability to create ballot questions where the candidate gets the number of votes equal to those allowed divided by number of selections.

6. For the ranked choice voting method, an election definition must include the ability to create ballot questions where the voter is allowed to rank contest options in order of preference, as first choice, second choice, etc.

7. For the cross-party endorsement voting method, an election definition must include the ability to create ballot questions about the necessary straight party contest and record the endorsements made by each party in the election definition. This supports gathering and recording votes for the slate of contest options endorsed by a given
political party when a given contest option is endorsed by two or more different political parties.

1.1.1-H – Election definition accuracy
An election definition must record the election contests, contest options, issues, and political and administrative subdivisions exactly as defined by EOs.

1.1.1-I – Voting options accuracy
An election definition must record the options for casting and recording votes exactly as defined by EOs.

1.1.1-J – Confirm recording of election definition
An election definition must check and confirm that its data is correctly recorded to persistent storage.

**Discussion**

"Persistent storage" includes storage systems such as nonvolatile memory, hard disks, and optical disks.

1.1.1-K – Election definition distribution
An election definition must provide for generating master and distributed copies of election definitions as needed to configure each voting device in the system.

1.1.1-L – Define ballot styles
An election definition must enable EOs to define ballot styles.

1.1.1-M – Auto-format
An election definition must be capable of automatically formatting ballots according to jurisdictional requirements for office and contest options qualified to be placed on the ballot for each political subdivision and election district.

1.1.1-N – Include contests
An election definition must provide for the inclusion in a given ballot style of all contests in which the voter would be entitled to vote.
1.1.1-O – Exclude contests
An election definition must provide for the exclusion from a given ballot style of any contest in which the voter would be prohibited from voting because of place of residence or other administrative criteria.

Discussion
In systems supporting primary elections, this would include the exclusion of party-specific contests that voters in a particular political party are not eligible to vote in.

1.1.1-P – Nonpartisan formatting
An election definition must support the uniform allocation of space and fonts used for each office, contest option, and contest so the voter does not perceive that one contest option is preferred over any other.

1.1.1-Q – Jurisdiction-dependent content
An election definition must enable EOs to add jurisdiction-dependent text, line art, logos, and images to ballot styles.

1.1.1-R – Primary elections, associate contests with parties
When implementing primary elections, an election definition must support the association of different contests with different political parties.

1.1.1-S – Ballot rotation
When implementing ballot rotation, an election definition must support producing rotated ballots or activating ballot rotation functions in vote-capture devices by including relevant metadata in distributed election definitions and ballot styles.

Related requirement: 1.1.5-I – Ballot rotation for contest options

1.1.1-T – Ballot configuration in combined or split precincts
When implementing combined or split precincts, an election definition must include the ability to create distinct ballot configurations for voters from two or more election districts that are served by a given polling place.
1.1.1-U – No advertising
The ballot presented to the voter must not display or link to any advertising or commercial logos of any kind, whether public service, commercial, or political.

1.1.1-V – Ballot style distribution
An election definition must include the option to generate master and distributed copies of ballot styles as needed to configure each voting device in the system.

1.1.1-W – Ballot style identification
An election definition must generate codes or marks as needed to uniquely identify the ballot style associated with any ballot.

Discussion
In paper-based systems, identifying marks would appear on the actual ballots. Electronic ballot markers would make internal use of unique identifiers for ballot styles but would not necessarily present these where the voter would see them. In both cases, the identifying mark also could be recorded in the cast vote record.

1.1.1-X – Retaining, modifying, reusing definitions
An election definition must support retaining, modifying, and reusing general districting or precinct definitions and ballot formatting parameters within the same election and from one election to the next.

1.1.1-Y – Ballot style protection
An election definition must prevent unauthorized modification of any ballot styles.

Discussion
See security requirements for information on techniques to prevent unauthorized modifications.

1.1.1-Z – Data inputs and outputs
An election definition must support NIST 1500-100 CDF specifications for election programming data inputs and outputs, including for:

1. import of election programming data
2. export of election programming data
3. reports of election programming data to ensure the data is inspected and verified
Discussion

Item 1 concerns import of pre-election data such as for identification of political geography, contest, candidate, ballot data, and other pre-election information used to setup an election and produce ballots. Items 2 and 3 refer to exporting and reporting the pre-election data from the election definition device so that it can be checked for accuracy or exchanged as needed.

<table>
<thead>
<tr>
<th>External reference:</th>
<th>NIST 1500-100 CDF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Related requirements</td>
<td>1.1.1-B – Election definition details</td>
</tr>
</tbody>
</table>

1.1.2 – Equipment setup

1.1.2-A – Equipment setup

The voting system must provide the capability to verify that:

1. all voting devices are properly prepared for an election using real world scenarios and collect data that verify equipment readiness
2. all system equipment is correctly installed and interfaced
3. hardware and software function correctly

Discussion

This requirement and its sub-requirements deal with equipment setup prior to the election. They deal primarily with logic and accuracy testing (L&A), whose purpose is to detect malfunctioning and misconfigured devices before polls are opened. Election personnel conduct equipment and system readiness tests before an election to:

- ensure that the voting system functions properly,
- confirm that system equipment has been properly integrated, and
- obtain equipment status and readiness reports.

The intent is that the voting system and devices be configured so real-world configuration scenarios will be supported and testable.

1.1.2-B – Built-in self-test and diagnostics

The voting system must include built-in measurement, self-testing, and diagnostic software and hardware for monitoring and reporting the system’s status and degree of operability.
1.1.2-C – Verify proper preparation of ballot styles
An election definition must allow for EOs to test that ballot styles and programs have been properly prepared.

1.1.2-D – Verify proper installation of ballot styles
The voting system must include the capability to automatically verify that the software and ballot styles have been properly selected and installed in the equipment and can immediately notify an EO of any errors.

Discussion
At a minimum, notification means an error message, a log entry, and a “failed” result on this portion of the L&A test. Examples of detectable errors include use of software or data intended for a different type of device or operational failures in transferring the software or data.

1.1.2-E – Verify compatibility between software and ballot styles
The voting system must include the ability to automatically verify that software correctly matches the ballot styles that it is intended to process and immediately notify an EO of any errors.

Discussion
At a minimum, notification means an error message, a log entry, and a "failed" result on this portion of the L&A test.

1.1.2-F – Test ballots
The voting system must allow for EOs to submit test ballots for use in verifying the integrity of the system.

1.1.2-G – Test all ballot positions
Scanners must allow for testing that uses all potential ballot positions as active positions.

1.1.2-H – Test Cast Vote Records
The voting system must include the ability to verify that CVRs are created and tabulated correctly by permitting EOs to compare the created CVRs with the test ballots.

Discussion
This requires providing a capability such as an export of CVRs and a tabulated summary that can be compared manually against their test ballot counterparts.
1.1.2-I – Test codes and images
The voting system must include the ability to verify that any encoded version or images of voter selections on a ballot are created correctly.

Discussion
The purpose is to ensure that an encoded version of voter selections such as provided by a ballot marking device (BMD) using QR codes contains the voter’s selections exactly as made. It will also ensure that any image of the ballot made by a scanner correctly matches the ballot. BMDs may encode other items as appropriate in codes, for example, ballot style ID.

1.1.2-J – Testing calibration
Scanners must support the use of test ballots to test the calibration of the paper-to-digital conversion (such as the calibration of optical sensors, the density threshold, and the logical reduction of scanned images to binary values, as applicable).

1.1.2-K – Ballot marker readiness
Ballot marking must allow for a way to verify that the ballot marking mechanism is properly prepared and ready to use.

1.1.2-L – L&A testing, no side-effects
Logic and accuracy testing functions must introduce no lasting effects on operation during the election other than:

1. audit log entries
2. status changes to note that the tests have been run with a successful or failed result
3. separate storage of test results
4. changes in the protective counter or life-cycle counter (if the device has one)
5. normal wear and tear

Discussion
Subsequent requirements preclude the device from actually serving in the election unless these tests are successful. Apart from that safeguard, it should be impossible (by design) for the L&A testing to have any influence on the operation of the device during the election or on the results that are reported for the election. Most notably, election results can never include any test votes that were counted during L&A testing.
1.1.2-M – Status and readiness reports
The voting system must provide the capability to produce status and equipment readiness reports.

Discussion
These reports typically are generated during pre-voting logic and accuracy testing.

1.1.2-N – Pre-election reports
The voting system must provide the capability to produce a report that includes:

1. The allowable number of votes in each contest
2. The counting logic (for example, N-of-M, cumulative, or ranked choice) that is used for each contest
3. The inclusion or exclusion of contests as the result of precinct splits
4. Any other characteristics that may be peculiar to the jurisdiction, the election, or the precincts
5. Manual data maintained by election personnel
6. Samples of all final ballot styles
7. Ballot preparation edit listings

Discussion
The purpose of this requirement is for sanity checks of the election configuration. Previous requirements mandate support for the NIST 1500-100 CDF specification.

External reference: NIST 1500-100 CDF specification

1.1.2-O – Readiness reports for each polling place
Readiness reports must include at least the following information for each polling place:

1. The election's identification data
2. The identification of the precinct and polling place
3. The identification of all voting devices deployed in the precinct
4. The identification of all ballot styles used in that precinct
5. Confirmation that no hardware or software failures were detected during setup and testing, or a record of those that occurred
6. Confirmation that all vote-capture devices are ready for the opening of polls, or identification of those that are not

1.1.2-P – Readiness reports, precinct tabulation
Readiness reports must include the following information for each voter-facing scanner or other precinct reporting device:

1. The election's identification data
2. The identification of the precinct and polling place
3. The identification of the voter-facing scanner
4. The contents of each active contest option register at all storage locations
5. Confirmation that no hardware or software failures were detected during setup and testing, or a record of those that occurred
6. Any other information needed to confirm the readiness of the equipment and to accommodate administrative reporting requirements

1.1.2-Q – Readiness reports, central tabulation
Readiness reports must include the following information for each batch-fed scanner or other central reporting device:

1. The election's identification data
2. The identification of the tabulator
3. The identification of all ballot styles used in the system extent
4. The contents of each active contest option register at all storage locations
5. Confirmation that no hardware or software failures were detected during setup and testing, or a record of those that occurred
6. Any other information needed to confirm the readiness of the equipment and to accommodate administrative reporting requirements

1.1.2-R – Readiness reports, public network test ballots
Systems that send ballots over a public network must provide a report of test ballots that includes:

1. the number of test ballots sent
2. when each test ballot was sent
3. the identity of the machine from which each test ballot was sent
4. the specific votes contained in the test ballots

1.1.3 – Opening the Polls

1.1.3-A – Opening the polls
The voting system must provide functions to enter and exit a mode in which voting is permitted.

Discussion
This and following requirements cover the process of enabling voting to occur by placing the voting system in a voting mode.

1.1.3-B – Verify L&A performed
The voting system must provide internal test or diagnostic capabilities to verify that the applicable tests specified in the equipment setup requirements have been successfully completed.

Discussion
When an L&A test is conducted, that test will indicate whether any aspects of the test were successful or failed.

1.1.3-C – Prevent opening the polls
The voting system must not enter the voting mode unless and until the readiness test has been performed successfully and any steps necessary to isolate test data from election data have been performed successfully.

Discussion
If a device has not been tested, has failed its L&A test, or the test data have not been isolated (that is, test votes could end up being included in election results), then the device is not ready for use in the election.
1.1.3-D – Non-zero totals
Tabulation must not enter the voting mode unless and until the L& A test has been performed successfully, any steps necessary to isolate test data from election data have been performed successfully, and all vote counters have been zeroed. An attempt to open polls with non-zero totals:

1. must be recorded in the audit log
2. an EO must be clearly notified of the event

Discussion
Jurisdictions that allow early voting before the traditional election day should note that a distinction is made between the opening and closure of polls, which can occur only once per election, and the suspension and resumption of voting between days of early voting. The open-polls operation, which requires zeroed counters, is performed only when early voting commences; the resumption of voting that was suspended overnight does not require that counters be zeroed again.

1.1.3-E – Scanners and ballot marking devices - verify activation
Scanners and ballot marking devices must include a means of verifying that they have been correctly activated and are functioning properly.

1.1.3-F – Scanners and ballot marking devices - enter voting mode
Scanners and ballot marking devices must provide designated functions for entering voting mode. They must include:

1. access control to prevent the inadvertent or unauthorized activation of the poll-opening function.
2. a means of enforcing the execution of poll-opening steps in the proper sequence if more than one step is required.
3. a means of verifying that the system has been correctly activated.

1.1.4 - Ballot Activation
This section deals with functions needed to activate the ballot for a voter. If ballot activation occurs on an electronic pollbook, one cannot test and verify whether these requirements are satisfied unless the entire pollbook is also tested.
1.1.4-A – Ballot activation
The voting system must support ballot activation.

1.1.4-A.1 – One cast ballot per session
The voting system must enable election workers either to initiate or to provide the voter with the credentials sufficient to initiate a voting session in which the voter may cast or print at most one ballot.

Discussion
A voting session on a BMD may end with the printing of the voter’s contest selections, that is, scanning contest selections need not be considered part of the voting session.

1.1.4-A.2 – Contemporaneous record
The voting system must create contemporaneous records of the credentials issued to a voter. The record, once made, will not be able to be modified by the voting system.

Discussion
The voting system creates a record at the time when credentials are issued to voters so that the records collected can be compared to the number of ballots voted. This may be done if the activation device prints a record or by using a paper pollbook.

1.1.4-A.3 – Control ballot configuration
The voting system must enable election workers to control the ballot configurations made available to the voter, whether presented in printed form or electronic display, so that each voter is permitted to record votes only in contests in which that voter is authorized to vote. The voting system must:

1. activate all portions of the ballot the voter is entitled to vote on.
2. disable all portions of the ballot the voter is not entitled to vote on.
3. enable the selection of the ballot configuration that is appropriate to the party affiliation declared by the voter in a primary election.

Discussion
For an electronic display, poll workers control the ballot configuration using an activation device and issuing credentials. In paper-based systems, open primaries have sometimes been handled by printing a single ballot style that merges the contests from all parties, instructing the voter to vote only in the contests applicable to a single party, and rejecting or discarding votes that violate this instruction. To use that approach on a paper-based BMD would violate this requirement.
1.1.5 - Casting

1.1.5-A – Voting methods when casting
The voting system must record all individual contest options for each contest using all voting methods indicated for them in the implementation statement.

Discussion
This requirement and its sub-requirements deal with general support for casting ballots using the most common voting methods used in the United States. (Voting methods are otherwise known as voting variations.) When a ballot is cast, the voting system will create an electronic record of the voter’s selections, that is, a cast vote record. The cast vote record need not include those contest options not selected by the voter; their absence in the cast vote record indicates their non-selection.

1.1.5-B – N-of-M voting
For the N-of-M voting method, the voting system must be capable of gathering and recording votes in contests where the voter is allowed to choose up to a specified number of contests from a list of contest options.

1.1.5-C – Yes/no measures and multiple-choice measures
For ballot measures, the voting system must be capable of gathering and recording votes in contests where the voter is allowed to:

1. vote yes or no on a measure
2. vote for selections from a list of choices

1.1.5-D – Indicate party affiliations and endorsements
The voting system must be capable of indicating the affiliation or endorsements of each contest option.

1.1.5-E – Closed primaries
For closed primaries, the voting system must be capable of gathering and recording votes within a voting process that:
1. assigns different ballot styles depending on the registered political party affiliation of the voter

2. supports both party-specific and non-party-specific contests

1.1.5-F – Open primaries
For open primaries, the voting system must be capable of gathering and recording votes within a voting process that assigns different ballot styles depending on the political party chosen by the voter at the time of voting and supports both party-specific and non-party-specific contests.

Discussion
In paper-based systems, open primaries have sometimes been handled by printing a single ballot style that merges the contests from all parties, instructing the voter to vote only in the contests applicable to a single party, and rejecting or discarding votes that violate this instruction.

1.1.5-G – Write-ins
The voting system must record the voter’s write-in of candidates whose names do not appear on the ballot and record as many write-in votes as the voter is allowed.

1.1.5-H – Write-in reconciliation
The voting system must be capable of gathering and recording votes within a voting process that allows for reconciliation of aliases and double votes resulting from write-ins.

Discussion
Reconciliation of aliases means allowing EOs to declare two different spellings of a candidate’s name to be equivalent (or not), as could happen from write-ins. Reconciliation of double votes means handling the case where, in an N-of-M contest, a voter has attempted to cast multiple votes for the same candidate using the write-in mechanism.

1.1.5-I – Ballot rotation for contest options
For ballot rotation, the voting system must be capable of gathering and recording votes when the ordering of contest options in ballot positions within each contest is variable in such a manner that does not show bias to any contest option.

Discussion
The intent is to ensure that the manner in which the rotation algorithm works does not show bias towards any candidate, that is, all contest options appear equally in rotated positions to the extent possible.

1.1.5-J – Straight party voting
For straight party voting, the voting system must be capable of gathering and recording votes for a special contest in which the selection of a political party implies votes for the contest options endorsed by that party in all straight-party contests on the ballot.

1.1.5-K – Cross-party endorsement
For cross-party endorsement, the voting system must be capable of gathering and recording straight-party votes when a given contest option is endorsed by two or more different political parties.

1.1.5-L – Precinct splits
The voting system must be capable of gathering and recording votes in a polling place where there are distinct ballot styles for voters from two or more political geographies.

1.1.5-M – Cumulative voting
For cumulative voting, the voting system must be capable of gathering and recording votes in contests where the voter is allowed to allocate up to a specified number of votes over a list of contest options, possibly giving more than one vote to a given contest option.

1.1.5-N – Ranked choice voting
For ranked choice voting, the voting system must be capable of gathering and recording votes in contests where the voter is allowed to rank contest options in a contest in order of preference, as first choice, second choice, etc.

1.1.5-O – Recallable ballots
The voting system must be capable of gathering and recording votes within a voting process that allows the decision of whether to count a particular ballot to be deferred until after election day.

Discussion
Unique identification of each recallable ballot is needed.
1.1.5-P – Review-required ballots
The voting system must be capable of gathering and recording votes within a voting process that requires certain ballots to be flagged or separated for review.

Discussion
In some systems and jurisdictions, all ballots containing write-in votes require flagging or separation for review. Support for this indicates that the system can flag or separate ballots in this manner and include the results of the review in the reported totals. Other reasons for which ballots are flagged or separated are jurisdiction-dependent.

1.1.6 – Recording Voter Choices

1.1.6-A – Casting and recording
All systems must support casting a ballot and recording each vote precisely as indicated by the voter, subject to the rules of the election jurisdiction.

1.1.6-B – Secure ballot boxes
Voting systems that include paper ballots must include secure receptacles for holding cast ballots.

1.1.6-C – Prevent counter overflow
When the voting system can no longer accept another ballot without the potential of overflowing a vote counter or otherwise compromising the integrity of the counts, it must notify the user or operator and cease to accept new ballots.

Discussion
Assuming that the counter size is large enough that the value will never be reached is not an adequate safeguard. Systems are required to detect and prevent an impending overflow condition. This requirement is in response to past issues in which devices would use up available memory but give no warning and continue to permit voters to cast ballots.

1.1.6-D – Ballot orientation
Ballot marking devices that use pre-printed ballots must either:

1. correctly mark pre-printed ballots regardless whether they are loaded upside down, right side up, forward, or reversed
2. detect and reject pre-printed ballots that are oriented incorrectly

1.1.6-E – Records consistent with feedback to voter

All CVRs and logs must be consistent with the feedback they give to the voter.

Discussion

This does not mean that every message displayed to the voter during an interactive session will be included in every CVR or log. It means that the records and the interactive messages will not be in conflict with one another. For example, it is not permissible to show a vote for candidate X on the display, and then record a vote for candidate Y.

1.1.6-F – Record contest selection information

The voting system must record contest selection information in the CVR that includes:

1. all contest selections made by the voter for all supported vote variations
2. positions on the ballot associated with each contest selection made by the voter, including when multiple selections are permitted, if applicable

1.1.6-G – Record write-in information

The voting system must record write-in information in the CVR that includes:

1. identification of write-in selections made by the voter
2. the text of the write-in, when using a BMD or other device that marks the ballot for the voter
3. an image or other indication of the voter’s write-in markings
4. an indication whether the write-in has been adjudicated and constitutes a tabulatable vote
5. the total number of write-ins in the CVR

1.1.6-H – Record election and contest information

The voting system must record additional contest information in the CVR that includes:

1. identification of all contests in which voter has made a contest selection
2. identification of the contest vote method including number of votes allowed in the contest and the maximum number of valid contest selections
3. identification of all overvoted and undervoted contests
4. the number of write-ins recorded for the contest
5. identification of the party for partisan ballots or partisan contests

**Discussion**

For identification of the party, a ballot in a partisan primary may in some cases contain contests for different parties. Thus, an indication as to whether the contest is partisan is required.

**1.1.6-I – Record ballot selection override information**

Scanners, if tabulating voter selections differently than as marked due to election or contest rules in effect, must record information in the CVR that includes:

1. identification of the original ballot selections made by the voter
2. identification of the changed voter selections
3. identification of the reasons for the changes

**Discussion**

When marking a ballot by hand, a voter may vote in contests in which the voter is not allowed to make contest selections. For example, a voter may elect to vote straight party, but then make contest selections in contests anyway. Election or contest rules may cause a scanner to invalidate the contest markings or require other actions.

**1.1.6-J – Record detected mark information**

Scanners must record, for each mark detected on the ballot, information in the CVR that includes:

1. indications of marginal marks that are made by the voter or that are due to imperfections on the ballot
2. mark quality information for each detected mark

**Discussion**

This applies to contest selections recognized as valid as well as to marginal marks or other detected facets of contest selection positions that are detected by the scanner. For example, a crease in the ballot may be detected by the scanner as a marginal mark. The measurement of mark quality may be specific to manufacturer and model of scanner.
1.1.6-K – Record audit information
The voting system must be capable of recording audit-related information in the CVR or collection of CVRs as they are created, that includes:

1. identification of the specific creating device such as a serial number
2. identification of the geographical location of the device
3. Identification of the ballot style corresponding to the CVR
4. identification of the corresponding voted ballot
5. for multi-sheet ballots, identification of the individual sheet corresponding to the CVR, along with the identification of the ballot style
6. identification of the batch containing the corresponding voted ballot, when applicable
7. sequence of the corresponding voted ballot in the batch, when applicable

Discussion
Item 4 can be satisfied by printing a unique ID on the ballot as it is scanned and including that ID in the corresponding CVR.

Item 5 ensures that every sheet of a multi-sheet ballot contains the sheet number as well as the ballot style ID. This way, a ballot style ID could be defined to include all sheets, or each sheet could be defined with a unique ballot style.

Items 6 and 7 are necessary when ballot batching is in effect.

1.1.7 – Ballot handling for paper ballot scanners

1.1.7-A – Ballot handling functions for scanners
Scanners must provide features for handling ballots when they are scanned individually using voter-facing scanners or scanned in batches using batch-fed scanners.

1.1.7-B – Detect and prevent ballot style mismatches
All voting systems must detect ballot style mismatches and prevent votes from being tabulated or reported incorrectly due to a mismatch.

Discussion
For example, if the ballot styles loaded on a scanner disagree with the ballot styles that were used by vote-capture devices, the system will raise an alarm and prevent the incorrect ballot styles from being used during tabulation. Otherwise, votes could be ascribed to the wrong contest options.

Such a mismatch should have been detected and prevented in L&A testing but if it was not, it needs to be detected and prevented before tabulation begins.

1.1.7-C – Detect and reject ballots that are oriented incorrectly
Scanners must do one of the following:

1. correctly count ballots regardless of whether they are fed upside down, right side up, forward, or reversed
2. detect and reject ballots that are oriented incorrectly

1.1.7-D – Ballot separation when batch feeding
In response to unreadable ballots, write-ins, and other designated conditions, batch-fed scanners must do one of the following:

1. out stack the ballot (that is, divert to a stack separate from the ballots that were normally processed)
2. stop the ballot reader and display a message prompting the EO to remove the ballot
3. mark the ballot with an identifying mark to facilitate its later identification

Discussion
The requirement to separate ballots containing write-in votes is not applicable in systems in which a BMD encodes write-in votes in machine-readable form and a scanner generates individual tallies for all written-in candidates automatically. Separation of ballots containing write-in votes is only necessary in systems that require the allocation of write-in votes to specific candidates to be performed manually.

1.1.7-E – Overvotes, undervotes, blank ballots
Voter-facing scanners must provide a capability that can be activated by EOs to stop the scanning and display a message to the EO to remove and correct the ballot in response to the following ballot conditions:

1. ballots containing overvotes in a designated contest
2. ballots containing undervotes in a designated contest
3. ballots containing contests that were not voted
4. blank ballots

1.1.7-F – Write-ins
When scanning a ballot containing a write-in vote, voter-facing scanners must segregate the ballot in a manner that facilitate its later identification.

Discussion
The requirement to separate ballots containing write-in votes is not applicable in systems in which a BMD encodes write-in votes in machine-readable form and a scanner generates individual tallies for all written-in candidates automatically. Separation of ballots containing write-in votes is only necessary in systems that require the allocation of write-in votes to specific candidates to be performed manually.

1.1.7-G – Ability to clear misfeed
If multiple feed or misfeed (jamming) occurs, a batch-fed scanner must:

1. halt in a manner that permits the operator to remove the ballots causing the error and reinsert them in the input hopper (if unread) or insert them in the ballot box (if read)
2. indicate whether or not the ballots causing the error has been read

Discussion
The second bullet deals with whether a CVR has been created for the ballots that jammed; EOs needs to know whether to re-feed the ballot.

1.1.7-H – Scan to manufacturer specifications
Scanners must detect marks made on paper ballots according to non-proprietary, published manufacturer specifications.

Discussion
Manufacturers will publish their specifications for detecting marks, and these specifications will be publicly available. Because voters may make any number of mistakes when marking a ballot, cannons need to interpret the marks according to these published specifications as well as possible. Requirements in the Casting section require the manufacturer to include, in the CVR, an indication of mark quality for each detected mark.

1.1.7-I – Ignore unmarked contest option positions
Scanners must ignore (that is, not record as votes) unmarked contest option positions.
Discussion

"Unmarked" in this requirement means containing no marks of any kind other than those designed to be present as part of the ballot style. This includes extraneous perforations, smudges, folds, and blemishes in the ballot stock.

1.1.7-J – Accurately detect perfect marks
Scanners must detect marks that conform to manufacturer specifications.

1.1.7-K – Accurately detect imperfect marks
Scanners must detect a 1 mm thick line that:

1. is made with a #2 pencil that crosses the entirety of the contest option position on its long axis,
2. is centered on the contest option position
3. is as dark as can practically be made with a #2 pencil

Discussion

Different optical scanning technologies will register imperfect marks in different ways. Variables include:

- the size, shape, orientation, and darkness of the mark;
- the location of the mark within the voting target;
- the wavelength of light used by the scanner;
- the size and shape of the scanner's aperture;
- the color of the ink;
- the sensed background-white and maximum-dark levels; and,
- the calibration of the scanner.

The mark specified in this requirement is intended to be less than 100% perfect, but reliably detectable, that is, not so marginal as to bring the uncontrolled variables to the forefront. In plain language: scanning technologies may vary, but as a minimum requirement, all of them should be capable of reliably reading this mark.
1.1.7-L – Ignore extraneous marks outside contest option position
Scanners must not record as votes any marks, perforations, smudges, or folds appearing outside the boundaries of contest option positions.

1.1.7-M – Ignore extraneous marks inside voting targets
Scanners must not record as votes any imperfections in the ballot stock, folds, and similar insignificant marks appearing inside voting targets.

Discussion
Insignificant marks appearing inside voting targets can be detected as votes. This problem should be minimized.

1.1.7-N – Ignore hesitation marks
Scanners must not record hesitation marks and similar insignificant marks as votes.

Discussion
It may be possible to reliably detect reasonable marks and reliably ignore hesitation and other insignificant marks if the scanner is calibrated to a specific marking utensil or, when an image is made of the ballot, analysis of the image.

1.1.7-O – Marginal marks, no bias
The detection of marginal marks from manually-marked paper ballots must not show a bias.

Discussion
Bias errors are not permissible in any system. An example of bias would be if marginal marks in the first ballot position were detected differently than marginal marks in the second ballot position.

1.1.7-P – Repeatability
The detection of marginal marks from manually-marked paper ballots must be repeatable.

Discussion
It is difficult to have confidence in the equipment if consecutive readings of the same ballots on the same equipment yield dramatically different results. However, it is technically impossible to achieve repeatable reading of ballots containing marks that fall precisely on the sensing threshold.
1.1.8 – Closing the Polls

1.1.8-A – Closing the polls
The voting system must provide designated functions for exiting election mode and stopping voting.

Discussion
When voting is conducted across multiple days, for example, for early voting, these requirements are still applicable even though the election itself may not be over, with the exception of requirement 1.1.8-E – Prevent reopening polls, which deals with preventing, on election day, re-opening of the polls once they have been closed.

1.1.8-B – No voting when polls are closed
The voting system must prevent the further enabling, activation, marking, or casting of ballots by any device once the polls have closed.

Discussion
A BMD cannot prevent a voter from marking a paper ballot with a writing utensil after polls have closed. This needs to be prevented through procedures.

1.1.8-C – Poll closing integrity check
The voting system must provide an internal test that verifies that the prescribed closing procedure has been followed and that the device status is normal.

1.1.8-D – Report on poll closing process
The voting system must provide a means to produce a diagnostic test record that verifies the sequence of events and indicates that the poll closing process has been activated.

1.1.8-E – Prevent reopening polls
The voting system must prevent reopening of the polls once the poll closing has been completed for an election.

Discussion
For early voting conducted across multiple days, this requirement does not prevent reopening of the polls on the following day. This requirement is only applicable on the final day of election.

1.1.9 – Tabulation

1.1.9-A – Voting methods when tabulating
Tabulation must support all voting methods indicated in the implementation statement.

1.1.9-B – N-of-M voting
For N-of-M voting, tabulation must be capable of tabulating votes, overvotes, and undervotes in contests where the voter is allowed to choose up to a specified number of contest options from a list of contest options.

1.1.9-C – Yes/no measure and multiple-choice measure
For yes/no measures and multiple-choice measures, tabulation must be capable of tabulating votes, overvotes, and undervotes in contests where the voter is allowed to:

1. vote yes or no on a measure
2. choose from a list of multiple choices on a measure

1.1.9-D – Recallable ballots
For recallable ballots, tabulation must be capable of tabulating votes, overvotes, and undervotes in contests where the decision whether to count a particular ballot is deferred until after election day.

1.1.9-E – Accept or reject recallable ballots individually
Tabulation must support the independent acceptance and rejection of individual recallable ballot.

**Discussion**

This is meant to rule out the mode of failure in which the IDs assigned to provisional ballots fail to be unique, rendering the system incapable of accepting one without also accepting the others with the same ID.

1.1.9-F – Accept or reject recallable ballots by category
Tabulation must support the acceptance and rejection of recallable ballots by category.
1.1.9-G – Primary elections
For primary elections, tabulation must be capable of keeping separate totals for each political party for the number of ballots read and counted.

Discussion
In paper-based systems, open primaries have sometimes been handled by printing a single ballot style that merges the contests from all parties and instructing the voter to vote only in the contests applicable to a single party. This approach requires additional logic in the tabulator to support rejecting or discarding votes that violate these special instructions, while the approach of assigning different ballot configurations to different parties does not. Support for the merged ballot approach is not required for a tabulator.

This requirement to separate by party applies only to the number of read ballots and counted ballots. It does not apply to contest option vote totals.

1.1.9-H – Write-ins
For write-ins, tabulation must be capable of tabulating votes for write-in candidates, with separate totals for each candidate.

1.1.9-I – Support write-in reconciliation
For write-ins, tabulation must be capable of tabulating votes within a voting process that allows for reconciliation of aliases and double votes.

Discussion
Reconciliation of aliases means allowing EOs to declare two different spellings of a candidate's name to be equivalent (or not). Reconciliation of double votes means handling the case where, in an N-of-M contest, a voter has attempted to cast multiple votes for the same candidate using the write-in mechanism.

1.1.9-K – Ballot rotation
Tabulation must be capable of tabulating votes when the ordering of contest options in ballot positions within each contest is variable.

Discussion
This simply means that ballot rotation will not impact the correctness of the count.

1.1.9-L – Straight party voting
Tabulation must be capable of tabulating straight party votes.
1.1.9-M – Tabulating straight party votes
A straight party vote must be counted as a vote in favor of all contest options endorsed by the chosen party in each straight-party-voting contest in which the voter does not cast an explicit vote.

**Discussion**
This requirement intentionally says nothing about what happens when there is both a straight party endorsed contest option and an explicit vote in a given contest (a straight party override). Jurisdictions may handle this in various ways, including to void the ballot or contest.

1.1.9-N – Cross-party endorsement
For cross-party endorsement, tabulation must be capable of tabulating straight-party votes when a given contest option is endorsed by two or more different political parties.

1.1.9-O – Precinct splits
Tabulation must be capable of tabulating votes for precinct splits or combinations of precincts.

1.1.9-P – Cumulative voting
For cumulative voting, tabulation must be capable of tabulating votes, overvotes, and undervotes in contests where the voter is allowed to allocate up to a specified number of votes over a list of contest options however they choose, possibly giving more than one vote to a given contest option.

1.1.9-Q – Ranked choice voting
For ranked choice voting, tabulation must be capable of determining the results of a ranked choice contest for each round of tabulation.

**Discussion**
This requirement is minimal. Since ranked choice voting is not currently in wide use, it is not clear what, other than the final result, will be computed.
1.1.10 – Reporting Results

1.1.10-A – Post-election reports
The voting system must have the capability to create precinct post-election reports.

1.1.10-B – Reporting device consolidation
When more than one vote-capture device or voter-facing scanner is used, it must be possible to consolidate the data contained in each unit into a single report for the polling place. If the consolidation of polling place data is done locally, the precinct reporting device needs to perform this consolidation in no more than 5 minutes per scanner.

Discussion
This requirement essentially requires precinct-based vote capture devices to be able to consolidate voting data for the purposes of issuing one consolidated report.

1.1.10-C – Reporting is non-destructive
The voting system must prevent data, including data in transportable memory, from being altered or destroyed by report generation.

Discussion
Appending an audit record reflecting the fact that a report has been generated is not considered an alteration.

1.1.10-D – Ballot and vote counts
The voting system must be capable of generating human-readable reports of the vote and ballot count, including the capability for:

1. alphanumeric headers
2. election, office, and issue text
3. alphanumeric entries generated as part of the audit record

Discussion
This requirement and its sub-requirements specify a minimum set of information that a voting system will report. They do not prohibit any voting system from reporting additional information that may be required by jurisdictions or otherwise found to be useful.
1.1.10-E – Report all votes cast
All systems must be able to produce an accurate, human-readable report of all votes cast.

**Discussion**

Binary document formats and text containing markup tags are not considered human-readable. The system may generate such documents, but it must also provide the functionality to render those documents in human-readable form (for example, by including the necessary reader application).

1.1.10-F – Account for all cast ballots and all valid votes
All systems must produce vote data reports that account for all cast ballots and all valid votes.

1.1.10-G Discrepancies detectable
Any discrepancy that is detectable by the system must be flagged in the system by an annotation or error message in the affected report or a separate discrepancy report.

**Discussion**

If this requirement is applicable, then the system has failed to satisfy Requirement 1.1.10-G and is therefore non-conforming. Nevertheless, in practice it is essential that discrepancies be flagged by the system as much as possible so that they are not overlooked by election judges. The system cannot detect discrepancies if no single voting device is ever in possession of a sufficient set of data.

1.1.10-H – Reporting combined precincts
The voting system must be capable of generating reports that consolidate vote data from selected precincts.

**Discussion**

Jurisdictions in which more than one precinct may vote at the same location on either the same ballot style or a different ballot style may desire reports that consolidate the voting location.

1.1.10-I – Precinct reporting devices, no tallies before polls close
The voting system must prevent the printing of vote data reports and extracting vote tally data before the polls close.

**Discussion**

Providing ballot counts does not violate this requirement. The prohibition is against providing vote totals. Ballot counts are required for ballot accounting, but early extraction of vote totals is an enabler of election fraud.
1.1.10-J – Report categories of cast ballots
All voting systems must report the number of ballots both in total and broken down by ballot style and by selected units of political geography including county, city, town or township, ward, precinct, and precinct split, for the following categories of cast ballots:

1. All read ballots and all counted ballots
2. For multi-page ballots, the number of different pages read, and number counted
3. Recountable read ballots and counted ballots
4. UOCAVA read ballots and counted ballots
5. Absentee read and counted ballots
6. Blank ballots (ballots containing no votes)

Discussion
There is no sub-requirement for separate reporting of provisional cast ballots because the system is unlikely to know whether a ballot is provisional until it is successfully read. Some jurisdictions find the number of blank ballots to be useful. Blank ballots sometimes represent a protest vote.

1.1.10-K – Report read ballots by party
Systems must report separate totals for each party in primary elections when reporting categories of read and counted cast ballots.

1.1.10-L – Report counted ballots by contest
All systems must report the number of counted ballots for each relevant N-of-M or cumulative voting contest.

Discussion
The count by contest could be inferred from the other counts that are broken down by ballot configuration, but providing this figure explicitly will make it easier to account for every vote. N-of-M in this requirement includes the most common type of contest, 1-of-M.

1.1.10-M – Report votes for each contest option
All systems must report the vote totals for each contest option in each relevant N-of-M or cumulative voting contest.

Discussion
N-of-M in this requirement includes the most common type of contest, 1-of-M.
1.1.10-N – Report overvotes for each contest
Systems must report the number of overvotes for each relevant N-of-M or cumulative voting contest.

Discussion
This count refers to votes lost to overvoting, not of ballots containing overvotes. This means that a ballot that overvotes an N-of-M contest would contribute N to the count of overvotes for that contest.

1.1.10-O – Reporting overvotes, ad hoc queries
All systems must be capable of producing a consolidated report of the combination of overvotes for any contest that is selected by an authorized official (for example, the number of overvotes in a given contest combining candidate A and candidate B, or combining candidate A and candidate C).

1.1.10-P – Report undervotes for each contest
All systems must report the number of undervotes for each relevant N-of-M or cumulative voting contest.

Discussion
Counting ballots containing undervotes instead of votes lost to undervoting is insufficient.

1.1.10-Q – Ranked choice voting, report results
Systems implementing ranked choice voting must report the contest option vote totals for each ranked choice contest for each round of tabulation.

Discussion
This requirement is minimal. Since ranked choice voting is not currently in wide use, it is not clear what needs to be reported, how bogus orderings are reported, or how it would be done in multiple reporting contexts.

1.1.10-R – Include all categories of votes
Systems must report all following categories of votes in the consolidated reports:

1. In-person voting
2. Absentee voting
3. Write-ins
4. Accepted recallable ballots
5. Accepted reviewed ballots

1.1.10-S – Post-election reports in common data format
The voting system must include support for the NIST 1500-100 CDF specification for post-election reports.

   External reference: NIST 1500-100 CDF

1.1.10-T – CVR export and import in common data format
The voting system must include support for the NIST 1500-102 CDF specification for cast vote records for exporting a collection of CVRs from the device that created the CVRs and for importing a collection of CVRs into devices that process CVRs.

Discussion
This requirement concerns export of CVRs from devices such as scanners or code and bar-code reading devices and import of the CVRs into adjudication devices, tabulators, and audit devices.

   External reference: NIST 1500-102 CDF

1.1.10-U – Reports are time stamped
All reports must include the date and time of the report’s generation, including hours, minutes, and seconds. Timestamps in reports need to comply with ISO 8601, provide all four digits of the year, and include the time zone.

   External reference: ISO 8601
1.2 – The voting system is designed to function correctly under real-world operating conditions.

1.2-A – Assessment of accuracy
The voting system’s accuracy must be assessed by using a combination of evidence items gathered during the entire course of testing, including:

1. A measurement of how accurately voter marks are recognized as valid or not valid according to manufacturer specifications.

2. A measurement of how accurately voter marks are tabulated and reported as results.

3. An assessment of whether the remaining VVSG requirements are satisfied.

Discussion
A voting system cannot be determined as accurate without some uncertainty; thus, a judgement must be made based on evidence. In this case, a volume test is used under real-world conditions, and evidence collected throughout the test campaign as to whether the voting system satisfies all other relevant VVSG requirements.

Prior VVSG source: New requirement

1.2-A.1 – Minimum ballot positions
A minimum of 10,000,000 ballot positions must be read by the voting system and tabulated accurately.

Discussion
The value of 10,000,000 ballot positions is taken from VVSG 1.0, however it is used here as the minimum number of ballot positions to test without error. If a larger number of ballot positions is used, there still can be no error.

Prior VVSG source: VVSG-1.0 - 4.1.1

1.2-A.2 – Ballot position distribution
The ballot positions must be spread across devices according to a typical volume per device in a typical election.

Discussion
The test lab determines the typical volume per device and then spreads the number of ballot positions to be tested accordingly across the devices, for example, 10% to the electronic ballot marker (EBM), 40% to the voter facing scanner, etc.
1.2-A.3 – Mark quality
For devices that read and interpret human-made marks on ballots, the mark quality of the marks must be spread across the manufacturer’s published specifications for valid marks and invalid marks according to expected distributions in typical elections.

**Discussion**
The goal of this requirement is to model real-world conditions. The test lab would prepare, using the manufacturer’s specifications for valid marks, a set of test ballots in which mark quality will vary as it would in typical elections. In the case of marks that are borderline valid or invalid, a scanner may flag the marks as requiring adjudication.

1.2-B – Assessment of reliability
The voting system’s reliability must be assessed using a combination of evidence items gathered during the entire course of testing, including:

1. Continuous operation of the voting system under typical environmental conditions.
2. Continuous operation of the voting system under varied environmental conditions across defined ranges.
3. An assessment of the manufacturer’s statement of the reliability of the voting system by applying best practices for reliability engineering practices and standard reliability analysis methods (e.g., failure modes and effects analysis (FMEA)).

**Discussion**
As with accuracy, reliability cannot be positively ascertained; a judgment of reliability has to be determined from evidence. In this case, a volume test is used to determine the reliability of the voting system operations, as well as data from the test campaign regarding relevant VVSG requirements. In bullet 3, a manufacturer needs to show that reliability has been built into the voting system using a reliability analysis such as in FMEA. Consequently, the test lab has to assess the manufacturer’s statement of reliability and weigh the performance of the voting system against that assessment.
1.2-B.1 – Continuous operation – typical environmental conditions

The voting system must operate for a continuous period of at least 163 hours during which ballots are cast and ballot positions are read and tabulated without error. Table 1 shows the volume of ballots that must be cast during this period for vote-capture devices. The duration of the testing is as follows:

1. When testing a single device, e.g., a single BMD, the period of testing must be no less than 163 hours.
2. When testing two or more of the same device, e.g., two identical BMDs, the period of testing must be no less than 81 hours.

Discussion

This requirement is, in essence, a volume test in which the voting system is expected to operate continuously for 7 days without error. A form of this requirement is in VVSG 1.0; VVSG 1.1 omitted it entirely. The continuous operation may occur under typical expected temperatures and humidity such as may be found in a standard test lab environment. For hybrid devices such as a BMD combined with a tabulator, two devices should be tested for the 163-hour duration, e.g., one tested as a tabulator, one tested as a BMD. For mixed mode devices such as an accessible BMD used for all voters, the modes should be alternated during the testing.

Prior VVSG source: VVSG-1.0 - 4.1.2-A.2

<table>
<thead>
<tr>
<th>DEVICE</th>
<th>VOLUME/HOUR</th>
</tr>
</thead>
<tbody>
<tr>
<td>CENTRAL SCANNER</td>
<td>Manufacturer’s stated maximum volume/4</td>
</tr>
<tr>
<td>VOTER FACING SCANNER</td>
<td>100</td>
</tr>
<tr>
<td>BMD INCLUDING ACCESSIBLE VERSION</td>
<td>Ballots cast for at least 15 minutes per hour</td>
</tr>
</tbody>
</table>

Table 1 – Volume per hour for vote-capture devices
1.2-B.2 – Continuous operation – varied environmental conditions
The voting system must operate for a continuous period of at least 24 hours during which ballots are cast and ballot positions are read and tabulated without error and in which temperature and humidity are varied.

1. The temperature must range from 41 °F to 104 °F (5 °C to 40 °C).
2. The relative humidity must range from 5 % to 85 %, noncondensing.

Discussion
In VVSG 1.0, the tests for humidity and temperature are included as requirements. For the VVSG 2.0, the same material will be specified as part of an EAC-governed test assertion and not included here.

Prior VVSG source: VVSG-1.0 - 4.1.2

1.2-B.3 – Failure Modes and Effect Analysis (FEMA)
The manufacturer must ensure the reliability of the voting system by applying best practices for reliability engineering practices and standard reliability analysis methods, for example, failure modes and effects analysis (FMEA).

Discussion
Manufacturers are now required to apply best practices to assure reliability in addition to the volume test-related requirements. If using FMEA for the manufacturer’s reliability analysis, each specific, individual, identified failure mode would be assigned a probability, and the system probability of failure would then be derived mathematically. Since the underlying probabilities are likely to depend on the volume that a device is expected to handle in the course of the election, minimum values for the assumed volume per device per election. Other credible forms of reliability analysis could be used, provided they are widely used and accepted in the reliability measurement field.

Prior VVSG source: VVSG-1.1-Vol2 – 5.6.6.2

1.2-C – No single point of failure
All systems must protect against a single point of failure that would prevent further voting at the polling place.

Prior VVSG source: VVSG-2007 - 6.3.1-B

1.2-D – Protect against failure of input and storage devices
All systems must withstand, without loss of data, the failure of any data input or storage device.

Prior VVSG source: VVSG-2007 - 6.3.1-C
1.2-E – Reliably detectable marks
For an optical scanner, the system must detect marks for detectable and marginal marks consistent with system mark specifications.

Discussion
The specification may have parameters for different configuration values. It should also state the degree of uncertainty.

Prior VVSG source: VVSG-2007 - 4.1.2-A.2
Related requirements Marginal marks Ref]

1.2-F – Misfeed rate benchmark
The misfeed rate must not exceed 0.002 (1 / 500).

Discussion
Multiple feeds, misfeeds (jams), and rejections of ballots that meet all manufacturer specifications are all treated collectively as "misfeeds" for benchmarking purposes; that is, only a single count is maintained.

Prior VVSG source: VVSG-2007 – 6.33
Related requirements Marginal marks Ref]

1.2-G – Respond gracefully to stress of system limits
The system must be able to respond gracefully to attempts to process more than the expected number of ballots per precinct, more than the expected number of precincts, higher than expected volume or ballot tabulation rate, or any similar conditions that tend to overload the system's capacity to process, store, and report data.

Discussion
In particular, this requirement should be verified through operational testing if the limit is practically testable.

Prior VVSG source: VVSG-2007 - 5.2.3-C

1.2-H – Handle realistic volume
The system must be able to handle a realistic volume of activities in conditions approximating normal use in an entire election process, from election definition through reporting and auditing final results.

Discussion
Data collected during this test contribute substantially to the evaluations of reliability, accuracy, and misfeed rate.

Prior VVSG source: VVSG-2007 - 5.2.3-D
1.3 – Voting system design supports evaluation methods enabling testers to clearly distinguish systems that correctly implement specified properties from those that do not.

1.3-A – Identifiability of basic and compound system components
The provided documentation and equipment must ensure that a tester is able to clearly and unambiguously identify the full set of the basic (not made of any components) and compound (made up of other components) elements of the system.

Discussion
This is a basic condition necessary for a tester to be able to properly distinguish whether or not a system has correctly implemented specified properties or not.

It may be fulfilled through satisfying guidelines 1.1, 1.2, all the guidelines of principle 2, and by providing information in the Technical Data Package (TDP) that will support this kind of understanding.

Prior VVSG source: New Requirement

1.3-B – Comprehensible processes that form system configurations
The provided documentation and equipment must ensure that a tester is able to clearly understand how particular configurations of process and technology are formed by combining their basic (and component) elements to produce the whole, final working system (whether in software, hardware, telecom, process, data, or other implemented aspect).

Discussion
This is a basic condition necessary for a tester to be able to properly distinguish whether or not a system has correctly implemented specified properties or not.

It may be fulfilled through satisfying guidelines 1.1, 1.2, all the guidelines of principle 2, and by providing information in the Technical Data Package (TDP) that will support this kind of understanding.

Prior VVSG source: New Requirement

1.3-C – Observable configurations via plausible observation methods
The provided documentation and equipment must ensure that a tester is able to identify and select plausible observational tools, techniques, or strategies that can be used to observe signs of the system configurations.
Discussion

This is a basic condition necessary for a tester to be able to properly distinguish whether or not a system has correctly implemented specified properties or not.

It may be fulfilled through satisfying guidelines 1.1, 1.2, all the guidelines of principle 2, and by providing information in the Technical Data Package (TDP) that will support this kind of understanding.

Prior VVSG source: New Requirement

1.3-D – Identifiable resolution limits for observation methods

From the provided documentation and equipment, for the observational tools, techniques, or strategies, a tester must be able to determine how well they can actually detect and distinguish each type of element and interconnection of elements in a system configuration.

Discussion

Every observational or measurement method has a limit to their resolution. Resolution is the threshold beyond which one cannot determine any more differences between two different things. This concept is sometimes known as the just noticeable difference of an observational method. This is like moving two things so close together that a given observer, eventually, cannot see powerfully enough to distinguish distances (differences) too small to detect with that technique. By identifying these limits, each evaluation method explicitly defines its power to distinguish certain observable configurations and characteristics from others.

This is a basic condition necessary for a tester to properly distinguish whether or not a system has correctly implemented specified properties or not.

It may be fulfilled through satisfying guidelines 1.1, 1.2, all the guidelines of principle 2, and by providing information in the TDP that will support this kind of understanding.

Prior VVSG source: New Requirement

1.3-E – Description of observational noise and consequences for observational methods

From the provided documentation and equipment, for the observational tools, techniques, or strategies, a tester must be able to:

- determine what sources of noise will likely arise from observing a given system configuration completely by some observational method;
- map observable signs of system configurations (through that noise) to actual attributes of system configurations.
Discussion

It is often the case, when observing a system during testing, that one cannot always *directly* see what they are attempting to observe. Instead, one often sees *indirectly* observable signs of facts that would most likely be true if one could observe the system or component directly. Thus, much of the task of testing is to be sure that one can strongly relate the secondary facts of directly observable signs to those aspects of a system that may not be directly observable at all. In this way, a tester always acknowledges the degree to which they can directly access signs of what they are actually evaluating.

In addition, very often the methods used for observing those signs may introduce some noise or error into the process for observing configurations. As a result, if not accounted for, such factors can significantly affect the degree to which one can understand and rely upon the relationship of the observed results to the configuration they strive to observe.

This is a basic condition necessary for a tester to properly distinguish whether or not a system has correctly implemented specified properties or not.

It may be fulfilled through satisfying guidelines 1.1, 1.2, all the guidelines of principle 2, and by providing information in the TDP that will support this kind of understanding.

Prior VVSG source: New Requirement

1.3-F – Explicitly-stated performance criteria

The provided documentation and equipment must ensure that a tester is able to state or use criteria that enable them to unambiguously decide whether or not an observed configuration exhibits intended properties.

Discussion

Before one can begin to evaluate the performance of a given system task (that is, a given system-implemented election function or process), one must be able to formulate some statements of facts that must be true of the original system configuration when there are observable signs of system configurations and their behaviors.

This is a basic condition necessary for a tester to properly distinguish whether or not a system has correctly implemented specified properties or not.

It may be fulfilled through satisfying guidelines 1.1, 1.2, all the guidelines of principle 2, and by providing information in the TDP that will support this kind of understanding.

Prior VVSG source: New Requirement
1.3-G – Creation and execution of evaluation methods

The provided documentation and equipment must ensure that a tester is able to derive, construct, and execute plausible evaluation methods (test methods, etc.) that can demonstrate an ability to:

1. observe valid and invalid system configurations through plausible use of observational tools or techniques;
2. decide whether or not a given system configuration has satisfied the stated performance criteria;
3. report the findings resulting from their ability to distinguish correct from incorrect configurations of the system.

Discussion

This is a basic condition that is both necessary and sufficient for a tester to properly distinguish whether or not a system has correctly implemented specified properties or not. It includes and relies upon the satisfaction of the other testability requirements (1.3-A – 1.3-F).

It may be fulfilled through satisfying guidelines 1.1, 1.2, all the guidelines of principle 2, and by providing information in the TDP that will support this kind of understanding.

Prior VVSG source: New Requirement
Principle 2
High Quality Implementation

The voting system is implemented using high quality best practices.

2.1 - The voting system software is implemented using trustworthy materials and best practices in software development.

2.2 - The voting system is implemented using best practice user-centered design methods that consider a wide range of representative voters, including those with and without disabilities, and election workers.

2.3 - Voting system logic is clear, meaningful, and well-structured.

2.4 - Voting system structure is modular, scalable, and robust.

2.5 – The voting system supports system processes and data with integrity.

2.6 - The voting system handles errors robustly and gracefully recovers from failure.

2.7 - The voting system performs reliably in anticipated physical environments.
Principle 2
High Quality Implementation

This principle covers core processes and functions that contribute to a voting system that has been implemented for quality. The requirements in this principle are basic best practices -- not a complete set of all quality practices. The Guidelines under Principle 2 are:

1. **Software quality**, including acceptable programming languages and coding styles, as well as coding constructs that should or should not be used to improve software integrity and security. Additional requirements deal with handling errors or device failures, and others cover electrical components.

2. **Design and implementation process** so that the voting system can be used effectively by voters and election staff.

3. **Voting system logic** or the overall structuring of voting system software. The goal is that the software structure be easily understood and clear to audiences such as test labs and maintained without causing major changes in the software structure.

4. **Modularity** and complexity of the system software structure.

5. **System processes and data** using basic best practices for software integrity and secure coding constructs. The Election Assistance Commission (EAC), working with voting system test labs, may augment or change these requirements based on the discovery of new vulnerabilities or emerging new threats.

5 and 6. **Graceful recovery** the capability of the voting system to handle and recover from errors, including failures of devices and components.

7. **Physical environments** includes the ability of a voting device to withstand influences from its physical environment whether due to humidity, temperature, shock, vibration, electrical, or related influences.

The requirements on electrical disturbances are primarily covered by conformance to the Federal Communications Commission’s regulation, Part 15, Class B [FCC19a]. The requirements here address items not covered by Class B, including the behavior of specific voting devices in the presence of electrical disturbances and cases where voting devices might interact with other devices or people.
2.1 - The voting system software is implemented using trustworthy materials and best practices in software development.

2.1-A – Acceptable programming languages
Application logic must be produced in a high-level programming language that has all of the following control constructs:

1. Sequence
2. Loop with exit condition (for example, for, while, or do-loops)
3. If/Then/Else conditional
4. Case conditional
5. Block-structured exception handling (for example, try/throw/catch).

This requirement can be satisfied by using COTS extension packages to add missing control constructs to languages that could not otherwise conform.

Discussion
A list of acceptable programming languages may be specified by the EAC in conjunction with voting system test labs.

By excluding border logic, this requirement allows the use of assembly language for hardware-related segments, such as device controllers and handler programs. It also allows the use of an externally-imposed language for interacting with an Application Program Interface (API) or database query engine. However, the special code should be insulated from the bulk of the code, for example, by wrapping it in callable units expressed in the prevailing language to minimize the number of places that special code appears.

The use of non-COTS extension packages or manufacturer-specific code for this purpose is not acceptable, as it would place an unreasonable burden on the test lab to verify the soundness of an unproven extension (effectively a new programming language). The package needs to have a proven track record of performance supporting the assertion that it would be stable and suitable for use in voting systems, just as the compiler or interpreter for the base programming language does.

Prior VVSG source: 2007 6.4.1.2-A
2007 6.4.1.5-A.1

2.1-B – COTS language extensions are acceptable
Requirement 2.1-A may be satisfied by using COTS extension packages to add missing control constructs to languages that could not otherwise conform.
Discussion

The use of non-COTS extension packages or manufacturer-specific code for this purpose is not acceptable, as it would place an unreasonable burden on the test lab to verify the soundness of an unproven extension (effectively a new programming language). The package must have a proven track record of performance supporting the assertion that it would be stable and suitable for use in voting systems, just as the compiler or interpreter for the base programming language must.

Prior VVSG source: VVSG-2007 - 6.4.2-A.1

2.1-C – Acceptable coding conventions

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

Discussion

Coding conventions may be specified by the EAC in conjunction with voting system test labs.

Prior VVSG source: 2007 6.4.1.3-A

2.1-D – Records last at least 22 months

All systems must maintain the integrity of election management, voting, and audit data, including cast vote records (CVRs), during an election and for a period of at least 22 months afterward, in temperatures ranging from 5 C to 40 C (41 F to 104 F) and relative humidity from 5% to 85%, non-condensing.

Prior VVSG source: VVSG-2007 - 6.5.1-A

2.1.1 – Workmanship

2.1.1-A – General build quality

All manufacturers of voting systems must practice proper workmanship.

Prior VVSG source: VVSG-2007 - 6.4.3-A

2.1.1-B – High quality products

All manufacturers must adopt and adhere to practices and procedures that ensure their products are free from damage or defect that could make them unsatisfactory for their intended purpose.
2.1.1-C – High quality parts
All manufacturers must ensure that components provided by external suppliers are free from damage or defect that could make them unsatisfactory or hazardous when used for their intended purpose.

2.1.1-D – Suitability of COTS components
Manufacturers must ensure that all COTS components included in their voting systems are designed to be suitable for their intended use under the requirements specified by the VVSG 2.0.

Discussion
For example, if the operating or storage environmental conditions specified by the manufacturer of a printer do not meet or exceed these requirements, a system that includes that printer cannot be found conforming.

2.1.1-E – Durability
Voting systems must be designed to withstand normal use without deterioration for a period of ten years.

2.1.1-F – Durability of paper
Paper specified for use with the voting system must conform to the applicable specifications contained within the Government Paper Specification Standards, February 1999 No. 11, or the government standards that have superseded them.

Discussion
This is to ensure that paper records will be of adequate quality to survive the handling necessary for recounts, audits, etc. without problematic degradation. The Government Paper Specification Standards include different specifications for different kinds of paper. As of 2007-04-05, the Government Paper Specification Standards, February 1999 No. 11, are available at http://www.gpo.gov/acquisition/paperspecs.htm [GPO19].
2.1.2 – Maintainability

2.1.2-A – Electronic device maintainability
Electronic devices must exhibit the following physical attributes:

1. labels and the identification of test points,
2. built-in test and diagnostic circuitry or physical indicators of condition,
3. labels and alarms related to failures, and
4. features that allow non-technicians to perform routine maintenance tasks.

Prior VVSG source: VVSG-2007 - 6.4.5-A

2.1.2-B – System maintainability
Voting systems must allow for:

1. a non-technician to easily detect that the equipment has failed;
2. a trained technician to easily diagnose problems;
3. easy access to components for replacement;
4. easy adjustment, alignment, and tuning of components; and
5. low false alarm rates (that is, indications of problems that do not exist).

Prior VVSG source: VVSG-2007 - 6.4.5-B

2.1.2-C – Nameplate and labels
All voting devices must:

1. Display a permanently affixed nameplate or label containing the name of the manufacturer or manufacturer, the name of the device, its part or model number, its revision identifier, its serial number, and if applicable, its power requirements.
2. Display a separate data plate containing a schedule for and list of operations required to service or to perform preventive maintenance, or a reference to where this can be found in the Voting Equipment User Documentation.
3. Display advisory caution and warning instructions to ensure safe operation of the equipment and to avoid exposure to hazardous electrical voltages and moving parts at all locations where operation or exposure may occur.

Prior VVSG source: VVSG-2007 - 6.4.5-C
2.2 – The voting system is implemented using best practice user-centered design methods that consider a wide range of representative voters, including those with and without disabilities, and election workers.

2.2-A – User-centered design process

The manufacturer must submit a report providing documentation that the system was developed following best practices for a user-centered design process.

The report must include, at a minimum:

- A listing of user-centered design methods used
- The types of voters and election workers included in those methods
- How those methods were integrated into the overall implementation process
- How the results of those methods contributed to developing the final features and design of the voting system

Discussion

The goal of this requirement is to allow the manufacturer to demonstrate, through the report, the way their implementation process included user-centered design methods.

“ISO-9241-210:2010 Ergonomics of human-system interaction—Part 210: Human-centered design for interactive systems provides requirements and recommendations for human-centered principles and activities throughout the life-cycle of computer-based interactive systems.” It includes the idea of iterative cycles of user research to understand the context of use and user needs, creating prototypes or versions, and testing to confirm that the product meets the identified requirements.

This requirement does not specify the exact user-centered design methods to be used, or their number or timing.

The ISO group of requirements, Software engineering -- Software product Quality Requirements and Evaluation (SQuaRE) -- Common Industry Format (CIF) includes several standards that are a useful framework for reporting on user-centered design activities and usability reports.

- ISO/IEC TR 25060:2010: General framework for usability-related information
- ISO/IEC 25062:2006: Usability test reports
- ISO/IEC 25064:2013: User needs report
The final research report from the Los Angeles Voting Systems for All People project is an example of a summary report of a user-centered design process to design a voting system.


Related requirements 8.3-A-Usability testing with voters
8.4-A-Usability testing with election workers
2.3 - Voting system logic is clear, meaningful, and well-structured.

2.3-A – Block-structured exception handling
Application logic must handle exceptions using block-structured exception handling constructs.

Prior VVSG source: VVSG-2007 - 6.4.1.5-A

2.3-B – Legacy library units
If application logic makes use of any COTS or third-party logic callable units that do not throw exceptions when exceptional conditions occur, those callable units must be wrapped in callable units that check for the relevant error conditions and translate them into exceptions, and the remainder of application logic must use only the wrapped version.

Prior VVSG source: VVSG-2007 - 6.4.1.5-A.1

2.3-C – Separation of code and data
Application logic must not compile or interpret configuration data or other input data as a programming language.

Discussion
The applicable requirement in VVSG2005 reads "Operator intervention or logic that evaluates received or stored data must not re-direct program control within a program routine." That attempt to define what it means to compile or interpret data as a programming language caused confusion.

Distinguishing what is a programming language from what is not requires some professional judgment. However, in general, sequential execution of imperative instructions is a characteristic of conventional programming languages that should not be exhibited by configuration data. Configuration data must be declarative or informative in nature, not imperative.

For example: Configuration data can contain a template that informs a report generating application about the form and content of a report that it should generate. However, configuration data cannot contain instructions that are executed or interpreted to generate a report, essentially embedding the logic of the report generator inside the configuration data.

The reasons for this requirement are

- mingling code and data is bad design, and
- embedding logic within configuration data evades the conformity assessment process for application logic.
Draft Requirements for VVSG 2.0

2.3-D – Hard-coded passwords and keys
Voting system software must not contain hard-coded

1. passwords, or
2. cryptographic keys

Discussion
Many examples of this vulnerability have previously been identified in voting system software. Additional information about this vulnerability can be found at CWE-259: Use of Hard-coded Password and CWE-321: Use of Hard-coded Cryptographic Key.

External references:
CWE-259: Use of Hard-coded Password
CWE-321: Use of Hard-coded Cryptographic Key

2.3.1 – Software flow

2.3.1-A – Unstructured control flow
Application logic must contain no unstructured control constructs.

Discussion
Although it is typically developed by the voting system manufacturer, border logic is constrained by the requirements of the third-party or COTS interface with which it interacts. It is not always possible for border logic to achieve its function while conforming to standard coding conventions. For this reason, border logic should be minimized relative to application logic and where possible, wrapped in a conforming interface. An example of border logic that could not be so wrapped is a customized boot manager that connects a bootable voting application to a COTS BIOS.

2.3.1-B – Goto
Arbitrary branches (also known as gotos) must not be used.

Prior VVSG source: VVSG-2007 - 6.4.1.5-B.1

2.3.1-C – Intentional exceptions
Exceptions must only be used for abnormal conditions. Exceptions must not be used to redirect the flow of control in normal ("non-exceptional") conditions.

Discussion
"Intentional exceptions" cannot be used as a substitute for arbitrary branch. Normal, expected events, such as reaching the end of a file that is being read from beginning to end or receiving invalid input from a user interface, are not exceptional conditions and should not be implemented using exception handlers.

Prior VVSG source: VVSG-2007 - 6.4.1.5-B.2

2.3.1-D – Unstructured exception handling
Unstructured exception handling (for example, On Error GoTo, setjmp/longjmp, or explicit tests for error conditions after every executable statement) is prohibited.

Discussion
The internal use of such constructs by a COTS extension package that adds block-structured exception handling to a programming language that otherwise would not have it, as described in Requirement 2.3-B, is allowed. Similarly, it is not a problem that source code written in a high-level programming language is compiled into low-level machine code that contains arbitrary branches. It is only the direct use of low-level constructs in application logic that presents a problem.

Prior VVSG source: VVSG-2007 - 6.4.1.5-B.3
2.4 - Voting system structure is modular, scalable, and robust.

2.4-A – Modularity
Application logic must be designed in a modular fashion.

Discussion
The modularity rules described here apply to the component submodules of a library.

Prior VVSG source: 2007 6.4.1.4-A

2.4-B – Module testability
Each module must have a specific function that can be tested and verified independently of the remainder of the code.

Discussion
In practice, some additional modules (such as library modules) can be needed to compile the module being tested, but the modular construction allows the supporting modules to be replaced by special test versions that support test objectives.

Prior VVSG source: 2007 6.4.1.4-A.1

2.4-C – Module size and identification
Modules must be small and easily identifiable.

Prior VVSG source: 2007 6.4.1.4-B

2.4-D – Lookup tables in separate files
Read-only lookup tables longer than 25 lines must be placed in separate files from other source code if the programming language permits it.

Prior VVSG source: 2007 6.4.1.4-B.2
2.5 - The voting system supports system processes and data with integrity.

2.5-A – Self-modifying code
Application logic must not be self-modifying.
Prior VVSG source: 2007 6.4.1.7-A.1

2.5-B – Unsafe concurrency
Application logic must be free of race conditions, deadlocks, livelocks, and resource starvation.
Prior VVSG source: 2007 6.4.1.7-A.2

2.5.1 – Code integrity

2.5.1-A – COTS compilers
If compiled code is used, it must only be compiled using a COTS compiler.

Discussion
This prohibits the use of arbitrary, nonstandard compilers and, consequently, the invention of new programming languages.
Prior VVSG source: 2007 6.4.1.7-A.3

2.5.1-B – Interpreted code, specific COTS interpreter
If interpreted code is used, it must only be run under a specific, identified version of a COTS runtime interpreter.

Discussion
This ensures that:

- no arbitrary, nonstandard interpreted languages are used, and
- the software tested and approved during the conformity assessment process does not change behavior because of a change to the interpreter.
Prior VVSG source: 2007 6.4.1.7-A.4
2.5.1-C – Prevent tampering with code

Programmed devices must prevent replacing or modifying executable or interpreted code (for example, by other programs on the system, by people physically replacing the memory or medium containing the code, or by faulty code) except where this access is necessary to conduct the voting process.

**Discussion**

This requirement can be partially satisfied through a combination of:

- read-only memory (ROM),
- the memory protection implemented by most popular COTS operating systems,
- error checking, and
- access and integrity controls.

Prior VVSG source: 2007 6.4.1.7-B

2.5.1-D – Prevent tampering with data

All voting devices must prevent access to or manipulation of configuration data, vote data, or audit records (for example, by physically tampering with the medium or mechanism containing the data, by other programs on the system, or by faulty code) except where this access is necessary to conduct the voting process.

**Discussion**

This requirement can be partially satisfied through a combination of:

- the memory protection implemented by most popular COTS operating systems,
- error checking, and
- access and integrity controls.

Systems using mechanical counters to store vote data need to protect the counters from tampering. If vote data are stored on paper, the paper needs to be protected from tampering. Modification of audit records after they are created is never necessary.

Prior VVSG source: 2007 6.4.1.7-C
2.5.2 – Input/output errors

2.5.2-A – Monitoring and defending for I/O errors
Programmed devices must provide the capability to monitor the transfer quality of I/O operations, reporting the number and types of errors that occur and how they were corrected.

Prior VVSG source: 2007 6.4.1.7-D

2.5.2-B – Validate and filter input
The voting system must validate all input against expected parameters, such as data presence, length, type, format, uniqueness, or inclusion in a set of whitelisted values.

**Discussion**
Input includes data from any input source: input devices (such as touchscreens, keyboards, keypads, optical/digital scanners, and assistive devices), networking port, data port, or file.

Prior VVSG source: 2007 6.4.1.8-A.1

2.5.2-C – Detect garbage input
Programmed devices must check information inputs for completeness and validity.

**Discussion**
This general requirement applies to all programmed devices, while the specific ones following are only enforceable for application logic.

Prior VVSG source: 2007 6.4.1.8-A

2.5.2-D – Defend against garbage input
Programmed devices must ensure that incomplete or invalid inputs do not lead to irreversible error.

Prior VVSG source: 2007 6.4.1.8-A.1

2.5.3 – Output protection

2.5.3-A – Escaping and encoding output
Software output must be properly encoded, escaped, and sanitized.
Discussion
The output of a software module can be manipulated or abused by attackers in unexpected ways to perform malicious actions. Ensuring that outputted data is of an expected type or format assists in preventing this abuse. Additional information about this software weakness can be viewed in **CWE 116: Improper Encoding or Escaping of Output**.

External sources: **CWE 116: Improper Encoding or Escaping of Output**

### 2.5.3-B – Sanitize output

The voting system must sanitize all output to remove or neutralize the effects of any escape characters, control signals, or scripts contained in the data which could adversely manipulate the output source.

Discussion
Output includes data to any output source: output devices (such as touchscreens, LCD screens, printers, and assistive devices), networking port, data port, or file. This applies to all parts of the voting system including the election management system (EMS).

### 2.5.3-C – Stored injection

The voting system must sanitize all output to files and databases to remove or neutralize the effects of any escape characters, control signals, or scripts contained in the data which could adversely manipulate the voting system if the stored data is read or imported at a later date or by another part of the voting system.

Discussion
A stored injection attack saves malicious data which is harmless when stored, but which is potent when read later in a different context or when converted to a different format. For example, a malicious script might be written to a file and do no harm to the voting machine, but later be evaluated and harmful when the file is transferred and read by the EMS. Input should also be filtered, but sanitizing stored output provides defense in depth.

### 2.5.4 – Error handling

#### 2.5.4-A – Mandatory internal error checking

Application logic that is vulnerable to the following types of errors must check for these errors at run time and respond defensively when they occur:

1. Common memory management errors, such as out-of-bounds accesses of arrays, strings, and buffers used to manage data
2. Uncontrolled format strings
3. CPU-level exceptions such as address and bus errors, dividing by zero, and the like
4. Variables that are not appropriately handled when out of expected boundaries
5. Numeric and integer overflows
6. Validation of array indices
7. Known programming language specific vulnerabilities

**Discussion**

Logic verification will show that some error checks cannot logically be triggered, and some exception handlers cannot logically be invoked. These checks and exception handlers are not redundant – they provide defense-in-depth against faults that escape detection during logic verification.

Prior VVSG source: 2007 6.4.1.8-B

### 2.5.4-B – Array overflows

If the application logic uses arrays, vectors, or any analogous data structures, and the programming language does not provide automatic run-time range checking of the indices, the indices must be ranged-checked on every access.

**Discussion**

Range checking code should not be duplicated before each access. Clean implementation approaches include:

- consistently using dedicated accessors (such as functions, methods, operations, subroutines, and procedures) that range-check the indices;
- defining and consistently using a new data type or class that encapsulates the range-checking logic;
- declaring the array using a template that causes all accessors to be range-checked; or
- declaring the array index to be a data type whose enforced range is matched to the size of the array.

Range-enforced data types or classes can be provided by the programming environment or they can be defined in application logic. If acceptable values of the index do not form a contiguous range, a map structure can be more appropriate than a vector.

Prior VVSG source: 2007 6.4.1.8-B.1

### 2.5.4-C – Buffer overflows

If an overflow does not automatically result in an exception, the application logic must explicitly check for and prevent the overflow.
2.5.4-D – CPU traps
The application logic must implement such handlers as needed to detect and respond to CPU-level exceptions.

Discussion
For example, under Unix, a CPU-level exception would manifest as a signal, so a signal handler is needed. If the platform supports it, it is preferable to translate CPU-level exceptions into software-level exceptions so that all exceptions can be handled in a consistent fashion within the voting application. However, not all platforms support it.

Prior VVSG source: 2007 6.4.1.8-B.3

2.5.4-E – Garbage input parameters
All scalar or enumerated type parameters whose valid ranges as used in a callable unit (such as function, method, operation, subroutine, and procedure) do not cover the entire ranges of their declared data types must be range-checked on entry to the unit.

Discussion
This applies to parameters of numeric types, character types, temporal types, and any other types for which the concept of range is well-defined. In cases where the restricted range is frequently used or associated with a meaningful concept within the scope of the application, the best approach is to define a new class or data type that encapsulates the range restriction, eliminating the need for range checks on each use.

This requirement deals with user input that is expected to contain errors. User input errors are a normal occurrence; the errors discussed here are grounds for throwing exceptions.

Prior VVSG source: 2007 6.4.1.8-B.4

2.5.4-F – Numeric overflows
If the programming language does not provide automatic run-time detection of numeric overflow, all arithmetic operations that could potentially overflow the relevant data type must be checked for overflow.

Discussion
Encapsulate overflow checking as much as possible.

Prior VVSG source: 2007 6.4.1.8-B.5
2.5.4-G – Uncontrolled format strings
Voting system software must not contain uncontrolled format strings.

Discussion
Many examples of this vulnerability have previously been identified in voting system software. Additional information about this vulnerability can be found at CWE 134: Use of Externally-Controlled Format String.

External reference: CWE 134: Use of Externally-Controlled Format String

2.5.4-H – Recommended internal error checking
Application logic that is vulnerable to the following types of errors must check for these errors at run time and respond defensively when they occur:

1. Pointer variable errors
2. Dynamic memory allocation and management errors

Prior VVSG source: 2007 6.4.1.8-C

2.5.4-I – Pointers
If application logic uses pointers or a similar mechanism for specifying absolute memory locations, the application logic must validate these pointers or addresses before they are used.

Discussion
The goal is to prevent improper overwriting, even if read-only memory would prevent the overwrite from succeeding. An attempted overwrite indicates a logic fault that must be corrected.

Pointer use that is fully encapsulated within a standard platform library is treated as COTS software.

Prior VVSG source: 2007 6.4.1.8-C.1

2.5.4-J – Memory mismanagement
If dynamic memory allocation is performed in application logic, the application logic must be able to be instrumented or analyzed with a COTS tool for detecting memory management errors.

Discussion
Dynamic memory allocation that is fully encapsulated within a standard platform library is treated as COTS software.

Prior VVSG source: 2007 6.4.1.8-D
2.5.4-K – Nullify freed pointers
If pointers are used, any pointer variables that remain within scope after the memory they point to is deallocated must be set to null or marked as invalid (pursuant to the idiom of the programming language used).

**Discussion**
If this is not done automatically by the programming environment, a callable unit should be dedicated to the task of deallocating memory and nullifying pointers. Equivalently, "smart pointers" like the C++ std::auto_ptr can be used to avoid the problem. One should not add assignments after every deallocation in the source code.

In languages using garbage collection, memory is not deallocated until all pointers to it have gone out of scope, so this requirement is moot.

Prior VVSG source: 2007 6.4.1.8-E

2.5.4-L – React to errors detected
Detecting any of the errors enumerated in these requirements must be treated as a complete failure of the callable unit in which the error was detected.

1. An appropriate exception must be thrown, and
2. Control must pass out of the unit immediately.

Prior VVSG source: 2007 6.4.1.8-F

2.5.3-M – Election integrity monitoring
To the extent possible, electronic devices must proactively detect or prevent basic violations of election integrity (for example, stuffing the ballot box or accumulating negative votes) and alert an election official or administrator if they occur.

**Discussion**
Equipment can only verify those conditions that are within the scope of what the equipment does. However, if the equipment can detect something that is blatantly wrong, it should do so and raise the alarm. This provides defense-in-depth to supplement procedural controls and auditing practices.

Prior VVSG source: 2007 6.4.1.8-K

2.5.3-N – SQL injection
The voting system application must defend against SQL injection.

**Discussion**
SQL injection is a classic type of software weakness still prevalent today. SQL injection is not just a web-based issue, as any application accepting untrusted user input and passing it to a database can be vulnerable. Additional information about this software weakness can be viewed in within **CWE 89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').**

**External source:** CWR 89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

**2.5.3-O – Parameterized queries**

Any structured statement or command being prepared using dynamic data (including user input) to be sent to a database or other process must parameterize the data inputs and apply strict type casting and content filters on the data (such as prepared statements).

**Discussion**

Parametrized queries are a common defense against this class of software weakness.
2.6 - The voting system handles errors robustly and gracefully recovers from failure.

2.6-A – Surviving device failure
All systems must be capable of resuming normal operation following the correction of a failure in any device.

Prior VVSG source: 2007 6.4.1.9-A

2.6-B – No compromising voting or audit data
Exceptions and system recovery must be handled in a manner that protects the integrity of all recorded votes and audit log information.

Prior VVSG source: 2007 6.4.1.9-A

2.6-C – Surviving component failure
All voting devices must be capable of resuming normal operation following the correction of a failure in any component (for example, memory, CPU, ballot reader, or printer) provided that catastrophic electrical or mechanical damage has not occurred.

Prior VVSG source: 2007 6.4.1.9-C

2.6-D – Controlled recovery
Error conditions must be corrected in a controlled fashion so that system status can be restored to the initial state existing before the error occurred.

Discussion
"Initial state" refers to the state existing at the start of a logical transaction or operation. Transaction boundaries must be defined in a conscientious fashion to minimize the damage. The final state is optional because election officials responding to the error condition might want the opportunity to select a different state, such as a controlled shutdown with memory dump for later analysis.

Prior VVSG source: 2007 6.4.1.9-D

2.6-E – Nested error conditions
Nested error conditions that are corrected without reset, restart, reboot, or shutdown of the voting device must be corrected in a controlled sequence so that system status can be restored to the initial state existing before the first error occurred.
2.6-F – Reset CPU error states

CPU-level exceptions that are corrected without reset, restart, reboot, or shutdown of the voting device must be handled in a manner that restores the CPU to a normal state and allows the system to log the event and recover as with a software-level exception.

Discussion

System developers should test to see how CPU-level exceptions are handled and make any changes necessary to ensure robust recovery. Invocation of any other error routine while the CPU is in an exception handling state is to be avoided – software error handlers often do not operate as intended when the CPU is in an exception handling state.

If the platform supports it, it is preferable to translate CPU-level exceptions into software-level exceptions so that all exceptions can be handled in a consistent fashion within the voting application. However, not all platforms support it.

2.6-G – Coherent checkpoints

When recovering from non-catastrophic failure of a device or from any error or malfunction that is within the operator’s ability to correct, the system must restore the device to the operating condition existing immediately before the error or failure, without loss or corruption of voting data previously stored in the device.

Discussion

If the system is left in something other than the last known good state for diagnostic reasons, this requirement clarifies that it must revert to the last known good state before being placed back into service.
2.7 - The voting system performs reliably in anticipated physical environments.

2.7-A – Ability to function in physical environment (non-operating)
All voting systems must be able to withstand non-operating physical environment conditions exercised in accordance with the appropriate procedures of MIL-STD-810D, "Environmental Test Methods and Engineering Guidelines" [MIL83].

<table>
<thead>
<tr>
<th>External reference</th>
<th>MIL-STD-810D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prior VVSG source:</td>
<td>VVSG-2007 - 5.1.4-A</td>
</tr>
</tbody>
</table>

2.7-B – Ability to support maintenance and repair physical environment conditions
All voting systems must be able to withstand physical environmental conditions exercised in accordance with MIL-STD-810D, Method 516.3. Procedure VI.

**Discussion**
This test simulates stresses faced during maintenance and repair.

<table>
<thead>
<tr>
<th>External reference</th>
<th>MIL-STD-810D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prior VVSG source:</td>
<td>VVSG-2007 - 5.1.4-A.1</td>
</tr>
</tbody>
</table>

2.7-C – Ability to support transport and storage physical environment conditions
All voting systems must be able to withstand physical environmental conditions exercised in accordance with MIL-STD-810D, Method 514.3, Category 1 Basic Transportation, Common Carrier.

**Discussion**
This test simulates stresses faced during transport between storage locations and polling places.

<table>
<thead>
<tr>
<th>External reference</th>
<th>MIL-STD-810D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prior VVSG source:</td>
<td>VVSG-2007 - 5.1.4-A.2</td>
</tr>
</tbody>
</table>

2.7-D – Ability to support storage temperatures in physical environment
All voting systems must be able to withstand physical environmental conditions exercised in accordance with MIL-STD-810D: Method 502.2, Procedure I Storage and Method 501.2, Procedure I Storage. The minimum temperature must be -4 degrees F, and the maximum temperature must be 140 degrees F.
Discussion
This test simulates stresses faced during storage.

<table>
<thead>
<tr>
<th>External reference</th>
<th>MIL-STD-810D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prior VVSG source:</td>
<td>VVSG-2007 - 5.1.4-A.3</td>
</tr>
</tbody>
</table>

2.7-E – Ability to support storage humidity levels in physical environment

All voting systems must be able to withstand physical environmental conditions exercised in accordance with humidity testing specified by MIL-STD-810D: Method 507.2, Procedure II Natural (Hot- Humid), with test conditions that simulate a storage environment.

Discussion
This test is intended to evaluate the ability of voting equipment to survive exposure to an uncontrolled temperature and humidity environment during storage.

<table>
<thead>
<tr>
<th>External reference</th>
<th>MIL-STD-810D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prior VVSG source:</td>
<td>VVSG-2007 - 5.1.4-A.4</td>
</tr>
</tbody>
</table>

2.7-F – Ability to operate as intended in physical environment

All voting systems must be able to withstand physical environmental conditions exercised in accordance with the appropriate procedures of MIL-STD-810D, "Environmental Engineering Considerations and Laboratory Tests" [MIL83].

<table>
<thead>
<tr>
<th>External reference</th>
<th>MIL-STD-810D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prior VVSG source:</td>
<td>VVSG-2007 - 5.1.5-A</td>
</tr>
</tbody>
</table>

2.7-G – Ability to operate as intended at low and high temperatures

All voting systems must be able to withstand physical environmental conditions exercised in the low temperature and high temperature testing specified by MIL-STD-810-D [MIL83]: Method 502.2, Procedure II -- Operation and Method 501.2, Procedure II -- Operation, with test conditions that simulate system operation.

<table>
<thead>
<tr>
<th>External reference</th>
<th>MIL-STD-810D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prior VVSG source:</td>
<td>VVSG-2007 - 5.1.5-A.1</td>
</tr>
</tbody>
</table>

2.7-H – Ability to operate as intended at specified humidity conditions

All voting systems must be able to withstand physical environmental conditions exercised in the humidity testing specified by MIL-STD-810-D: Method 507.2, Procedure II Natural (Hot Humid), with test conditions that simulate system operation.
2.7.1 – Ability to withstand electrical disturbances

2.7.1-A – Electrical disturbances
All voting devices must continue to operate in the presence of electrical disturbances generated by other devices and people and must not cause electrical disruption to other devices and people.

Discussion
Voting devices located in a polling place or other places need to continue to operate despite disruption from electrical emanations generated by other devices, including static discharges from people. Likewise, voting devices need to operate without causing disruption to other devices and people due to electrical emanations from the devices.

2.7.1-B – FCC Part 15 Class A and B conformance
Voting devices must comply with the requirements of the Federal Communications Commission, Part 15:

1. Voting devices located in polling places must comply with Class B requirements.
2. Voting devices located in non-place setting, such as back offices, must minimally comply with Class A requirements.

2.7.1-C – Power supply from energy service provider
Voting devices located in polling places must be powered by a 120 V, single phase power supply derived from typical energy service providers.

Discussion
It is assumed that the AC power necessary to operate the voting system will be derived from the existing power distribution system of the facility housing the polling place. This single-phase power may be a leg of a 120/240 V single phase system, or a leg of a 120/208 V three-phase system, at a frequency of 60 Hz.

2.7.1-D – Power port connection to the facility power supply
All electronic voting systems installed in a polling place must comply with Class B emission limits affecting the power supply connection to the energy service provider.

Discussion
The normal operation of an electronic system can produce disturbances that will travel upstream and affect the power supply system of the polling place, creating a potential deviation from the expected electromagnetic compatibility of the system. The issue is whether these actual disturbances (after possible mitigation means incorporated in the equipment) reach a significant level to exceed stipulated limits.

2.7.1-E – Leakage from grounding port
All electronic voting systems installed in a polling place must comply with limits of leakage currents effectively established by the trip threshold of all listed Ground Fault Current Interrupters (GFCI), if any, installed in the branch circuit supplying the voting system.

Discussion
Excessive leakage current is objectionable for two reasons:

- For a branch circuit or wall receptacle that could be provided with a GFCI (depending upon the wiring practice applied at the particular polling place), leakage current above the GFCI built-in trip point would cause the GFCI to trip and therefore disable the operation of the system.
- Should the power cord lose the connection to the equipment grounding conductor of the receptacle, a personnel hazard would occur. (Note the prohibition of “cheater” adapters in the discussion of general requirements for the polling place.)

2.7.1-F – Outages, sags, and swells
All electronic voting systems must be able to withstand, without disruption of normal operation or loss of data, a complete loss of power lasting two hours.

Discussion
The Information Technology industry has adopted a recommendation that IT equipment should be capable of operating correctly for swells reaching 120% of the nominal system voltage with duration ranging from 3 ms to 0.5 s and permanent overvoltages up to 110% of nominal system voltage.

2.7.1-G – Withstand conducted electrical disturbances
All electronic voting systems must withstand conducted electrical disturbances that affect the power ports of the system.

2.7.1-H – Emissions from other connected equipment
All elements of an electronic voting system must be able to withstand the conducted emissions generated by other elements of the voting system.
2.7.1-I – Electrostatic discharge immunity
All electronic voting systems must withstand, without disruption of normal operation or loss of data, electrostatic discharges (ESD) associated with human contact and contact with mobile equipment (such as service carts and wheelchairs).

Discussion
ESD events can originate from direct contact between an “intruder” (person or object) charged at a potential different from that of the units of the voting system, or from an approaching person about to touch the equipment – an “air discharge.” The resulting discharge current can induce disturbances in the circuits of the equipment. This requirement is meant to ensure that voting devices are conformant to the typical ESD specifications met by other electronic devices used by the public such as ATMs and vending kiosks.

2.7.1-J – Radiated radio frequency emissions
All electronic voting systems installed in a polling place must comply with emission limits according to the Rules and Regulations of Class B for radiated radio-frequency emissions.

Discussion
Electronic equipment in general and modern high-speed digital electronic circuits in particular have the potential to produce unintentional radiated and conducted radio-frequency emissions over wide frequency ranges. These unintentional signals can interfere with the normal operation of other equipment, especially radio receivers, in close proximity.
Principle 3
Transparent

The voting system and voting processes are designed to provide transparency.

3.1 - The documentation describing the voting system design, operation, accessibility features, security measures, and other aspects of the voting system can be read and understood.

3.2 - The processes and transactions, both physical and digital, associated with the voting system are readily available for inspection.

3.3 - The public can understand and verify the operations of the voting system throughout the entirety of the election.
Principle 3
TRANSPARENT
The voting system and voting processes are designed to provide transparency.

Guideline 3.1 contains requirements for the documentation that manufacturers supply to jurisdictions that use their systems. In this context, "user" refers to election officials, and "system" refers to a voting system or individual voting device. The user documentation is also included in the technical date package (TDP) given to test labs. The sections in 3.1 cover:

1 - **System overview** covers documentation that explains the physical and logical structure of the system, its components, how it is structured, details about the software, and so forth.

2 - **System performance** documentation gives details on how the system performs in normal operation as well as its constraints and limits.

3 - **System security** documentation describes the features of the system that provide or contribute to its security and includes how to operate the system securely. Physical security and audit are included in this documentation.

4 - **Software installation** documentation describes in exact detail what software is installed, how it is installed, and how it is to be maintained.

5 - **System operations** documentation deals with operating and using the equipment to conduct elections, including setup, testing, voting operations, reporting, and so forth.

6 - **System maintenance** documentation deals with proper maintenance of the voting equipment and how to correct various issues or problems.

7 - **Training material** lists what the manufacturer needs to cover about the personnel resources and training required for a jurisdiction to operate and maintain the system.

8 - **Training documentation** lays out various information that would be important when training users on the voting equipment.

It is not the intent of these requirements to prescribe an outline for user documentation. Manufacturers are encouraged to innovate in the quality and clarity of their user documentation.

In 3.2, **Setup inspection documentation** explains how to verify that the system is properly setup and configured, and how to monitor its operations.

In 3.3, **Public documentation** requirements cover details of how a manufacturer codes the election event log, implements a CDF, builds bar codes, and implements audits.
3.1 – The documentation describing the voting system design, operation, accessibility features, security measures, and other aspects of the voting system can be read and understood.

3.1.1 – System overview

3.1.1-A – System overview documentation
In the system overview, the manufacturer must provide information that enables the user to identify the functional and physical components of the system, how the components are structured, and the interfaces between them.

3.1.1-B – System overview, functional diagram
The system overview must include a high-level functional diagram of the voting system that includes all of its components. The diagram must portray how the various components relate and interact.

3.1.1-C – System description
The system description must include written descriptions, drawings, and diagrams that present, as applicable:

1. a description of the functional components (or subsystems) as defined by the manufacturer (for example, environment, election management and control, vote recording, vote conversion, reporting, and their logical relationships)
2. a description of the operational environment of the system that provides an overview of the hardware, firmware, software, and communications structure
3. a concept of operations that explains each system function and how the function is achieved in the design
4. descriptions of the functional and physical interfaces between components
5. identification of all COTS products (both hardware and software) included in the system or used as part of the system's operation, identifying the name, manufacturer, and version used for each such component
6. communications (dial-up, network) software
7. interfaces among internal components and interfaces with external systems
8. for components that interface with other components for which multiple products may be used, file specifications, data objects, or other means used for information exchange including the public standard used for such file specifications, data objects, or other means

9. benchmark directory listings for all software, firmware, and associated documentation included in the manufacturer's release in the order in which each piece of software or firmware would normally be installed upon system setup and installation

3.1.1-D – Identify software and firmware by origin
The system overview must include the identification of all software and firmware items, indicating items that were:

1. written in-house
2. written by a subcontractor
3. procured as COTS
4. procured and modified, including descriptions of the modifications to the software or firmware and to the default configuration options

3.1.1-E – Traceability of procured software
The system description must include a declaration that procured software items were obtained directly from the manufacturer or a licensed dealer or distributor.

Discussion
For most noncommercial software, this would mean a declaration that the software was downloaded from the canonical site or a trustworthy mirror. It is generally accepted practice for the core contributors to major open-source software packages to digitally sign the distributions. Verifying these signatures provides greater assurance that the package has not been modified.
3.1.2 – System performance

3.1.2-A – System performance
The manufacturer must provide system performance information including:

1. device capacities and limits that were stated in the implementation statement
2. if not already covered in the implementation statement, performance characteristics of each operating mode and function in terms of expected and maximum speed, throughput capacity, maximum volume (maximum number of voting positions and maximum number of ballot styles supported), and processing frequency
3. quality attributes such as reliability, maintainability, availability, usability, and portability
4. provisions for safety, security, privacy, and continuity of operation
5. design constraints, applicable standards, and compatibility requirements

3.1.2-B – Maximum tabulation rate
The maximum tabulation rate for a bulk-fed scanner must be documented by the manufacturer. This documentation must include the maximum tabulation rate for individual components that impact the overall maximum tabulation rate.

Discussion
The capacity to convert the marks on individual ballots into signals is uniquely important to central count systems.

3.1.2-C – Reliably detectable marks
For an optical scanner, the manufacturer must document what constitutes a reliably detectable mark versus a marginal mark.

3.1.2-D – Processing capabilities
The manufacturer must provide a listing of the system's functional processing capabilities, encompassing capabilities required by the VVSG, and any additional capabilities provided by the system, with a description of each capability.

1. The manufacturer must explain the capabilities of the system that were declared in the implementation statement.
2. Additional capabilities (extensions) must be clearly indicated.
3. Required capabilities that may be bypassed or deactivated during installation or operation by the user must be clearly indicated.
4. Additional capabilities that function only when activated during installation or operation by the user must be clearly indicated.
5. Additional capabilities that normally are active but may be bypassed or deactivated during installation or operation by the user must be clearly indicated.

3.1.3 – System security documentation

3.1.3-A – System security
The manufacturer must provide information that enables the user to understand the security-related functions of the system and how they are to be used properly.

3.1.3-B – Access control implementation
Manufacturers must provide user documentation containing:

1. guidelines and usage instructions on implementing, configuring, and managing access control capabilities
2. an access control policy template or instructions to facilitate the implementation of the access control policy and associated access controls on the voting system
3. an access control policy under which the voting system was designed to operate and a description of the hazards of deviating from this policy
4. information on all privileged accounts included on the voting system

Discussion
Access control policy requirements include the minimum baseline policy definitions necessary for testing and implementing the voting system. The policies may be defined within the voting system or provided as guidelines in the documentation. The access control policy includes the assumptions that were made when the system was designed, the justification for the policy, and the hazards of deviating from the policy. Information on privileged accounts include the name of the account, purpose, capabilities and permissions, and how to disable the account in the user documentation.

3.1.3-C – Physical security
Manufacturers must provide user documentation explaining how to implement all physical security controls for the voting device, including model procedures necessary for effective use of countermeasures.
3.1.3-D – Audit Procedures
The manufacturer must provide information that enables the user to conduct audit procedures to determine whether tabulation is accurate.

3.1.3-E – Risk Analysis
The manufacturer must provide a report of a risk analysis for the voting system that contains a list of possible threats, risks of threat occurrence, and mitigation strategies employed by the voting system.

3.1.4 – Software Installation

3.1.4-A – Software installation
The manufacturer must provide a list of all software to be installed on the programmed devices of the voting system and the installation software used to install the software in the user documentation.

Discussion
Software to be installed on programmed devices of the voting system includes executable code, configuration files, data files, and election specific software.

3.1.4-B – Software information
The manufacturer must provide at a minimum in the user documentation the following information for each piece of software to be installed or used to install software on programmed devices of the voting system:

1. software product name
2. software version number
3. software manufacturer name
4. software manufacturer contact information
5. type of software (application logic, border logic, third party logic, COTS software, or installation software)
6. list of software documentation
7. component identifiers (such as filenames) of the software, and type of software component (executable code, source code, or data)
3.1.4-C – Software location information
The manufacturer must provide in the user documentation the location (such as full path name or memory address) and storage device (such as type and part number of storage device) where each piece of software is installed on programmed devices of the voting system.

**Discussion**
This requirement applies to software installed on programmed devices of the voting system. The full directory path is the final destination of the software when installed on non-volatile storage with a file system.

3.1.4-D – Election specific software identification
The manufacturer must identify election specific software in the user documentation.

3.1.4-E – Installation software and hardware
The manufacturer must provide a list of software and hardware required to install software on programmed devices of the voting system in the user documentation.

3.1.4-F – Software installation procedure
The manufacturer must document the software installation procedures used to install software on programmed devices of the voting system in user documentation.

3.1.4-G – Compiler installation prohibited
The software installation procedures used to install software on programmed devices of the voting system must result in no compilers being installed on the programmed device.

3.1.4-H – Baseline binary image creation
To replicate programmed device configurations, the software installation procedures must create a baseline binary image of the initial programmed device configuration on an unalterable storage media with a digital signature.

3.1.4-I – Programmed device configuration replication
The software installation procedures must use the baseline binary image of the initial programmed device configuration on an unalterable storage media to replicate the configuration onto other programmed devices.
3.1.4-J – Software installation record creation

The software installation procedures must specify the creation of a software installation record that includes at a minimum:

1. a unique identifier (such as a serial number) for the record
2. a list of unique identifiers of unalterable storage media associated with the record
3. the time, date, and location of the software installation
4. names, affiliations, and signatures of all people present
5. copies of the procedures used to install the software on the programmed devices of the voting system
6. the certification number of the voting system
7. list of the software installed on programmed devices of the voting system
8. a unique identifier (such as a serial number) of the vote-capture device or election management system (EMS) which the software is installed

3.1.4-K – Procurement of voting system software

The software installation procedures must specify that voting system software be obtained from test labs or distribution repositories.

Discussion

Distribution repositories provide software they receive to parties approved by the owner of the software.

3.1.4-L – Open market procurement of COTS software

The software installation procedures must specify that COTS software be obtained from the open market.

3.1.4-M – Erasable storage media preparation

The software installation procedures must specify how previously stored information on erasable storage media is removed before installing software on the media.

Discussion

The purpose of this requirement is to prepare erasable storage media for use by the programmed devices of the voting system. The requirement does not mandate the prevention of previously stored
information leakage or recovery. Simply deleting files from file systems, flashing memory cards, and removing electrical power from volatile memory satisfies this requirement.

3.1.4-N – Unalterable storage media
The software installation procedures must specify that unalterable storage media be used to install software on programmed devices of the voting system.

3.1.5 – System operations

3.1.5-A – Operations manual
The system operations manual must provide all information necessary for system use by all personnel who support pre-election and election preparation, polling place activities, and central counting activities, as applicable, with regard to all system functions and operations.

Discussion
The nature of the instructions for operating personnel will depend upon the overall system design and required skill level of system operations support personnel.

3.1.5-B – Support training
The system operations manual must contain all information that is required for the preparation of detailed system operating procedures and for the training of administrators, central election officials, election judges, and election workers.

3.1.5-C – Functions and modes
The manufacturer must provide a summary of system operating functions and modes to permit understanding of the system’s capabilities and constraints.

3.1.5-D – Roles
The roles of operating personnel must be identified and related to the operating modes of the system.

3.1.5-E – Conditional actions
Decision criteria and conditional operator functions (such as error and failure recovery actions) must be described.
3.1.5-F – References
The manufacturer must also list all reference and supporting documents pertaining to the use of the system during election operations.

3.1.5-G – Operational environment
The manufacturer must identify all facilities, furnishings, fixtures, and utilities that will be required for equipment operations, including a statement of all requirements and restrictions regarding:

1. environmental protection
2. electrical service
3. recommended auxiliary power
4. telecommunications service
5. any other facility or resource required for the proper installation and operation of the system

3.1.5-H – Readiness testing
The manufacturer must provide specifications for testing system installation and readiness.

Discussion
Readiness testing refers to steps that election officials can take after configuring equipment to establish that it was correctly configured. Logic and accuracy testing would be part of this.

3.1.5-I – Features
The manufacturer must provide documentation of system operating features that includes:

1. detailed descriptions of all input, output, control, and display features accessible to the operator or voter
2. examples of simulated interactions to facilitate understanding of the system and its capabilities
3. sample data formats and output reports
4. illustration and description of all status indicators and information messages

3.1.5-J – Operating procedures
The manufacturer must provide documentation of system operating procedures that:
1. provides a detailed description of procedures required to initiate, control, and verify proper system operation

2. provides procedures that clearly enable the operator to assess the correct flow of system functions (as evidenced by system-generated status and information messages)

3. provides procedures that clearly enable the administrator to intervene in system operations to recover from an abnormal system state

4. defines and illustrates the procedures and system prompts for situations where operator intervention is required to load, initialize, and start the system

5. defines and illustrates procedures to enable and control the external interface to the system operating environment if supporting hardware and software are involved. (This information is provided for the interaction of the system with other data processing systems or data interchange protocols.)

6. provides administrative procedures and off-line operator duties (if any) if they relate to the initiation or termination of system operations, to the assessment of system status, or to the development of an audit trail

7. supports successful ballot and program installation and control by central election officials

8. provides a schedule and steps for the software and ballot installation, including a table outlining the key dates, events, and deliverables

9. specifies diagnostic tests that may be employed to identify problems in the system, verify the correction of problems, and isolate and diagnose faults from various system states

3.1.5-K – Support

The manufacturer must provide documentation of system operating procedures that:

1. defines the procedures required to support system acquisition, installation, and readiness testing

2. describes procedures for providing technical support, system maintenance, and correction of defects, and for incorporating hardware upgrades and new software releases
3.1.5-L – Transportation
The manufacturer must include any special instructions for the care and handling of voting devices and any removable media or records for

1. shipment
2. storage
3. archiving information

3.1.6 – System Maintenance

3.1.6-A – System maintenance manual
The system maintenance manual must provide information to support election workers, information systems personnel, or maintenance personnel in adjusting or removing and replacing components or modules in the field.

Discussion
Technical documentation needed solely to support the repair of defective components or modules ordinarily done by the manufacturer or software developer is not required.

3.1.6-B – General contents
The manufacturer must describe service actions recommended to correct malfunctions or problems, personnel and expertise required to repair and maintain the system, and equipment and materials facilities needed for proper maintenance.

3.1.6-C – Maintenance viewpoint
The manufacturer must describe the structure and function of the hardware, firmware, and software for election preparation, programming, vote recording, tabulation, and reporting in sufficient detail to provide an overview of the system for maintaining and identifying faulty hardware or software.

3.1.6-D – Equipment overview details
The description must include a concept of operations that fully describes such items as:

1. electrical and mechanical functions of the equipment
2. for paper-based systems, how ballot handling and reading processes are performed
3. for electronic vote-capture devices, how vote selection and ballot casting are performed
4. how data transmission over a network is performed (if applicable)
5. how data are handled in the processor and memory units
6. how data output is initiated and controlled
7. how power is converted or conditioned
8. how test and diagnostic information is acquired and used

3.1.6-E – Maintenance procedures
The manufacturer must describe preventive and corrective maintenance procedures for hardware, firmware, and software.

3.1.6-F – Preventive maintenance procedures
The manufacturer must identify and describe:

1. all required and recommended preventive maintenance tasks, including software and data backup, database performance analysis, and database tuning
2. the number and skill levels of personnel required for each task
3. the parts, supplies, special maintenance equipment, software tools, or other resources needed for maintenance
4. any maintenance tasks that must be coordinated with the manufacturer or a third party (such as coordination that may be needed for COTS used in the system)

3.1.6-G – Troubleshooting procedures
The manufacturer must provide fault detection, fault isolation, correction procedures, and logic diagrams for all operational abnormalities identified by design analysis and operating experience.

3.1.6-H – Troubleshooting procedure details
The manufacturer must identify specific procedures to be used in diagnosing and correcting problems in the system hardware, firmware, and software. Descriptions must include:

1. steps to replace failed or deficient equipment
2. steps to correct deficiencies or faulty operations in software or firmware
3. modifications that are necessary to coordinate any modified or upgraded software or firmware with other modules

4. number and skill levels of personnel needed to accomplish each procedure

5. special maintenance equipment, parts, supplies, or other resources needed to accomplish each procedure

6. any coordination required with the manufacturer, or other party, for COTS

3.1.6-I – Special equipment
The manufacturer must identify and describe any special purpose test or maintenance equipment recommended for fault isolation and diagnostic purposes.

3.1.6-J – Parts and materials
Manufacturers must provide detailed documentation of parts and materials needed to operate and maintain the system.

3.1.6-K – Approved parts list
The manufacturer must provide a complete list of approved parts and materials needed for maintenance. This list must contain sufficient descriptive information to identify all parts by:

1. type
2. size
3. value or range
4. manufacturer's designation
5. individual quantities needed
6. sources from which they may be obtained

3.1.6-L – Marking devices
The manufacturer must identify specific marking devices that, if used to make the prescribed form of mark, produce readable marked ballots so that the system meets the performance requirements for accuracy.

Discussion
Includes pens or pencils and possibly a compatible electronic ballot marker (EBM).
3.1.6-M – Approved manufacturers
For marking devices manufactured by multiple external sources, the manufacturer must specify a listing of sources and model numbers that satisfy these requirements.

3.1.6-N – Ballot stock specification
The manufacturer must

1. specify the required paper stock, weight, size, shape, opacity, color, watermarks, field layout, orientation, size and style of printing, size and location of vote response fields and
2. identify unique ballot styles, placement of alignment marks, ink for printing, and folding and bleed-through limitations for preparation of ballots that are compatible with the system.

3.1.6-O – Ballot stock specification criteria
User documentation for optical scanners must include specifications for ballot materials to ensure that votes are read from only a single ballot at a time, without bleed-through or transferal of marks from one ballot to another.

3.1.6-P – Printer paper specification
User documentation for voting systems that include printers must include specifications of the paper necessary to ensure correct operation, minimize jamming, and satisfy Requirement 2.1.1-F – Durability of paper and 2.1.1-F – Durability of paper.

Discussion
This requirement covers all printers, either stand-alone or integrated with another device, regardless whether they are used for reporting, for logging, for voter verified paper records (VVPR), etc.

Related requirements: 2.1.1-E – Durability, 2.1.1-F – Durability of paper

3.1.6-Q – System maintenance, maintenance environment
The manufacturer must identify all facilities, furnishings, fixtures, and utilities that will be required for equipment maintenance.
3.1.6-R – System maintenance, maintenance support and spares
Manufacturers must specify:

1. recommended number and locations of spare devices or components to be kept on hand for repair purposes during periods of system operation
2. recommended number and locations of qualified maintenance personnel who need to be available to support repair calls during system operation
3. organizational affiliation (for example, jurisdiction, manufacturer) of qualified maintenance personnel

3.1.7 – Training material

3.1.7-A – Training requirements
The manufacturer must describe the personnel resources and training required for a jurisdiction to operate and maintain the system.

3.1.7-B – Personnel
The manufacturer must specify the number of personnel and skill levels required to perform each of the following functions:

1. pre-election or election preparation functions (such as, entering an election, contest and candidate information, designing a ballot, and generating pre-election reports)
2. system operations for voting system functions performed at the polling place
3. system operations for voting system functions performed at the central count facility
4. preventive maintenance tasks
5. diagnosis of faulty hardware, firmware, or software
6. corrective maintenance tasks
7. testing to verify the correction of problems

3.1.7-B – User functions versus manufacturer functions
The manufacturer must distinguish which functions may be carried out by user personnel and which must be performed by manufacturer personnel.
3.1.7-C – Training requirements

The manufacturer must specify requirements for the orientation and training of administrators, central election officials, election judges, and election workers.

3.2 – The processes and transactions, both physical and digital, associated with the voting system are readily available for inspection.

3.2-A – Setup inspection process

The manufacturer must specify a setup inspection process that the voting device was designed to support and description of the risks of deviating from the process in the user documentation.

**Discussion**

The setup inspection process provides a means to inspect various properties of voting devices as needed during the election process.

3.2-B – Minimum properties included in the setup inspection process

The setup inspection process must at a minimum include

1. inspecting voting system software
2. inspecting storage locations that hold election information that changes during an election
3. inspecting other voting device properties
4. executing logic and accuracy testing related to readiness of use in an election

3.2-C – Setup inspection record generation

The setup inspection process must describe the records that result from performing the setup inspection process.

3.2-D – Installed software identification procedure

The manufacturer must provide the procedures to identify all software installed on programmed devices of the voting system in the user documentation.

**Discussion**
This requirement provides the ability to identify if the proper software is installed and that no other software is present on programmed devices of the voting system. This requirement covers software stored on storage media with or without a file system.

3.2-E – Software integrity verification procedure
The manufacturer must describe the procedures to verify the integrity of software installed on programmed devices of the voting system in the user documentation.

3.2-F – Election information value
The manufacturer must provide the values of voting device storage locations that hold election information that changes during the election, except for the values set to conduct a specific election in the user documentation.

3.2-G – Maximum and minimum values of election information storage locations
The manufacturer must provide the maximum and minimum values that voting device storage locations that hold election information changes during an election can store in the user documentation.

3.2-H – Variable value inspection procedure
The manufacturer must provide the procedures to inspect the values of voting device storage locations that hold election information that changes for an election in the user documentation.

3.2-I – Backup power operational range
The manufacturers must provide the nominal operational range for the backup power sources of the voting device in the user documentation.

3.2-J – Backup power inspection procedure
The manufacturer must provide the procedures to inspect the remaining charge of the backup power sources of the voting device in the user documentation.

3.2-K – Cabling connectivity inspection procedure
The manufacturer must provide the procedures to inspect the connectivity of the cabling attached to the voting device in the user documentation.
3.2-L – Communications operational status inspection procedure
The manufacturer must provide the procedures to inspect the operational status of the communications capabilities of the voting device in the user documentation.

3.2-M – Communications on/off status inspection procedure
The manufacturer must provide the procedures to inspect the on/off status of the communications capabilities of the voting device in the user documentation.

3.2-N – Quantity of voting equipment
The manufacturer must provide a list of consumables associated with the voting device, including estimated number of usages per unit in the user documentation.

3.2-O – Consumable inspection procedure
The manufacturer must provide the procedures to inspect the remaining amount of each of the voting device’s consumables in the user documentation.

3.2-P – Calibration of voting device components
The manufacturer must provide:

1. a list of components associated with the voting device that require calibration
2. the nominal operating ranges for each component in the user documentation
3. the procedures to inspect the calibration of each component in the user documentation
4. the procedures to adjust the calibration of each component in the user documentation

3.2-Q – Checklist of properties to be inspected
The manufacturer must provide a checklist of other properties of the voting device to be inspected, to include:

1. a description of the risks of not performing each documented inspection
2. power sources
3. cabling for communications
4. capabilities
5. consumables
6. calibration of voting device components
7. general physical features of the voting device
8. securing external interfaces of the voting device not being used
3.3 – The public can understand and verify the operations of the voting system throughout the entirety of the election.

3.3-A – System security, system event logging
Manufacturers must provide user documentation that:

1. describes system event logging capabilities and usage
2. publicly available and free of charge, fully documents the log format information

Discussion
The log format and the meaning of all possible types of log entries must be fully documented in sufficient detail to allow independent manufacturers to implement utilities to parse the log file. This documentation must be publicly available, free of charge, and not just in the TDP. The documentation may be housed by the EAC or the test lab.

3.3-B – Specification of common data format usage
Voting device and system manufacturers must include a freely-available specification describing how the manufacturer has implemented a NIST CDF specification for a particular device or function. This includes such items as:

1. descriptions of how elements and attributes are used
2. constraints on data elements
3. extensions as well as any constraints

Discussion
Conformance to a common data format does not guarantee data interoperability. The manufacturer needs to document fully how it has interpreted and implemented a NIST CDF specification for its voting devices and the types of data exchanged or exported.

3.3-C Bar and other codes
The voting system’s user documentation must fully specify the bar code or other encoding standards or algorithms used on ballots or audit material.

Discussion
The voting system documentation needs to include the name and version of the standard used for bar codes or for any other codes that encode information that the public sees on ballots or other material that can be used in audits or verification of the election.
3.3-D Encodings
The voting system’s user documentation must, publicly available and free of charge, fully specify any encodings of data used on ballots, including how data may be compressed prior to encoding.

Discussion
The voting system documentation needs to include the name and version of the standard used for bar codes or for any other codes that encode information that the public sees on ballots or other material that can be used in audits or verification of the election. The documentation also needs to include how the data may be packed or compressed within the encoding.

3.3-E Audit
The voting system’s user documentation must fully specify a secure, transparent, workable, and accurate process for producing all records necessary from the devices and carrying out audits.

Discussion
The voting system documentation needs to provide enough information for election officials to carry out all auditing steps. This includes explaining how to generate all needed reports, how to check the reports against one another for agreement, and how to deal with errors and other unusual problems that come up during the audit steps.
Principle 4
Interoperable

The voting system is designed to support interoperability in its interfaces to external systems, its interfaces to internal components, its data, and its peripherals.

4.1 - Voting system data that is imported, exported, or otherwise reported, is in an interoperable format.

4.2 - Standard, publicly-available formats for other types of data are used, where available.

4.3 - Widely-used hardware interfaces and communications protocols are used.

4.4 - Commercial-off-the-shelf (COTS) devices can be used if they meet applicable VVSG requirements.
Principle 4
INTEROPERABLE

The voting system is designed to support interoperability in its interfaces to external systems, its interfaces to internal components, its data, and its peripherals.

This Principle covers requirements that ensure all system data is in an interoperable format and explains when standard, publicly available formats are used. It also addresses widely used hardware interfaces and when COTS devices are permitted. The Guidelines under Principle 4 are:

1 - **Interoperable format** requirements, which include voting system data that is imported, exported, or otherwise reported.

2 - **Standard formats** covering when publicly available formats for other types of data not addressed by NIST CDF specifications can be used.

3 - **Interfaces and communication protocols**, describing the need to use standard hardware interfaces and communication protocol when connecting devices.

4 - **COTS** covering the requirement that any COTS devices used meet all applicable requirements.
4.1 – Voting system data that is imported, exported, or otherwise reported, is in an interoperable format.

4.1-A – Data export and exchange format
Voting devices must include support for the NIST SP Common Data Format (CDF) specifications for data inputs and output:

1. Election programming and results reporting data, NIST SP 1500-100
2. Election event logging data, NIST SP 1500-101
3. Cast vote records, NIST SP 1500-102
4. Voter registration-related data, NIST SP 1500-104

Discussion
Manufacturers can use proprietary data formats but need to also include support for the NIST CDF specifications. Implementations that do this using translations or conversions from a proprietary format would be considered in conformance.

4.1-B – Election programming data input and output
Election definition processes must include support for the NIST CDF specifications regarding:

1. Import and export of election programming data
2. Import and export of ballot programming data

Discussion
This requirement concerns import and export of pre-election data into an election definition device, such as for identification of political geography, contest, candidate, ballot data, and other pre-election information used to setup an election and produce ballots. This also includes reports of pre-election data from the election definition device that can be used to verify the election programming setup.

Applies to: election definition

4.1-C – Tabulator report data
Tabulation processes must include support for the NIST CDF specifications for import and export of election results reporting data.

Discussion
Importing results data is required so as to provide support for aggregations of vote data from different election management systems such as what occurs during state roll-ups on election night and during the process of election results certification.

External reference: URL to SP 1500-100, 102
Applies to: tabulation, reporting

4.1-D – Exchange of cast vote records (CVRs)
Casting, tabulation, and audit processes that use CVRs must include support for the NIST CDF specifications for export and import of those records.

Applies to: casting, tabulation, audit

Discussion
Devices that export or import CVRs typically include voter-facing and batch-fed scanners, election management systems, and other devices used for adjudication or auditing.

4.1-E – Exchange of voting device election event logs
The voting devices comprising the voting system must include support for the NIST CDF specifications for import or export of election event log data.

Discussion
This requirement refers to election event logs and not system logs provided by common operating systems such as Microsoft Windows or Apple iOS. This requirement does not mandate that manufacturers use the format for storing election log information; a manufacturer can meet this requirement by conversion or translation from a native format into the CDF.

4.1-F – Voting device event code documentation
Voting device and system manufacturers must include a specification for event codes used in their equipment and make this available upon request.

Discussion
Use of SP 1500-101 for election event logs only addresses the data format; it does not mandate a common lexicon for event codes. SP 1500-101 provides a separate schema for including documentation of event codes; manufactures may make this available publicly or upon request without condition.
4.1-G – Specification of common format usage

Voting device and system manufacturers must include a specification describing how the manufacturer has implemented a NIST CDF specification for a particular device or function. This includes such items as descriptions of how elements and attributes are used, as well as any constraints or extensions.

**Discussion**

Conformance to a common data format does not guarantee data interoperability. The manufacturer needs to document fully how it has interpreted and implemented a NIST CDF specification for its voting devices and the types of data exchanged or exported.
4.2 - Standard, publicly-available formats for other types of data not addressed by NIST CDF specifications are used.

4.2-A – Standard formats
Standard, publicly-available, and publicly-documented formats must be used, where possible, for exchanging data or encoding data.

Discussion
Examples include the use of common data encodings such as bar or QR codes.

4.2-B – Public documented manufacturer formats
Where it is not possible to meet requirement 4.1-A, manufacturers must include a publicly documented specification that describes the protocol or data format.

Discussion
As an example, a manufacturer’s algorithm or method for packing or compressing of data before encoding in a QR code will be documented so that its implementation and usage is available publicly.
4.3 - Widely-used hardware interfaces and communications protocols are used.

4.3-A – Standard device interfaces
Standard, common hardware interfaces and protocols must be used to connect devices.

Discussion
Examples include using published communications protocols, such as, IEEE, and using common hardware interfaces, such as, USB, when connecting to printers, disks, and other devices.
4.4 - Commercial-off-the-shelf (COTS) devices can be used if they meet all applicable VVSG requirements.

4.4-A – COTS devices meet applicable requirements
COTS devices, if used, must satisfy all applicable VVSG requirements.

Discussion
As an example, use of a COTS scanner to scan ballots is potentially possible, but there needs to be associated software to interpret the voter marks, create a cast vote record, and include support for the NIST CVR CDF. Together, the COTS scanner and associated software will meet applicable requirements for casting, counting, reporting, etc.
Principle 5
Equivalent and Consistent

All voters can access and use the voting system regardless of their abilities, without discrimination.

5.1 - Voters have a consistent experience throughout the voting process within any method of voting.

5.2 - Voters receive equivalent information and options in all modes of voting.
Principle 5
EQUIVALENT AND CONSISTENT VOTER ACCESS

All voters can access and use the voting system regardless of their abilities, without discrimination.

Principle 5 ensures that all voters can cast their votes easily and accurately, regardless of any disabilities they may have. This fulfills the requirements of the Help America Vote Act (HAVA), Section 301(a)(3) which states, “The voting system shall (A) be accessible for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters.”

It also addresses Section 508 of the Rehabilitation Act (amended in 1998) which requires that electronic and information technology be accessible to people with disabilities, and the language access requirements in the Voting Rights Act (VRA).

The goal of both guidelines in Principle 5 is to ensure that everyone can use the voting system, regardless of their abilities or preferences. Voting equipment can present ballot choices in a variety of ways which make it possible for people with a wide range of disabilities to vote. The equipment must also fully support all the languages that the manufacture claims to support. The big differences are that Guidelines:

1 – **Consistent experience** also covers the requirement that all vote records must be auditable by those who speak only English. And, in addition to actually casting their votes, people must have access to those same modes of presentation for all information and instructions related to casting those votes.

2 – **Equivalent information** also addresses the requirement that these modes of presentation (visual, audio, enhanced video) or interaction (touch, tactile, non-manual) must offer consistent and equivalent support for the actions required to vote, and offer them in a way that does not introduce bias. In addition, if the voter switches modes mid-stream, for example from video to audio mode or from Spanish to English, the system must preserve all settings and votes cast.

Finally, note that this principle’s requirements, including supporting the interaction modes listed in 5.1-A, also apply to all of the usability and accessibility requirements in Principles 6-8.
5.1 – Voters have a consistent experience throughout the voting process within any method of voting.

5.1-A – Interaction modes
All interaction modes including audio, tactile, enhanced visual, and non-manual must have the same capabilities as the visual interaction mode including ballot activation, voting, verification, and casting.

Discussion
For voting systems to meet this requirement they would need to include (among others):

- Features that support non-manual interaction enable voters with limited dexterity, that is those who lack fine motor control or the use of their hands, to submit their ballots privately and independently without manually handling the ballot.
- Features for paper ballots or paper verification records that assist voters with poor reading vision to read these ballots and records.
- Features to allow blind voters and voters with limited dexterity to perform paper-based verification, or feed their own optical scan ballots into a reader, if all other voters do so. For example, ballot papers or smart cards might provide tactile cues that allow the correct insertion of the card.
- Support for all methods of making ballot selections. For example, if a visual ballot supports voting a straight party ticket and then changing the vote for a single contest, so do all other interaction modes.

External reference: WCAG 2.0/Section 508
Prior VVSG sources: VVSG 1.1 - 3.2.5g, 3.3.3.b.i, 3.3.3.d, 3.3.3.e, 3.3.4.b, 3.3.8

5.1-B – Languages
The voting system must be capable of displaying, printing, and storing the ballot, contest options, review screens, vote verification records, and voting instructions in all languages the manufacturer has declared the system supports, in both visual and audio formats.

Discussion
Both written and unwritten languages are within the scope of this requirement.

The system will be tested in all languages that the manufacturer claims it is capable of supporting.

External reference: VRA
Prior VVSG sources: VVSG 1.1 - 3.2.7.a, 7.8.6.c, 7.8.6.ci, 7.8.6.cii
5.1-C – Vote records
All records, including paper ballots and paper verification records, must have the information required to support auditing by election workers and others who can read only English.

Discussion
Although the system needs to be easily usable by voters using an alternative language, records of the vote also need to be fully available to English-only readers for auditing purposes. Additional information, such as precinct and election identifiers may be in English to support election administration and auditing.

To meet this requirement, a paper ballot may not be a fully bilingual ballot. For instance, the full text of a ballot question might appear only in the alternative language, but the contest option (for example, “yes / no”) needs to be readable by English-only readers.

Prior VVSG source: VVSG 1.1 - 3.2.7.a.iii

5.1-D – Accessibility features
Accessibility features must be integrated into the manufacturer’s voting system so accessibility for voters with disabilities is supported throughout the voting session, including any steps to activate the ballot at the voting station, ballot marking, verification, and casting.

Discussion
This requirement ensures accessibility to the voter throughout the entire session. Not only are individual system components (such as ballot markers, paper records, and optical scanners) accessible, but they also work together to support voters with disabilities.

External Reference: HAVA
Prior VVSG source: VVSG 1.1: - 3.3.1.a

5.1-E – Reading paper ballots
If the voting system generates a paper record (or some other durable, human-readable record) that can be the official ballot or determinative vote record, then the voting system must allow the voter to verify the paper record using the same access features they used to mark the ballot, including audio, tactile, enhanced visual, and non-manual.

Discussion
Paper records present difficulties for voters who use large font, high contrast, alternative languages, and other settings. The purpose of this requirement is to ensure that all voters have a similar opportunity for vote verification.
This requirement allows the voter to use the same access features throughout the entire voting system. It also does not preclude the voter from choosing a different access feature to verify the record. For example, the voting system might provide a reader that converts the paper record contents into audio output.

**5.1-F – Accessibility documentation**

As part of the overall system documentation the manufacturer must include descriptions and instructions for all accessibility features that describe:

- recommended procedures that fully implement accessibility for voters with disabilities, and
- how the voting system supports those procedures.

**Discussion**

The purpose of this requirement is for the manufacturer not simply to deliver system components, but also to describe the accessibility scenarios they are intended to support, so that election offices have the information they need to effectively make accessibility features available to voters with disabilities.
5.2 – Voters receive equivalent information and options in all modes of voting.

5.2.A – No bias
The voting system must not introduce bias for or against any of the contest options presented to the voter. In audio, tactile, enhanced visual, and non-manual modes, all ballot options are to be presented in an equivalent manner.

Discussion
Certain differences in presentation are mandated by state law, such as the order in which candidates are listed and provisions for voting for write-in candidates. This requirement ensures that comparable characteristics such as font size or audio volume and speed are the same for all ballot options.

Prior VVSG source: VVSG 1.1 - 3.2.4.d

5.2-B – Presenting content in all languages
All information that is presented in English must also be presented in all other languages that are supported, whether the language is in visual or audio format. This includes instructions, warnings, messages, notification of undervotes or overvotes, contest options, and vote verification information.

Discussion
It is not sufficient simply to present the ballot options in the alternative languages. All the supporting information voters need to mark their ballot is also covered in this requirement.

External reference: VRA
Prior VVSG source: VVSG 1.1 - 3.2.7.a.ii

5.2-C – Information in all modes
Instructions, warnings, messages, notifications of undervotes or overvotes, and contest options must be presented to voters in the interaction modes required in 5.1-A – Interaction modes for all functions. This includes ballot activation, voting, verification, and casting.

Discussion
Examples of how to meet this requirement in the audio format include:
• An audio that includes cues to help users know what to expect. For example, announcing the number of items in a list of candidates or contests makes it easier to jump from one item to another without waiting for the audio to complete.

• Audio cues that also ensure the voter is aware of possible undervotes or overvotes.

External reference: WCAG 2.0/Section 508
Prior VVSG source: VVSG 1.1 - 3.3.1.b

5.2-D – Audio synchronized
The voting system must provide the option for synchronized audio output to convey the same information that is displayed visually.

Discussion
This requirement covers all information, including information entered by the voter such as write-in votes.

This requirement applies to any audio output, whether it is recorded or generated as text-to-speech.

Any differences between audio and visual information are for functional purposes only, with variations only based on differences in the interaction mode, especially for instructions.

This feature can assist voters with cognitive disabilities.

External reference: WCAG 2.0/Section 508
Prior VVSG source: VVSG 1.1 - 3.3.2.c

5.2-E – Sound cues
Sound and visual cues must be coordinated so that:

• Sound cues are accompanied by visual cues unless the system is in audio-only mode.

• Visual cues are accompanied by sound cues, unless the system is in visual-only mode.

Discussion
The voting equipment might beep if the voter attempts to overvote. If so, there has to be an equivalent visual cue, such as the appearance of an icon or a blinking element. If the voting system has been set to audio-only mode, there would be no visual cue.

Audio output also supports non-written languages, voters with low literacy, or voters with low vision.

External reference: WCAG 2.0/Section 508
Prior VVSG source: VVSG 1.1 - 3.3.6.b
5.2-F – Preserving votes
The voting system must allow the voter to switch among all modes including audio, tactile, enhanced visual, and non-manual, and change languages at any time during the voting session while preserving the current votes. When switching mode or language, the system will also preserve navigation, screen position, visual settings, audio settings, and other information within and across contests.

Discussion
A voter who initially chooses an English version of the ballot might switch to another language in order to read a referendum question.

Many blind voters have preferences for audio settings, including the rate of speech and volume that are important for comprehension.

Changing visual settings for text size might change the layout of the information on the screen, making it important to maintain the screen position.

External reference: WCAG 2.0/Section 508
Prior VVSG sources: VVSG 1.1 - 3.3.2.c.ii, 3.3.2.a, 3.2.7.a.i, 3.3.3.c.v, 3.3.3.c.vii, 3.3.6.a
Principle 6
Voter Privacy

Voters can mark, verify, and cast their ballot privately and independently.

6.1 - The voting process preserves the privacy of the voter's interaction with the ballot, modes of voting, and vote selections.

6.2 - Voters can mark, verify, and cast their ballot or other associated cast vote record, without assistance from others.
Principle 6

VOTER PRIVACY

Voters can mark, verify, and cast their ballot privately and independently.

Privacy for voters refers to the property of a voting system that is designed and deployed to enable voters to obtain a ballot, and mark, verify, and cast it without revealing their ballot selections or selections of language, display, and interaction modes to anyone else.

Privacy covers:

- electronic and paper interfaces,
- audio and video systems, and
- warning systems that must also preserve confidentiality.


The related Principle 10: Ballot Secrecy covers preventing links between a voter and a ballot after the ballot has been cast.

The Guidelines under Principle 6 cover:

1 – Privacy of interaction which describes the requirement that the voting process preserves the privacy of the voter’s interaction with the ballot, modes of voting and vote selections

2 – Voting without assistance which mandates that voters can mark, verify, and cast their ballot or other cast vote record without assistance from others.
6.1 - The voting process preserves the privacy of the voter’s interaction with the ballot, modes of voting, and vote selections.

6.1-A – Preserving privacy for voters
Privacy for voters must be preserved during the entire voting session including ballot activation, voting, verifying, and casting the ballot.

Discussion
This requirement allows for different approaches for electronic and paper interfaces. In both cases, appropriate shielding of the voting station is important -- for example, privacy screens for the voting stations.

When a paper record with ballot information needs to be transported by the voter, devices such as privacy sleeves can be necessary. This requirement applies to all records with information on votes (such as a vote verification record) even if that record is not itself a ballot.

External reference: HAVA
Prior VVSG source: VVSG 1.1 - 7.8.5.a, 3.2.3.1.b
Related requirements: 7.2-F – Voter speech

6.1-B – Warnings
The voting system must issue all warnings in a way that preserves privacy for voters and the confidentiality of the ballot.

Discussion
HAVA 301 (a)(1)(C) mandates that the voting system notifies the voter of an attempted overvote in a way that preserves privacy for voters and the confidentiality of the ballot. This requirement addresses that mandate.

External reference: HAVA
Prior VVSG source: VVSG 1.1 - 3.2.3.1.d
Related requirements: 7.3-K – Warnings, alerts, instructions

6.1-C – Enabling or disabling output
The voting system must make it possible for the voter to independently enable or disable either the audio or the video output and be notified of the change, resulting in a video-only or audio-only presentation.

Discussion
Voters can be notified of the change to the display or audio output in a variety of ways including beep, voice, or visual notification. An unobtrusive notification that the system has changed the visual display mode is helpful to voters who cannot see the screen to confirm the change visually.

- **External reference:** WCAG 2.0/Section 508
- **Prior VVSG source:** VVSG 1.1 - 3.3.2.c.i
- **Related requirements:** 7.2-A – Display and interaction options
  7.3-K – Warnings, alerts, instructions

### 6.1.D – Audio privacy
Audio during the voting session must be audible only to the voter.

**Discussion**

Voters who are hard of hearing but need to use an audio interface sometimes need to increase the volume of the audio. Such situations require headphones or other devices (such as a hearing loop) with low sound leakage so the contents of the audio cannot be overheard and understood by others. Voters who are hard of hearing can share audio interfaces with their designated assistants.

- **External reference:** WCAG 2.0/Section 508
- **Prior VVSG source:** 3.2.3.1.c
- **Related requirements:** 7.2-F – Voter speech
  8.1-J – Hearing aids
6.2 - Voters can mark, verify, and cast their ballot or other associated cast vote record without assistance from others.

6.2-A - Voter Independence

Voters must be able to mark, verify, and cast their ballot or other associated cast vote records independently and without assistance from others.

Discussion

This requirement ensures that voters can vote with their own interaction preferences and without risk of intimidation or influence.

HAVA 301 (a)(1)(C) mandates that the voting system be accessible for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters. This requirement directly addresses this mandate.

External reference: HAVA
Prior VVSG source: 7.8.5.a, 3.2.3.1.b
Related requirements: 5.1-D – Accessibility features
5.1-E – Reading paper ballots
2.2-A – User-centered design process.
Principle 7
Marked, Verified, and Cast as Intended

Ballots and vote selections are presented in a perceivable, operable, and understandable way and can be marked, verified, and cast by all voters.

7.1 - The default voting system settings present a ballot usable for the widest range of voters, and voters can adjust settings and preferences to meet their needs.

7.2 - Voters and election workers can use all controls accurately, and voters have direct control of all ballot changes and selections.

7.3 - Voters can understand all information as it is presented, including instructions, messages from the system, and error messages.
Principle 7
MARKED, VERIFIED, AND CAST AS INTENDED

Ballots and vote selections are presented in a perceivable, operable, and understandable way and can be marked, verified, and cast by all voters.

This principle covers the core actions of voting, supporting voters in marking, verifying, and casting their ballot. It includes all voting systems including both paper ballots and electronic interfaces.

The requirements in P-7 are derived from federal laws, including:

- the Help America Vote Act (HAVA),
- Section 508 (part of the Rehabilitation Act of 1973)
- Web Content and Accessibility Guidelines (WCAG), and,
- the Voting Rights Act.

This principle is divided into three sections which follow 508/WCAG’s well-known organizing principles of Perceivable, Operable, and Understandable. Robust, the final POUR principle is included in Principle 8 – Robust, safe, usable and accessible. The Guidelines under Principle 7 are:

1 – Default settings covers how ballot information is presented using audio and visual settings, as well as the voter’s ability to adjust the voting system to meet their needs or preferences. This includes using color and contrast, adjusting font size, and ensuring audio settings result in understandable speech.

2 – Controls covers a voter’s operation of the voting system, that is, the interaction with and control of the ballot during voting, including how the information is displayed and the voter’s ability to navigate the system. It addresses the voter’s ability to scroll through the electronic ballot, use the audio and touch controls, and use simple gestures. It also includes the need for adequate space for those who use wheelchairs. Both voters and election workers must be able to use all controls accurately.

3 – Understandable information covers the ability of the voter to understand all information on the ballot as it is presented, including instructions and messages from the system. Among other elements, it includes preventing contest layouts that can cause confusion, making clear the maximum number of choices a voter has, notifying the voter of any errors on the ballot (such as overvotes) before it is cast, and letting the voter know when they have successfully voted. It also covers ensuring that instructions for election workers are understandable.
7.1 – The default voting system settings present a ballot usable for the widest range of voters, and voters can adjust settings and preferences to meet their needs.

7.1-A – Reset to default settings
If the adjustable settings of the voter interface have been changed by the voter or election worker during the voting session, the system must automatically reset to the default setting when the voter finishes voting, verifying, and casting.

Discussion
This ensures that the voting system presents the same initial appearance to every voter.

This requirement covers all settings that can be adjusted, including font size, color, contrast, audio volume, rate of speech, turning on or off audio or video, and enabling alternative input devices.

External reference: WCAG 2.0/Section 508
Prior VVSG source: VVSG 1.1 - 3.2.5.b
Related requirement: 7.1-K – Audio settings
Applies to: Electronic interfaces

7.1-B – Reset by voter
If either the voter or an election worker can adjust the settings of the voter interface, there must be a way for the voter to restore the default settings while preserving the current votes.

Discussion
This requirement allows a voter or election worker who has adjusted the system to an undesirable state to reset all settings and start over.

External reference: WCAG 2.0/Section 508
Prior VVSG source: VVSG 1.1 - 3.2.5.c
Related requirement: 5.2F – Preserving votes
Applies to: Electronic interfaces
7.1-C – Default contrast
The default contrast ratio must be at least 10:1 for all elements that visually convey information such as text, controls, and infographics or icons.

1. For electronic displays for voters and election workers, this is measured as a luminosity contrast ratio between the foreground and background colors of at least 10:1.
2. For paper ballots and other paper records, the contrast ratio will be at least 10:1 as measured based on ambient lighting of at least 300 lx.

Discussion
For example, this applies to:

- candidate names,
- a broken arrow,
- the outline of an oval, circle, or rectangular target used to mark voter selections, or
- informational icons identifying voter selections or other information.

Purely decorative elements that do not communicate meaning do not have to meet this requirement.

A 10:1 luminosity contrast ratio provides enough difference between the text and background to enable people with most color vision deficiencies to read the ballot. This is higher than the highest contrast requirements of 7:1 in WCAG 2.0 Checkpoint 1.4.6 (Level AAA) to accommodate a wider range of visual disabilities. There are many free tools available to test color luminosity contrast using the WCAG 2.0 algorithm.

External reference: WCAG 2.0/Section 508
Prior VVSG source VVSG 1.1 - 3.2.2.2.f.ii, 3.2.5.h, 3.2.5.h.i, 3.2.5.h.ii

7.1-D – Contrast options
The voting system must provide options for high and low contrast displays, including the alternative display contrast options as listed below:

1. A high contrast option with a white background and dark text, with a luminosity contrast ration of at least 20:1

2. A high contrast option with a black background (between #000000 and #111111) and one of the following foreground options:
   a. Yellow text similar to #FFFF00, providing a contrast ratio of at least 17.5:1
   b. Cyan text similar to #00FFFF, providing a contrast ratio of at least 15:1
   c. White text similar to #FAFAFA, providing a contrast ratio of at least 18:1

1. A low contrast option, providing a contrast ratio in the range of 4.5:1 to 8:1
Discussion

This requirement for options for the overall display contrast ensures that there is an option for the visual presentation for people whose vision requires either high or low contrast.

High and low contrast options apply to the entire screen, including decorative elements.

Examples of color combinations for a low contrast options include:

- Brown text similar to #BB9966 on a black background (7.8:1)
- Black text on a background with text similar to #BB9966 (7.8:1)
- Grey text similar to #6C6C6C on a white background (5.2:1)
- Grey/brown text similar to #97967E on a black background (6.9:1)
- Grey text similar to #898989 on a dark background similar to #222222 (4.5:1)

External reference: WCAG 2.0/Section 508
Prior VVSG source: VVSG 1.1 - 3.3.2.a.i, 3.2.5.h.ii
Applies to: Electronic interfaces

7.1-E – Color conventions

The use of color by the voting system must follow these common conventions:

1. Green, blue, or white is used for general information or as a normal status indicator
2. Amber or yellow is used to indicate warnings or a marginal status
3. Red is used to indicate error conditions or a problem requiring immediate attention

External reference: WCAG 2.0/Section 508
Prior VVSG source: VVSG 1.1 - 3.2.4.f

7.1-F – Using color

Color coding must not be used as the only means of communicating information, indicating an action, prompting a response, distinguishing a visual element, or providing feedback on voter actions or selections.

Discussion

While color can be used for emphasis, some other non-color mode is also needed. This could include shape, lines, words, text, or text style. For example, an icon for “stop” can be red enclosed in an octagon shape. Or, a background color can be combined with a bounding outline and a label to group elements on the ballot.

External reference: WCAG 2.0/Section 508
Prior VVSG source: VVSG 1.1 - 3.2.5.i
7.1-G – Text size (electronic display)

A voting system’s electronic display must be capable of showing all information in a range of text sizes that voters can select from, with a default text size at least 4.8 mm (based on the height of the uppercase I), allowing voters to both increase and decrease the text size.

The voting system may meet this requirement in one of the following ways:

1. Provide continuous scaling with a minimum increment of 0.5 mm that covers the full range of text sizes from 3.5 mm to 9.0 mm.
2. Provide at least four discrete text sizes, in which the main ballot options fall within one of these ranges.
   a) 3.5-4.2 mm (10-12 points)
   b) 4.8-5.6 mm (14-16 points)
   c) 6.4-7.1 mm (18-20 points)
   d) 8.5-9.0 mm (24-25 points)

Discussion

The text size requirements have been updated from the VVSG 1.1 requirement to better meet the needs of voters who need larger text, including older voters, voters with low literacy, and voters with some cognitive disabilities.

This requirement also fills a gap in the text sizes required in VVSG 1.1 which omitted text sizes needed or preferred by many voters. Although larger font sizes assist most voters with low vision, certain visual disabilities such as tunnel vision require smaller text.

The sizes are minimums. These ranges are not meant to limit the text on the screen to a single size. The text can fall in several of these text sizes. For example, candidate names or voting options might be in the 4.8-5.6 mm range, secondary information in the 3.5-4.2 mm range, and titles or button labels in the 6.4-7.1 mm range.

The default text size of 4.8 mm is based on “Information and Communication Technology (ICT) Final Standards and Guidelines” (36 CFR Parts 1193 and 1194, RIN 3014-AA37, published in the Federal Register on January 18, 2017)

External reference: WCAG 2.0/Section 508
Prior VVSG source: VVSG 1.1 - 3.2.5.d, 3.2.5.e
Related requirements: 5.2-A – No bias
5.2-F – Preserving votes
7.2-D – Scrolling
7.3-B – No split contests
Applies to: Electronic interfaces
7.1-H – Scaling and zooming (electronic display)

When the text size is changed, all other information in the interface, including informational icons, screen titles, buttons, and ballot marking target areas, must change size to maintain a consistent relationship to the size of the text. Informational elements in the interface do not have to be scaled beyond the size of the text.

1. When the text is enlarged up to 200% (or 7.1 mm text size), the ballot layout must adjust so that there is no horizontal scrolling or panning of the screen.

2. When the text is enlarged more than 200%, there may be horizontal scrolling or panning if needed to maintain the layout of the ballot and a consistent relationship between the text for ballot options and associated marking targets.

Discussion

The intention of this requirement is that all of the informational elements of the interface change size in response to the text size. However, some interface designs include elements that are already large enough that making them larger would distort the layout. In this case, this does not require those elements to grow proportionately beyond the size of the text.

Techniques for managing scaling and zooming an electronic interface while adjusting the layout to fit the new size are sometimes called responsive design or responsive programming.

This requirement does not preclude novel approaches to on-screen magnification such as a zoom lens showing an enlarged view of part of a screen (as long as it meets the requirements in 7.2 for the operability of the controls).

This requirement follows WCAG 2.0 in requiring scaling with no horizontal scrolling up to 200% and allowing zooming with horizontal scrolling for larger text.

External reference: WCAG 2.0/Section 508
Related requirements: 7.1-G – Text size (electronic display) 7.2-D – Scrolling 5.1-A – Interaction modes 5.2-A – No Bias 5.2-C – All information in all modes 5.2-F – Preserving votes

Applies to: Electronic interfaces

7.1-I – Text size (paper)

The voting system must be capable of printing paper ballots and other paper records with a minimum font size of 3.5 mm (10 points).

Discussion
Although the system can be capable of printing in several font sizes, local or state laws and regulations can also govern the use of various font sizes.

If the voting system includes a large-print display option, a good range for the text size is 6.4-7.1 mm matching the size in 7.1-G-Text size (electronic display)

If typography changes such as text size or display style are used to differentiate languages on a multi-lingual ballot, the requirements in 5.2-A-No bias (and relevant state election law for ballot design) still apply.

Prior VVSG source: VVSG 1.1 - 3.2.5.i
Related requirements: 5.1-E – Reading paper ballots
7.1-G – Text size (electronic display)
Applies to: Printed Material

7.1-J – Sans-serif font
The voting system must be capable of presenting text intended for the voter in a sans-serif font.

Discussion
This requirement ensures that systems are capable of best practice while allowing them to also meet local or state laws or regulations that might differ.

In general, sans-serif fonts are easier to read on-screen, look reasonably good when their size is reduced, and tend to retain their visual appeal across different platforms. Examples of sans-serif fonts with good readability characteristics include Arial, Calibri, Microsoft Tai Le, Helvetica, Univers, Clearview ADA, or Open Sans.

“Information and Communication Technology (ICT) Final Standards and Guidelines” (36 CFR Parts 1193 and 1194, RIN 3014-AA37, published in the Federal Register on January 18, 2017) requires that at least one mode of characters displayed on the screen be a sans-serif font.

The guidance on suitable fonts replaces the detailed text characteristics in VVSG 1.1

External reference: WCAG 2.0/Section 508
Prior VVSG sources: VVSG 1.1 - 3.2.5.f, 3.2.5.d

7.1-K – Audio settings
The voting system must meet the following requirements:

1. The settings for volume and rate of speech are followed regardless of the technical means of producing audio output.

2. The default volume for each voting session is set between 60 and 70 dB SPL.
3. The volume is adjustable from a minimum of 20dB SPL up to a maximum of 100 dB SPL, in increments no greater than 10 dB.

4. The rate of speech is adjustable throughout the voting session while preserving the current votes, with 6 to 8 discrete steps in the rate.

5. The default rate of speech is 125 to 150 words per minute (wpm).

6. The range of speech rates supported is from 50 wpm to 300 wpm (or 75% to 200% of the default rate).

7. Adjusting the rate of speech does not affect the pitch of the voice.

Discussion
This requirement is intended to be tested using “real ear” measurements not simply measurements at the point of the audio source.

According to an explanation written by the Trace Center (http://trace.umd.edu/docs/2004-About-dB), 60 dB SPL is the volume of ordinary conversation.

FCC regulations for hearing aids, 47 CFR Parts 20 and 68: Hearing Aid Standard, includes useful information about how to test audio volume and quality.

External reference: WCAG 2.0/Section 508
Prior VVSG source: VVSG 1.1 - 3.3.3.c.iv
Related requirements: 7.1-A – Reset to default settings

7.1-L – Speech frequencies
The voting system’s audio format interface must be able to reproduce frequencies over the audible speech range of 315 Hz to 10 KHz.

Discussion
The required frequencies include the range of normal human speech. This allows the reproduced speech to sound natural.

This is a requirement for the capability of the system so that it is possible to create intelligible audio. It is not a requirement for a ballot in a real election, which is outside of the scope of the VVSG.

External reference: WCAG 2.0/Section 508
Prior VVSG source: VVSG 1.1 - 3.3.3.c.iv

7.1-M – Audio comprehension
The voting system must be capable of presenting audio content so that it is comprehensible to voters who have normal hearing and are proficient in the language with:
1. proper enunciation, normal intonation, accurate pronunciation in the context of the information, and the capability to pronounce candidate names as intended

2. low background noise

3. recording or reproduction in dual-mono, with the same audio information in both ears.

Discussion

This requirement covers both recorded and synthetic speech. It applies to those aspects of the audio content that are inherent to the voting system or that are generated by default. To the extent that election officials designing the ballot determine the audio presentation, it is beyond the scope of this requirement.

Support for non-written languages and low literacy includes audio output that is usable by voters who can see the screen.

The International Telecommunications Union (ITU) provides a set of freely available test signals for testing audio quality in Rec. ITU-T P.50 Appendix I (http://www.itu.int/net/itu-t/sigdb/genaudio/AudioForm-g.aspx?val=1000050)

External reference: WCAG 2.0/Section 508
ITU-T P.50 Appendix I

Prior VVSG source: VVSG 1.1 - 3.3.3.c.vii

7.1-N – Tactile keys

Mechanically operated controls, buttons, keys, or any other hardware interfaces (including dual switches or sip-and-puff devices) on the voting system available to the voter must:

1. be tactiley discernible without activating those controls or keys
2. include a Braille label if there is a text label
3. not require sequential, timed, or simultaneous presses or activations, unless using a full keyboard.

Discussion

A blind voter can operate the voting system by “feel” alone. This means that vision is not necessary for such operations as inserting a smart card or plugging into a headphone jack.

Controls that are distinguished only by shape without a text label do not need a Braille label.

Controls do not depend on fine motor skills.

External reference: WCAG 2.0/Section 508
Prior VVSG source: VVSG 1.1 - 3.3.3.f
Related requirement; 7.2-E – Touchscreen gestures  
7.2-H – Accidental activation  
7.2-R – Control labels visible  
7.3-L – Icon labels

7.1-O – Toggle keys
The status of all locking or toggle controls or keys (such as the "shift" key) for the voting system must be visually discernible, and also discernible through either touch or sound.

External reference: WCAG 2.0/Section 508  
Prior VVSG source: VVSG 1.1 - 3.3.3.g

7.1-P – Identifying controls
Buttons and controls that perform different navigation or selection functions must be distinguishable by both shape and color for tactile and visual perception.

Well-known arrangements of groups of keys may be used only for their primary purpose. For example, a full alphabetic keyboard is acceptable for entering a write-in candidate name, but individual keys cannot be used for navigation or selection.

Discussion
This applies to buttons and controls implemented either on-screen or in hardware. For on-screen controls, shape includes the label on the button.

Redundant cues help those with low vision. They also help individuals who have difficulty reading the text on the screen, those who are blind but have some residual vision, and those who use the controls on a voting system because of limited dexterity. While this requirement primarily focuses on those with low vision, features such as tactile controls and on-screen controls intended primarily to address one kind of disability often assist other voters as well. The Trace Center’s EZ Access design is an example of button functions distinguishable by both shape and color:  https://trace.umd.edu/ez

EAC RFI 2007-05 is incorporated into this requirement.

External Reference: WCAG 2.0/Section 508  
EAC RFI 2007-05

Prior VVSG source: VVSG 1.1 - 3.3.2.b
7.2 – Voters and election workers can use all controls accurately, and voters have direct control of all ballot changes.

7.2-A – Display and interaction options
The voting system must provide at least the following display formats and control or navigation options to enable voters to activate their ballot, mark their ballot to vote, and verify and cast their ballot, supporting the full functionality in each mode:

1. Visual format with enhanced visual options
2. Audio format
3. Tactile controls
4. Limited dexterity controls

Discussion
Voters need to be able to choose the combination of display formats and types of controls that work for them, for example, combining the audio format with tactically discernible controls.

Limited dexterity controls are defined in the Glossary as those that do not require dexterity and can be operated without use of hands.

Full functionality includes at least instructions and feedback:

- on initial activation of the ballot (such as insertion of a smart card), if applicable;
- on how to use accessibility features and setting;
- on a change in the display format or control options;
- for navigating the ballot;
- for contest options, including write-in candidates;
- on confirming and changing votes; and
- on final ballot submission.

External reference: WCAG 2.0/Section 508
Prior VVSG sources: VVSG 1.1 - 3.3.3.b, 3.3.8
Related requirements: 5.1-A – Interaction modes 5.2-A – No bias

7.2-B – Navigation between contests
The electronic ballot interface must provide navigation controls that allow the voter to advance to the next contest or go back to the previous contest before completing their vote.

Discussion
For example, voters are not forced to proceed sequentially through all contests before going back to check their votes within a previous contest.

This requirement applies whether the voter is using the visual or audio format, or synchronized audio and video.

As with all requirements, this applies to all interaction modes.

External reference: WCAG 2.0/Section 508
Prior VVSG sources: VVSG 1.1 - 3.2.2.1.e, 3.3.3.3.e
Related requirements: 7.2-A – Display and interaction options

7.2-C – Voter control
An electronic ballot interface must give voters direct control over making or changing vote selections within a contest:

1. In a vote-for-one contest, selecting a candidate may deselect a previously selected candidate, but the system must announce the change in audio and visual display.

2. In a vote-for-N-of-M contest, the system must not deselect any candidate automatically.

3. 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.

4. 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.

5. Ballots with preferential or ranking voting methods must not re-order candidates except in response to an explicit voter command.

Discussion
This requirement covers any selection, de-selection, or change to ballot options. It can be met in a variety of ways, including notifications or announcements of the action the system is taking. For example, if a voter attempts to mark a selection for more candidates than allowed, the system does not take an independent action to de-select a previously selected candidate, but instead notifies the voter of the problem and offers ways to correct it.

As with all requirements, this applies to all interaction modes.

This requirement addresses situations in which the voter cannot see the change take effect because the previously selected candidate is on another screen, has scrolled off the visible display area, or is out of the voter’s field of vision. It is particularly important to voters using the audio format and no
visual display because they often do not have a way to know that a change that occurs higher up in the contest has taken place.

Examples of feedback include visual changes on the screen and related sounds or messages in text and audio. For example, selecting a candidate is often announced visually with a check-mark image and in audio by naming the candidate selected.

If there is a visual change or announcement about the number of candidates selected (or selections still available), for example, the audio says “you have selected the maximum number of candidates in this contest” in a vote-for-N contest.

An example of feedback on the result of a complex action, such as making a selection in straight party voting, might be a message confirming the party whose candidates were selected, or even the number of candidates and contests affected by the voter’s action.

Related requirements: 7.2-A – Display and interaction options
7.3-E – Feedback
7.3-F – Correcting the ballot

7.2-D – Scrolling

If the number of candidates or length of the ballot question means that the contest does not fit on a single screen using the voter’s visual display preferences, the voting system must provide a way to navigate through the entire contest.

1. The voting system may display the contest by:
   - Pagination - Dividing the list of candidates or other information into “chunks,” each filling one screen and providing ways for the voter to navigate among the different chunks, or
   - Scrolling – Keeping all of the content on a single long display and providing controls that allow the voter to scroll continuously through the content.

2. For either display method, the voting system interface must:
   - have a fixed header or footer that does not disappear so voters always have access to navigation elements, the name of the current contest, and the voting rules for the contest,
   - include easily perceivable cues in every interaction mode to indicate that there is more information or there are more contest options available, and
   - include an option for an audio format and visual presentation that sync during scrolling.

3. The navigation method must ensure that the voting system:
• meets all requirements for providing feedback to the voter,
• accurately issues all warnings and alerts including notifications of undervotes and overvotes,
• meets all requirements for control size and interaction, and keeping all controls visible,
• does not rely only on conventional platform scroll bars, and
• provides an opportunity to review and correct selections before leaving the contest.

Discussion
The ability to scroll through a list of candidates on a single logical page can be particularly important when a voter selects larger text or is using the audio format.

Information elements that need not scroll might include the name of the contest (“City Council Member”), the voting rules (“vote for 1”) and general controls including preference settings or navigation between contests.

A scrolling interface that meets this requirement offers voters a combination of easily perceivable controls or gestures to navigate through the list of candidates or text of a ballot question. For example:

• Navigation within the contest does not rely on knowledge of any particular computer platform or interface standard.
• Navigation within the contest does not only rely on conventional platform scroll bars, which operate differently on two of the major commercial computer platforms.
• Controls have visible labels that include words or symbols.
• Controls are located in the voter’s visual viewing area at the bottom (or top) of the scrolling area, for example in the center of the column of names or paragraph of text. This is especially helpful for people with low digital or reading literacy.
• Controls are identified in the audio format and can be activated in all interaction modes.

This overall requirement relates to 7.1-G-Text size, 7.1-H-Scaling and zooming, and 7.3-B-No split contests

The controls used to meet this requirement also need to meet all other requirements including 7.2-H – Accidental activation, 7.2.I-Touch area size, 7.2-F-Voter speech, and 7.2-E-Touch gestures.

Meeting requirements for notifications relates to 7.3-E-Feedback, 7.3-F-Correcting the ballot, 7.3-H-Overvotes, 7.3-I-Undervotes, and 7.3-K-Warnings, alerts, and instructions.

Prior VVSG source: VVSG 1.1 - 3.2.6.a
7.2-E – Touchscreen gestures

Voting systems with a touch screen may use touchscreen gestures (physical movements by the user while in contact with the screen to activate controls) in the interface if the following conditions are met:

1. Gestures are offered as another way of interacting with a touch screen and an optional alternative to the other interaction modes.
2. Gestures are limited to simple, well-known gestures.
3. Gestures do not include navigation off the current contest.
4. Gestures are used in a way that does not create accidental activation of an action through an unintended gesture.
5. Gestures work consistently across the entire voting interaction.
6. Gestures do not require sequential, timed or simultaneous actions.

**Discussion**

This requirement ensures that the use of gestures does not interfere with the accessibility features of the voting system or make the interface difficult to use by relying on a control mode with no easy way to make them perceivable in the visual or audio formats.

In relying on simple and common gestures, this requirement does not intend to fully duplicate the gestures for commercial mobile platforms used with an audio mode for accessibility.

Tapping (touching the screen briefly) is the most basic gesture and is used on all touch screens. Other commonly used gestures include:

- Pinching or spreading fingers to zoom
- Swiping to scroll
- Pressing and holding to drag
Examples of gestures that require sequential or simultaneous actions are double-tapping, 2, 3 or 4 finger swiping, touch and hold for a set period of time, or those that require coordinated actions with fingers on both hands. On desktop systems, assistive preference options like Sticky Keys can make these complex gestures accessible, but they require familiarity beyond what is acceptable in a voting system.

Examples of timed gestures include differentiating between long and short touches or which require touching twice in rapid succession to highlight and then activate the button or selection.

Related requirement: 7.2-H – Accidental activation
7.1-N – Tactile keys

7.2-F – Voter speech
If the voting system includes speech or human sounds as a way of controlling the system:

1. it must not require the voter to speak recognizable voting selections out loud, and
2. speech input must not be the only non-visual interaction mode.

Discussion
This requirement allows the use of speech input as long as voters can choose other ways of interacting with the voting system that do not require either vision or use of their hands.

It is also important to consider how speech would work as a way of voting in a noisy polling place environment.

External reference: WCAG 2.0/Section 508
Prior VVSG source VVSG 1.1 - 3.3.9.a
Related requirements: 6.1-A-Preserving privacy for voters
6.1-D-Audio privacy

7.2.G – Voter control of audio
The voting system must allow the voter to control the audio presentation including:

1. pausing and resuming the audio
2. repeating any information
3. skipping to the next or previous contest, and
4. skipping over the reading of the ballot question text.

Discussion
These features can also be useful to voters with cognitive disabilities.

This is comparable to the ability of sighted voters to:
• move on to the next contest once they have made a selection or to abstain from voting on a contest altogether, or
• skip over the wording of a referendum on which they have already made a decision prior to the voting session (for example, "Vote yes on proposition #123").

External reference: WCAG 2.0/Section 508
Prior VVSG sources; VVSG 1.1 - 3.3.3.b.ii, 3.3.3.b.iii, 3.3.3.b.iv, 3.3.3.b.v, 3.3.8
Applies to: Electronic interfaces

7.2-H – Accidental activation
Both on-screen and physical controls on the voting system must be designed to prevent accidental activation.

Discussion
There are at least two kinds of accidental activation:

• When a control is activated to execute an action as it is being “explored” by the voter because the control is overly sensitive to touch.
• When a control is in a location where it can easily be activated unintentionally. For example, when a button is in the very bottom left corner of the screen where a voter might hold the unit for support.

Work on the next version of WCAG includes a similar requirement and offers guidelines for preventing accidental activation including that the activation be on the release of the control (an “up-event”) or equivalent, or that the system provides an opportunity to confirm the action.

In addition to the accessibility needs for preventing accidental activation, it can be an issue if voters perceive the voting system as changing their voting selections.

External references: WCAG 2.0/Section 508
Prior VVSG source: VVSG 1.1 - 3.2.6.c
Related requirements: 7.2-E – Touch gestures
7.1-N – Tactile keys

7.2-I – Touch area size
If the voting system has a touch screen, the touch target areas must:

1. be at least 12.7 mm (0.5 inches) in both vertical and horizontal dimensions,
2. be at least 2.54 mm (0.1 inches) away from adjacent touch areas, and
3. not overlap another touch area.

Discussion
The requirements for touch size areas on voting systems are larger than commercial standards for mobile devices:

- to ensure that the touch areas are large enough for voters with unsteady hands,
- to ensure that voting systems allow full adjustment to the most comfortable posture, and
- to allow for touchscreens that do not include advanced algorithms to detect the center point of a touch.

The required touch area size is larger than some of the commercial standards for mobile phones to allow for use by voters with limited dexterity.

The required marking area size is within sizes suggested in the draft WCAG 2.1 for target areas that accept a touch action.

An MIT Touch Lab study of Human Fingertips to Investigate the Mechanics of Tactile Sense found that the average human finger pad is 10-14 mm and the average fingertip is 8-10 mm.

External references: WCAG 2.0/Section 508
VVSG 1.1: 3.2.6.c.i
Applies to: Touch screen interfaces

7.2-J – Paper ballot target areas

On a paper ballot that a voter marks by hand, the area of the target used to mark a voting selection must be at least 3 mm (0.12 inches) across in any direction.

Discussion

This requirement applies to marking ovals, circles, squares, or other optical scan ballot designs.

Although the marking target for hand-marked paper ballots needs to be large enough to see, a target that is too large can also make it hard to fill in the area completely.

Prior VVSG source: VVSG 1.1 - 3.2.2.2.f.i
Applies to: Paper ballots

7.2-K – Key operability

Physical keys, controls, and other manual operations on the voting station must be operable with one hand and not require tight grasping, pinching, or twisting of the wrist. The force required to activate controls and keys must be no greater than 5 lbs. (22.2 N).

Discussion
Voters can operate controls without excessive force. This includes operations such as inserting an activation card, and inserting and removing ballots.

This does not apply to on-screen controls.

7.2-L – Bodily contact

The voting station controls must not require direct bodily contact or for the body to be part of any electrical circuit. If some form of contact is required, a stylus or other device with built-in permanent tips will be supplied to activate capacitive touch screens.

Discussion

This requirement ensures that controls and touch screens can be used by individuals using prosthetic devices or that it is possible to use a stylus on touch screens for either greater accuracy or limited dexterity input.

One type of touch screen – capacitive touch panels – rely on the user’s body to complete the circuit. EAC RFI 2015-05 states that they can be used if manufacturers supply a stylus or other device that activates the capacitive screen.

7.2-M – No repetitive activation

Voting system keys or controls must not have a repetitive effect when they are held in an active position.

Discussion

This is to preclude accidental activation. For instance, if a voter is typing in the name of a write-in candidate, depressing and holding the "e" key results in only a single "e" added to the name.

7.2-N – System response time

The voting system’s response time must meet the following standard response times:

1. The system initially responds to a voter action in no more than:
a. 0.1 seconds for a visual change
b. 0.5 seconds for an audio response

2. The system responds to a voter marking a vote in no more than 1 second for both a visual response and an initial audio response.

3. The system completes the visual response or display in no more than 1 second or displays an indicator that a response is still being prepared.

**Discussion**

This is so the voter can very quickly perceive that an action has been detected by the system and is being processed. The voter never gets the sense of dealing with an unresponsive or "dead" system. Note that this requirement applies to both auditory and visual voting system responses.

For example, if the voter touches a button to indicate a vote for a candidate, a visual system might display an "X" next to the candidate's name, and an audio system might announce, "You have voted for John Smith for Governor". Even for "large" operations such as initializing the ballot or painting a new screen, the system never takes more than 10 seconds.

In the case of audio systems, no upper limit is specified, since certain operations can take longer, depending on the length of the text being read (for example, reading out a long list of candidates running in a contest). For instance, the system might present a progress bar indicating that it is "busy" processing the voter's request. This requirement is intended to preclude the "frozen screen" effect, in which no detectible activity is taking place for several seconds. There need not be a specific "activity" icon, as long as some visual change is apparent (such as progressively "painting" a new screen or providing audio feedback).

**External references:**
WCAG 2.0/Section 508
Prior VVSG sources; VVSG 1.1 - 3.2.6.1.a, 3.2.6.1.b, 3.2.6.1.c, 3.2.6.1.d
Applies to: Electronic interfaces

**7.2-O – Inactivity alerts**

If the voter has not interacted with the voting system for a long time (that is, between 2-5 minutes), the system must notify the voter and meet the following requirements:

1. Each system must specify what they mean by inactivity time and keep a record of it.

2. When the voter’s inactivity time expires, the electronic ballot interface must issue an alert and provide a way for the voter to receive additional time.

3. The alert time must be between 20 and 45 seconds.

4. If the voter does not respond to the alert within the alert time, the electronic ballot interface must go into an inactive state requiring election worker intervention.
Discussion

Each type of system will have a given inactivity time that is consistent among and within all voting sessions. This ensures that all voters are treated equitably.

The timer starts when the voter finishes reading a referendum.

External references: WCAG 2.0/Section 508
Prior VVSG sources: VVSG 1.1 - 3.2.6.1.e, 3.2.6.1.f
Applies to: Electronic interfaces

7.2-P – Floor space

When used according to the manufacturer’s installation instructions, the voting station must allow floor space for voters using a wheelchair or a voter’s assistant by:

1. providing a clear area for a wheelchair of 760 mm (30 inches) wide and 1220 mm (48 inches) deep, and
2. providing adequate room for a voter’s assistant, including enough room for both the voter and an assistant to enter the area of the voting station.

Discussion

This requirement ensures that a voter using a wheelchair, or a voter and an assistant, have enough room to enter and leave the voting station and use the voting system.

External references: WCAG 2.0/Section 508
Prior VVSG sources: VVSG 1.1 - 3.3.5.a, 3.3.5.b

7.2-Q – Physical dimensions

The physical dimensions of the voting station must meet the U.S. Access Board requirements in Appendix A to Part 1194 – Section 508 of the Rehabilitation Act: Application and Scoping Requirements, Chapter 4: Hardware, Section 407.8 Operable Parts: Reach Height and Depth.

Discussion


The text of the requirements for reach height and depth with illustrations can be found on the U.S. Access Board website at https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/proposed-rule/text-of-the-proposed-rule#f407121
Many voting systems can be set up in a variety of ways for use in a polling place or vote center. For example, a system might sit on a table that allows voters to put their legs under the table in a polling place, but on a counter with no legroom in a vote center. Wheelchairs and scooters also allow voters different degrees of freedom to reach controls, and the voter might approach the voting system from the front or side, depending on the physical design and how it is presented to the voter.

The basic measurements in the Access Board requirements are:

For a voting system that sits on a table with clear space underneath

- A table height between 27” and 34”
- Clear space for the voter’s knees and toes at least 30” wide and 25” deep
- Reach depth of less than 20” from the front of the table to the farthest control
- Reach height of less than 44” from the ground to the highest control

For a voting system that is mounted on a wall or has a solid front surface

- Reach depth of less than 10” to the farthest control
- Reach height of less than 46” to the highest control
- Reach height of more than 15” to the lowest control

If we combine these dimensions to allow for the possibility that the voting system might be placed on a counter without clear space, and to allow for a voter to position their wheelchair in either a side or front approach, the most restrictive measurements are:

- Reach depth of less than 10” to the farthest control
- Reach height of less than 44” to the highest control
- Reach height of more than 15” to the lowest control

External reference: WCAG 2.0/Section 508
Prior VVSG sources: VVSG 1.1 - 3.3.5.c, 3.3.5.1.a, 3.3.5.1.b, 3.3.5.1.c, 3.3.5.1.d

7.2-R – Control labels visible
Control labels must be placed:

1. on a surface of the voting system where voters can see them from a normal seated or standing posture, and
2. within the dimensions required in 7.2-Q – Physical Dimensions.

Discussion
This requirement ensures that voters can find controls, even if they are placed on a side or top surface of the voting system, and that blind voters can discover any Braille labels associated with the text label by touch.

Related requirements:
7.1-N – Tactile Keys
7.2-Q – Physical Dimensions
7.3-L – Icon labels
7.3 – Voters can understand all information as it is presented, including instructions, messages from the system, and error messages.

### 7.3-A – System-related errors
The voting system must help voters complete their ballots effectively, ensuring that the features of the system do not lead to voters making errors during the voting session.

Prior VVSG sources: VVSG 1.1 - 3.2.1.a, 3.2.1.b

### 7.3-B – No split contests
The voting system must have the capability to display a ballot so that no contest is split into two groups of options.

1. For paper ballot formats, the system must include a way of presenting a contest that does not divide the options across two columns or two pages.
2. For electronic interfaces, if a contest does not fit onto one screen view, the system must include a way to meet the requirements in 7.2-D-Scrolling for managing the way the list of options is displayed.

**Discussion**

There is strong evidence from recent elections that when a contest is split into two or more sections, there is a risk that the voter can perceive one contest as two (and overvote), or fail to see all of the contest options (and vote for a candidate other than the one they intend to).

This a requirement for a capability of the ballot design or election management tools for the voting system to allow election officials to lay out a ballot with good usability.

External reference: WCAG 2.0/Section 508
Prior VVSG source: VVSG 1.1 - 3.2.4.e.i
Related requirement: 7.2-D – Scrolling

### 7.3-C – Contest information
All ballots must clearly indicate the office or question title and the maximum number of choices allowed for each contest.

In an electronic ballot marking interface, the information for each contest includes, in a consistent order:
1. The title of the office or ballot question, including any distinguishing information such as the length of the term or the jurisdiction
2. The maximum number of selections allowed in the contest
3. In the audio format only, the number of options or candidates
4. If any selections have already been made, the number of selections remaining
5. In the audio format only, if any selections have been made, the currently selected candidates or options
6. Any instructions or reminders of how to find marking instructions, placed visually and in audio after the contest information

**Discussion**

This requirement is intended to work with any relevant state election laws or regulations for ballot design.

For voters using audio features, best practice is to announce how many candidates or voting options are available, providing an audio cue similar to a visual scan of the ballot in a similar way to assistive technology such as screen readers.

Placing basic instructions last helps voters using the audio format know when they can skip to making selections in the contest without missing any important information.

Prior VVSG source: VVSG 1.1 - 3.2.4.e.ii
Related requirements: 7.3-C – Maximum number of selections

**7.3-D – Consistent relationship**

The relationship between the name of a candidate or other voting option and the way the voter marks that selection, including the location on the ballot, must be consistent throughout the ballot including, all types of contests.

**Discussion**

A type of contest includes contests to:

- vote for one or more candidates,
- answer a ballot question,
- vote whether to retain a judge,
- indicate preferential ranking of candidates, or
- make a selection in other contests with distinct voting methods.
An example of how to meet this requirement is to ensure that the mechanism for marking a selection is not to the left of some candidates' names and to the right of others.

Prior VVSG source: VVSG 1.1 - 3.2.4.e.iii
Related requirements: 7.3-N – Instructions for voters
5.2-A – No bias

7.3-E – Feedback
The voting system must provide unambiguous feedback confirming the voter’s selection, such as displaying a checkmark beside the selected option or conspicuously changing its appearance.

Discussion
This requirement applies to electronic interfaces because on paper ballots the voter supplies the mark to indicate a selection, not the voting system.

This requirement also applies to the audio format. It is especially important that the way the status of the process of making selections is announced in the audio format is unambiguous. For example, the phrase “is selected” and “de-selected” can sound similar, especially at faster audio speeds. Choosing phrases that are more distinct, paying attention to the audio phrasing, and testing with the maximum audio speed can help avoid this problem.

Designers of paper ballots that include straight-party voting should test feedback features carefully to ensure that voters can understand the scope of their selection and the ballot options it affects.

Prior VVSG source: VVSG 1.1 - 3.2.6.b
Applies to: Electronic interfaces
Related requirements: 7.2-C – Voter Control
7.3-G – Full ballot selections review

7.3-F – Correcting the ballot
The voting system must provide the voter the opportunity to correct the ballot before it is cast and counted.

An electronic ballot interface must:

1. allow the voter to change a vote within a contest before advancing to the next contest,
2. provide the voter the opportunity to correct the ballot before it is cast or printed, and
3. allow the voter to make these corrections without assistance.

Discussion
For paper ballots, this can be achieved through appropriately placed written instructions, including requiring the voter to obtain a new paper ballot to correct a mistake.
Vote-by-mail ballots can have different instructions for making corrections from those cast in-person. Some voting methods allow a voter to print a replacement ballot, as long as they only cast one. Also, note the requirements for precinct-count optical scanners in 7.3-H-Overvotes below.

7.3-G – Full ballot selections review
A voting system with an electronic voting interface must provide the voter with a function to review their selections before printing or casting their ballot that:

1. displays all of the contests on the ballot with:
   - the voter’s selections for that contest, or
   - a notification that they have not made an election, or
   - a notification that they have made fewer selections than allowed, and
2. offers an opportunity to change the selections for a contest and return directly to the review screen to see the results of that change, and
3. allows the voter to continue to the function for casting the ballot without making a correction at any time in the review process.

The review function may also be provided on a scanner or other device where the voter casts a paper ballot.

Discussion
This requirement is an implementation of the HAVA requirement that voters be able to review and change their ballot before casting.

Electronic interfaces are required to prevent overvotes. This is usually done while originally marking a contest, so there are no overvoted contests to display on the review screen.

Including a review screen on a scanner that accepts ballots marked by hand gives those voters an opportunity to review how their ballot will be read by the scanner and make any corrections before casting the ballot.
7.3-H – Overvotes
The voting system must notify the voter if they attempt to select more than the allowable number of options within a contest (overvotes) and inform them of the effect of this action before the ballot is cast and counted.

1. An electronic ballot interface must prevent voters from selecting more than the allowable number of options for each contest.
2. A scanner or other device that a voter uses to cast a paper ballot must be capable of providing feedback both visually and in audio format to the voter that identifies specific contests for which the voter has overvoted.

Discussion
This requirement does not specify exactly how the system will respond when a voter attempts to select an "extra" candidate. For instance, the system can present the warning, or, in the case of a single-choice contest (vote for 1), simply change the vote selection and issue a warning.

For electronic ballot interfaces, this requirement does not allow disabling the features that prevent overvotes.

In the case of paper ballot systems, voters can be informed of the effect of overvoting through appropriately placed instructions.

In all cases, all requirements for accessibility apply to the notifications and warnings.

External reference: HAVA
Prior VVSG sources: VVSG 1.1 - 3.2.2.a, 3.2.2.1.a, 3.2.2.2.a
Related requirements: 7.2-C – Voter control
7.3-K – Warnings, alerts, and instructions
Applies to: Electronic interfaces and ballot scanners

7.3-I – Undervotes
The voting system must notify voters in both visual and audio formats of the specific contest in which they select fewer than the allowable number of options (that is, for undervotes).

1. Both electronic interfaces and scanners must allow the voter to submit an undervoted ballot without correction.
2. The voting system may allow election officials to disable the notification of undervotes on a scanner.

Discussion
For electronic interfaces, this notification can be incorporated into the review feature.

External reference: HAVA
7.3-J – Notification of casting
If the voter successfully casts or prints the ballot, the voting system must let the voter know in both visual and audio format that they succeeded.

1. If the voter takes the appropriate action to cast a ballot, but the electronic interface does not accept and record it successfully, including failure to store the ballot image, then the interface must let the voter know and provide clear instruction as to the steps the voter will take to cast the ballot.
2. If the voter takes the appropriate action to cast a ballot, but the system does not accept and record it successfully, including failure to read the ballot or to transport it into the ballot box, the system must let the voter know.
3. A scanning device must also be capable of notifying the voter that they have submitted a paper ballot that is blank on one or both sides. The system may provide a means for an authorized election official to deactivate this capability.

Discussion
The purpose of this requirement is to provide feedback to voters to assure them that the voting session has been completed. Note that either a false notification of success or a missing confirmation of actual success violates this requirement.

Detecting situations in which the voter might be unaware that the ballot is two-sided and left one side blank is distinct from the ability to detect and warn about undervoting.

At a minimum, this requirement is intended to ensure that blind and low-vision voters receive an audio notification that a ballot is successfully cast. This might be a sound that is the audio equivalent of a waving flag or other visual.

External references: WCAG 2.0/Section 508
Prior VVSG sources: VVSG 1.1 - 3.2.2.d, 3.2.2.1.f, 3.2.2.2.c, 3.2.2.2.g, 3.2.2.2.a, 3.2.2.1.b

7.3-K – Warnings, alerts, and instructions
Warning, alerts, and instructions issued by the voting system must be distinguishable from other information.

1. Warnings and alerts must clearly state in plain language:
2. Each distinct instruction must be separated from others:

- spatially in a visual presentation,
- with a noticeable pause for audio formats.

Discussion

For instance, “Do you need more time? Select ‘Yes’ or ‘No’.” rather than “System detects imminent timeout condition.” In case of an equipment failure, the only action available to the voter might be to get assistance from an election worker.

Keeping instructions separate includes not "burying" several unrelated instructions in a single long paragraph.

Alerts intended to confirm visual changes to a voter using the audio format (such as confirmation that the screen has been turned on or off) can be communicated in audio, with a short text or sound.

---

7.3-L – Icon labels

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

The only exception is that the two 3.5 mm (1/8 inch) jacks for audio and personal assistive technology (PAT) may be labeled with tactilely discernable and visually distinct icons of a headset (for audio) and wheelchair (for the PAT connector) that are at least 13 x 13 mm in size.

Discussion

While icons can be used for emphasis when communicating with the voter, they are not to be the only means by which information is conveyed, since there is no widely accepted "iconic" language, and therefore, not all voters might understand a given icon.
7.3-M – Identifying languages

When presenting a list of languages to the voter:

1. the electronic ballot interface must use the native name of each language, and
2. the controls to identify or change language must be visible on the screen, not hidden in a help or settings feature.

Discussion

The English name or spelling can also be used to identify language, along with the native name.

External reference: VRA
Prior VVSG source: VVSG 1.1 - 3.2.7.a.i
Applies to: Electronic interfaces

7.3-N – Instructions for voters

The voting system must provide voters with instructions for all its operations at any time during the voting session.

1. For electronic interfaces, the voting system must provide a way for voters to get help directly from the system.
2. For paper ballots, the system must be capable of including on the ballot both text and images with instructions for how to mark the ballot.
3. Best practice is for all voting systems to present all instructions, including the verification process, near to where they are needed during the voting session.

Discussion

The purpose of this requirement is to minimize voters’ need for assistance from an election worker and to permit the voter to cast and verify, privately and independently, the votes selected.

When the system works correctly, the voter will find the help they need from the system when and where they need it. For instance, only general instructions should be grouped at the beginning of the ballot; those pertaining to specific situations should be presented near those situations.

If an operation is available to the voter, it will be documented. Examples include how to make a vote selection, navigate among contests, cast a straight party vote, cast a write-in vote, adjust display and audio characteristics, or select a language.

Electronic ballot interface systems often provide assistance with a distinctive "help" button.

Instructions can be on the ballot itself or separate from the ballot, as long as the voter can find them easily.
7.3-O – Instructions for election workers

The voting system must include clear, complete, and detailed instructions and messages for setup, polling, shutdown, and how to use accessibility features.

1. The documentation required for normal voting system operation must be:
   - presented at a level appropriate for election workers who are not experts in voting system and computer technology, and
   - in a format suitable for use in the polling place.

2. The instructions and messages must enable the election workers to verify that the voting system
   - has been set up correctly (setup),
   - is in correct working order to record votes (polling), and
   - has been shut down correctly (shutdown).

Discussion

This requirement covers documentation for those aspects of system operation normally performed by election workers and other "non-expert" operators. It does not address inherently complex operations such as ballot definition. The instructions are usually in the form of a written manual, but can also be presented on other media, such as a DVD or videotape. In the context of this requirement, "message" means information delivered by the system to the election workers as they attempt to perform a setup, polling, or shutdown operation. For specific guidance on how to implement this requirement, please see: “NISTIR 7519: Style Guide for Voting System Documentation” at http://www.nist.gov/itl/vote/upload/NISTIR-7519.pdf.

For instance, the documentation should not presuppose familiarity with personal computers. And a single large reference manual that simply presents details of all possible operations would be difficult to use, unless accompanied by aids such as a simple "how-to" guide.

It is especially important that election workers and other non-expert workers know how to set up accessibility features which are not used frequently. This will help ensure voters who need these features can vote privately and independently.

Overall, election workers should not have to guess whether a system has been setup correctly. The documentation should make it clear what the system "looks like" when correctly configured.

Prior VVSG sources: VVSG 1.1 - 3.2.8.1.c, 3.2.8.1.c.i, 3.2.8.1.c.ii, 3.2.8.1.c.iii
Related requirement: 5.1-F – Accessibility documentation
7.3-P – Plain language

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

**Discussion**

The plain language requirements apply to instructions that are inherent to the voting system or that are generated by default. To the extent that instructions are determined by election officials designing the ballot, they are beyond the scope of this requirement.

Any legally required text is an exception to this plain language requirement.

Plain language best practices are guidelines for achieving clear communication and include:

- Using familiar, common words and avoiding technical or specialized words that voters are not likely to understand. For example, "There are more contests on the other side" rather than "Additional contests are presented on the reverse."
- Issuing instructions on the correct way to perform actions, rather than telling voters what not to do. For example, “Fill in the oval for your write-in vote to count” rather than, “If the oval is not marked, your write-in vote cannot be counted.”
- Addressing the voter directly rather than use passive voice when giving instructions. For example, "remove and retain this ballot stub" rather than "this ballot stub must be removed and retained by the voter."
- Stating a limiting condition first, followed by the action to be performed when an instruction is based on a condition. For example, use "In order to change your vote, do X", rather than "Do X, in order to change your vote."
- Avoiding the use of gender-based pronouns. For example, "Write in your candidate’s name directly on the ballot" rather than "Write in his name directly on the ballot."


Although part of general usability, using plain language is also expected to assist voters with cognitive disabilities.

Information written in plain language is easier to translate to meet language access requirements.

See the guidance paper on **Testing for Plain Language** for information on how this requirement might be tested using both automated evaluation programs and manual inspection.

**External references:** WCAG 2.0/Section 508

**Prior VVSG sources:** VVSG 1.1 - 3.2.4.c, 3.2.8.a, 3.2.4.c, 3.2.4.c.ii, 3.2.4.c.iii, 3.2.4.c.v, 3.2.4.c.vi, 3.2.4.c.vii,
Principle 8
Robust, Safe, Usable, and Accessible

The voting system and voting processes provide a robust, safe, usable, and accessible experience.

8.1 - The voting system’s hardware, software, and accessories are robust and do not expose users to harmful conditions.

8.2 - The voting system meets currently accepted federal standards for accessibility.

8.3 - The voting system is evaluated with a wide range of representative voters, including those with and without disabilities, for effectiveness, efficiency, and satisfaction.

8.4 - The voting system is evaluated for usability by election workers.
Principle 8
ROBUST, SAFE, USABLE, AND ACCESSIBLE

The voting system and voting processes provide a robust, safe, usable, and accessible experience.

This principle covers how the voting system performs in use, including physical safety and the usability and accessibility of the complete voting system. The Guidelines under Principle 8 are:

1 - **Protect from Harmful Conditions** covers requirements that ensure the voting system is Robust (completing the Web Content Accessibility Guidelines’ (WCAG’s) organizing principles known as POUR (Perceivable, Operable, Understandable, Robust)) and does not present any harmful conditions to voters and election workers. It addresses how an electronic screen displays information the voter needs and covers personal assistive technology (PAT) and topics such as audio connectors, jacks, hearing aids, and handsets.

2 - **Meet Accessibility Standards** explicitly includes the entire Federal standard for accessibility, the basis for many of the requirements in Principle 7 for voting system electronic interfaces. This standard can fill in any gaps the VVSG 2.0 does not specifically address. This is especially important for the part of the voting system that might use general interfaces, such as a browser-based ballot marking system that runs on personal computers.

3 and 4 - **Usability Tests** require usability testing the voting system to ensure that it not only meets the detailed design requirements but will function well for both voters and election workers in use. Testing with a variety of voters, including those with and without disabilities, ensures the voting system is usable and accessible to all voters. The testing with election workers ensures that the system’s setup, polling, and shutdown are relatively easy to learn, understand, and perform.

Principle 8 is related to Guideline 2.2, which requires a user-centered design and development process for the entire voting system. It covers election workers and a wide range of representative voters, including those with and without disabilities.
8.1 – The voting system’s hardware, software, and accessories are robust and do not expose users to harmful conditions.

8.1-A – Electronic display screens

If the voting system uses an electronic display screen as the primary visual interface for the voter, the display must have the following characteristics:

1. Minimum display brightness: 130 cd/m²
2. Minimum display darkroom 7×7 checkerboard contrast: 150:1
3. Minimum display pixel pitch: 85 pixels/inch (0.3 mm/pixel)
4. Minimum display area: 700 cm²
5. Antiglare screen surface that shows no distinct virtual image of a light source
6. Minimum uniform diffuse ambient contrast ratio for 500 lx illuminance: 10:1

Discussion

Two EAC Requests for Interpretation offered exceptions to the requirements for Display Pixel Pitch and Minimal Display Area:

The EAC Decision on Request for Interpretation 2016-01 (Display Pixel Pitch) created an exception to this requirement based on usability testing: “...larger screens that can be shown to provide acceptable usability and accessibility will not be strictly held to the 85 pixels/inch requirement if the product has undergone thorough usability testing and the submitted usability test reports demonstrate good usability and accessibility performance (in particular, works for low literacy, low vision, and dexterity).” They based this on “...a scenario in which content that meets all usability and accessibility requirements on a 24-inch 1080p resolution screen could not meet the standard if displayed on a 1080p 32-inch screen, even though the content is larger.” The discussion also noted that commercial products for very large screens that can meet the display pixel pitch requirement may not be available or might be prohibitively expensive.

The EAC Decision on Request for Interpretation 2015-04 (Visual Display Characteristics; Minimal display area) reviewed the requirements for screen sizes and concluded that “It is both reasonable and desirable that a voting machine ballot display should meet the 700cm² display area requirement.”

This Request for Information (RFI) also offered an exception for smaller screens by requiring usability evidence that they meet good usability and accessibility.

“If the minimum display area is smaller than 700 cm², the burden of proof of the usability and accessibility of a smaller display is on the manufacturer. This implies that the product has undergone thorough usability testing and the submitted usability test reports demonstrate good usability and accessibility performance (in particular, works for low literacy, low vision, and dexterity). In these
cases, EAC will have the reports evaluated by usability/human factors experts to confirm the findings in the manufacturer submitted usability test report(s).”

The table below calculates the display area for some popular monitor sizes, highlighting the ones that meet the 700 cm² requirement.

### Display Sizes of Select Monitors (width, height, and area numbers rounded)

<table>
<thead>
<tr>
<th>Diagonal (in)</th>
<th>Diagonal (cm)</th>
<th>5:4 Aspect Ratio Width (cm)</th>
<th>5:4 Aspect Ratio Height (cm)</th>
<th>5:4 Aspect Ratio Area (cm)</th>
<th>4:3 Aspect Ratio Width (cm)</th>
<th>4:3 Aspect Ratio Height (cm)</th>
<th>4:3 Aspect Ratio Area (cm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.6</td>
<td>29</td>
<td>23</td>
<td>18</td>
<td>423</td>
<td>24</td>
<td>18</td>
<td>417</td>
</tr>
<tr>
<td>13.3</td>
<td>34</td>
<td>26</td>
<td>21</td>
<td>557</td>
<td>27</td>
<td>20</td>
<td>548</td>
</tr>
<tr>
<td>14</td>
<td>36</td>
<td>28</td>
<td>22</td>
<td>617</td>
<td>28</td>
<td>21</td>
<td>607</td>
</tr>
<tr>
<td><strong>15</strong></td>
<td><strong>38</strong></td>
<td><strong>30</strong></td>
<td><strong>24</strong></td>
<td><strong>708</strong></td>
<td><strong>30</strong></td>
<td><strong>23</strong></td>
<td><strong>697</strong></td>
</tr>
<tr>
<td><strong>15.4</strong></td>
<td><strong>39</strong></td>
<td><strong>31</strong></td>
<td><strong>24</strong></td>
<td><strong>746</strong></td>
<td><strong>31</strong></td>
<td><strong>23</strong></td>
<td><strong>734</strong></td>
</tr>
<tr>
<td><strong>17</strong></td>
<td><strong>43</strong></td>
<td><strong>34</strong></td>
<td><strong>27</strong></td>
<td><strong>910</strong></td>
<td><strong>35</strong></td>
<td><strong>26</strong></td>
<td><strong>895</strong></td>
</tr>
</tbody>
</table>

External references:  
EAC Decision on Request for Interpretation 2016-01  
(Visual Display Characteristics; Minimal display area)

Prior VVSG sources:  
VVSG 1.1 - 3.2.5.a.i, 3.2.5.a.ii, 3.2.5.a.iii, 3.2.5.a.iv, 3.2.5.a.v, 3.2.5.a.vi, 3.2.5.a.vii

Applies to:  
Electronic interfaces

### 8.1-B – Flashing

If the voting system emits lights in flashes, there must be no more than three flashes in any one-second period.

#### Discussion

This requirement has been updated to meet WCAG 2.0 and Section 508 software design issue standards, see:

- WCAG 2.0 requirements for flickering and flashing
- Section 508 requirements for flicker and flash

External references:  
WCAG 2.0/Section 508

Prior VVSG sources:  
VVSG 1.1 - 3.2.5.a.i

Applies to:  
Electronic interfaces
8.1-C – Personal Assistive Technology (PAT)
The support provided to voters with disabilities must be intrinsic to the voting system. This means a voter’s personal assistive devices will not be necessary to operate the voting system correctly. This does not apply to personal assistive technology required to comply with 5.1-A.

Discussion
This requirement does not preclude the voting system from providing interfaces to assistive technology. (See definition of "personal assistive devices" in the Glossary). Its purpose is to ensure that voters are not required to bring special devices with them in order to vote successfully.

This requirement assumes that voters will have with them any personal headsets, hearing aids, eyeglasses, canes, or other assistive devices they customarily use.

See the White Paper: Assistive Technology in the Polling Place: Current and emerging technology, Dec. 28, 2016

External references: WCAG 2.0/Section 508
Prior VVSG source: VVSG 1.1 - 3.3.1.c

8.1-D – Secondary ID and biometrics
If a voting system uses biometric measures for identifying or authenticating voters and election workers, it must provide an alternative that does not depend on the same biometric capabilities.

Discussion
For example, if fingerprints are used for voter identification, another mechanism will be provided for voters without usable fingerprints.

External references: WCAG 2.0/Section 508
Prior VVSG source: VVSG 1.1 - 3.3.1.d

8.1-E – Standard audio connectors
The voting system must provide its audio signal through an industry standard connector using a 3.5 mm (1/8 inch) stereo headphone jack to allow voters to use their own audio assistive devices for private listening.

External references: WCAG 2.0/Section 508
Prior VVSG source: VVSG 1.1 - 3.3.3.c.i
Applies to: Electronic interfaces
8.1-F – Discernable audio jacks

The audio jack must be in a location that voters can easily discover, discernable by touch while sitting or standing in front of the unit, and not located near a sharp edge.

**Discussion**

For example, if the jack is slightly recessed with a round bezel, it will be easier for voters to identify the jack and to insert the headset plug into it.

8.1-G – Telephone style handset

If the voting system uses a telephone style handset or headphone to provide audio information, it must provide a wireless T-Coil 9 coupling for assistive hearing devices so it provides access to that information for voters with partial hearing, achieving at least a category T4 rating as defined by the American National Standard Institute (ANSI) for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19 [ANSI11].

**External references:** WCAG 2.0/Section 508
ANSI C63.19

**Prior VVSG source:** VVSG 1.1 - 3.3.3.c.ii

**Related requirement:** 8.1-J – Hearing aids
6.1.2 – Audio privacy

8.1-H – Sanitized headphones

A sanitized headphone or handset must be made available to each voter.

**Discussion**

This requirement can be achieved in various ways, including the use of "throwaway" headphones or sanitary coverings.

**Prior VVSG source:** VVSG 1.1 - 3.3.3.c.iii

8.1-I – Standard PAT jacks

The voting system must provide a 3.5 mm (1/8 inch) industry standard jack voters can use to connect their personal assistive technology switch to the system.

1. This jack must allow only switch data to be transmitted to the system.
2. The system must accept switch input that is functionally equivalent to other input methods.
3. All the functionality of the voting system must be available through technology using this input mechanism.
Discussion

This requirement ensures that the voting systems are operable by voters with limited dexterity who do not have the use of their hands. Examples of personal assistive technology switches include dual switches and "sip and puff" devices.

Ideally, the jack will be on the tactile keypad or have some other mechanism to provide sufficient reach to a wheelchair tray or the voter’s lap.

While it is desirable that the voter be able to independently initiate use of the non-manual input mechanism, this requirement guarantees only that the voter can vote independently once the mechanism is enabled.

External references: WCAG 2.0/Section 508
Prior VVSG source: VVSG 1.1 - 3.3.4.a

8.1-J – Hearing aids

Voters who use assistive hearing devices must be able to use voting devices as intended:

1. The voting device must not cause electromagnetic interference with assistive hearing devices that would substantially degrade the performance of those devices.

2. The voting device, measured as if it were a wireless device, must achieve at least a category T4 rating as defined by American National Standard [ANSI11] for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19 [ANSI11].

Discussion

"Hearing devices" include hearing aids and cochlear implants.

External references: WCAG 2.0/Section 508
ANSI C63.19
Prior VVSG source: VVSG 1.1 - 3.3.6.c
Related requirement: 8.1-G – Telephone style handset

8.1-K – Eliminating hazards

Devices associated with the voting system must be certified in accordance with the requirements of UL 60950-1 [UL07], Information Technology Equipment – Safety – Part 1 by a certification organization accredited by the Department of Labor, Occupational Safety and Health Administration’s Nationally Recognized Testing Laboratory program.

The certification organization’s scope of accreditation is acceptable if it includes IEC/UL 60950-1 [UL07].
Discussion

IEC/UL 60950 is a comprehensive standard for IT equipment and addresses all the hazards discussed above under Safety.

External references: IEC/UL 60950-1
Prior VVSG sources: VVSG 1.1 - 3.2.8.2.a, 3.2.8.2.b
8.2 – The voting system meets currently accepted federal standards for accessibility.

8.2-A – Federal standards for accessibility
Voting systems must meet federal standards for accessibility, including the current version of Section 508 of the Rehabilitation Act, in effect as of January 18, 2018, and the WCAG 2.0 Level AA checkpoints included in that standard.

Discussion
The Section 508 Standards apply to electronic and information technology, including computer hardware and software, websites, multimedia, and other technology such as video, phone systems, and copiers. The final rule was published in the Federal Register on January 18, 2017 as 36 CFR Parts 1193 and 1194 (RIN 3014-AA37) and can be found on the Access Board website: https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule

External references: WCAG 2.0/Section 508 and ADA
Applies to: Electronic interfaces
8.3 – The voting system is evaluated with a wide range of representative voters, including those with and without disabilities, for effectiveness, efficiency, and satisfaction.

8.3-A – Usability tests with voters

The manufacturer must conduct usability tests on the voting system, including all voter activities in a voter session from ballot activation to verification and casting.

1. The test participants must include voters who represent the following:
   o General population, using the visual interface
   o Voters who speak all supported languages as their primary language
   o Blind voters, using the audio format plus tactile controls
   o Voters with low vision, using the enhanced visual features with or without audio
   o Voters with limited dexterity, using the visual-tactile interface

2. The manufacturer must submit a report of the results of their usability tests as part of the Technical Data Package (TDP) using the version of the Common Industry Format modified for voting systems (CIF-for-Voting Systems).

Discussion

Voting system developers are required to conduct realistic usability tests on their product before submitting the system to conformance testing. This is to ensure that the user-centered design process required for quality implementation has produced a usable and accessible voting system.

Prior VVSG sources; Related requirements: VVSG 1.1 - 3.3.3.a, 3.3.3.a.i, 3.3.10.a-c, 3.2.7.a.iv
      5.1-D – Accessibility features
      2.2-A – User-centered design process
8.4 – The voting system is evaluated for usability by election workers.

8.4-A – Usability tests with election workers

Voting system setup, polling, and shutdown, as documented by the manufacturer, must be reasonably easy for the typical election worker to learn, understand, and perform.

1. The manufacturer must conduct usability tests on the voting system using individuals who are representative of election workers and report the test results as part of the Technical Data Package, using the Common Industry Format.

2. The tasks to be covered in the test must include:
   o Setup and opening for voting
   o Operation during voting
   o Use of assistive technology or language options that are part of the voting system
   o Shutdown at the end of a voting day during a multi-day early voting period, if supported by the voting system
   o Shutdown at the end of voting including running any reports

Discussion

This requirement covers procedures and operations for those aspects of system operation normally performed by election workers and other "non-expert" operators. It does not address inherently complex operations such as ballot definition or system repair. These "normal" procedures should not require any special expertise. The procedures may require a reasonable amount of training, similar to the training generally provided for temporary election workers.

To ensure that the needs of voters with disabilities and who use language options are included in the testing, scenarios for election workers include scenarios for:

- providing ballots in different languages
- selecting the correct ballot type (for example, for vote centers)
- setting up the voting system to use different interaction methods

Prior VVSG sources: VVSG 1.1 - 3.2.8.1.a, 3.2.8.1.b, 3.2.8.1.b.i
Related requirement: 7.3-N – Instructions for election workers
2.2-A – User-centered design process
Principle 9
Auditable

The voting system is auditable and enables evidence-based elections.

9.1 - An error or fault in the voting system software or hardware cannot cause an undetectable change in election results.

9.2 - The voting system produces readily available records that provide the ability to check whether the election outcome is correct and, to the extent possible, identify the root cause of any irregularities.

9.3 - Voting system records are resilient in the presence of intentional forms of tampering and accidental errors.

9.4 - The voting system supports efficient audits.
**Principle 9**

**AUDITABLE**

The voting system is auditable and enables evidence-based elections.

The requirements for Principle 9 include ensuring that an error in the voting system cannot cause an undetectable change in the election results, that the system produces records that are resilient and can be checked, and produces records that enable an efficient compliance audit.

**The sections in Guideline 9.1 cover:**

1. **Software independence** requires that the voting system provide proof that the ballots have been recorded correctly and are compliant within the Paper-based System Architecture or Cryptographic E2E System Architectures. In addition, the manufacturer documents the mechanism used to provide software independence.

2. **Tamper-evident records** are needed to enable detection of incorrect election outcomes. They need to capture the voter’s ballot selection when each ballot is cast.

3. **Voter verification records** need to allow voters the opportunity to verify that the system correctly interpreted their ballot selections and that they can identify errors and restart a voting session if a ballot is unacceptable.

4. **Auditable** means the voting system generates records that enable external auditors to verify that ballots are correctly tabulated, even if the system is compromised or there are faults in components. The manufacturer is to provide a procedure to verify that cast records are correctly tabulated.

5. **Paper records** covers the requirement that the voting system produce a verifiable paper record of the voter’s ballot selection and retain a copy of that selection which has a unique identifier. The voter needs to be able to understand the recorded ballot selection and it needs to agree with the selections made by the voter.

6. **E2E cryptography** deals with the protocol used in the voting system, requiring that it be publicly available for review for 2 years before it enters the voting system. Individuals will get a receipt and be able to confirm that the system correctly interpreted their ballot selections. Voters will also be able to verify that their ballots are included in the tabulation results.

7. **Audit support** deals with the requirement that the system manufacturer documents the procedure to determine the number of ballots to be checked to reach an election-official-specified margin of error for a given contest, including the possible use of random numbers.

**In 9.2 – Audit procedures** deals with the need to produce readily available records so the election outcomes can be checked for correctness, and also help identify the cause of any
irregularities. Problems need to be identified in a post-election audit both during the audit and when completed. The voting systems needs to count and report the number of ballots cast.

**In 9.3 - Resilient records** covers the data protection requirements necessary to ensure that voting system records are resilient in the presence of both intentional forms of tampering and accidental errors.

**In 9.4 - Efficient audit** describes the system that will produce the records that assist election officials in conducting compliance audits.
9.1 - An error or fault in the voting system software or hardware cannot cause an undetectable change in election results.

9.1.1 – Software independence

9.1.1-A – Software independent
The voting system must be software independent.

Discussion
Software independence means that an undetected error or fault in the voting system’s software is not capable of causing an undetectable change in election results. All voting systems need to be software independent in order to conform to the VVSG.

There are two essential concepts behind applying software independence:

- it is be possible to audit voting systems to verify that ballots are being recorded correctly, and
- testing software is so difficult that audits of voting system correctness cannot rely on the software itself being correct.

Therefore, voting systems need to be ‘software independent’ so that the audits do not have to trust that the voting system’s software is correct. The voting system will provide proof that the ballots have been recorded correctly, that is, voting records will be produced in ways in which their accuracy does not rely on the correctness of the voting system’s software.

This is a major change from previous versions of the VVSG, because previous versions permitted voting systems that are software dependent, that is, voting systems whose audits rely on the correctness of the software. One example of a software dependent voting system is the DRE, which is now non-conformant to this version of the VVSG.

There are currently two methods specified in the VVSG for achieving independence:

- through the use of independent voter-verifiable paper records, and
- E2E cryptographic voting systems.

Prior VVSG source: 2007 VVSG 2.7-A

9.1.1-B – Paper-based or cryptographic E2E system
Voting systems must meet the requirements within the Paper-based System Architectures or Cryptographic E2E System Architectures section, or both.

Discussion
Both of these architectures are software independent, but they can both be used within the same voting system. In this case, the system would need to be compliant with both sets of requirements.

9.1.1-C – Mechanism documentation
A voting system manufacturer must document the mechanism used to provide software independence.

Discussion
Without knowing the specific mechanism, it is difficult to determine if the system truly is software independent.

9.1.2 – Tamper evidence

9.1.2-A – Tamper evident records
The voting system must produce tamper-evident records that enable detection of incorrect election outcomes, including:

1. capturing the contents of each vote at the time of each ballot’s casting, and
2. recording detected errors in a tamper-evident manner.

Discussion
Tamper-evident records include paper ballots and artifacts from an E2E voting system.

The record also ensures that identified issues and other problems cannot be lost or unintentionally modified once they are discovered.

Applies to: Voting Device

9.1.2-B – Tamper-evident record creation
A tamper-evident record of the voter’s ballot selections must be captured when each ballot is cast.

Discussion
Precinct-based voting systems are the only way to meet this requirement. Entirely separate voting channels, such as remote vote-by-mail, do not offer this opportunity to the voter.

Applies to: Precinct-based voting systems
9.1.3 – Voter verification

9.1.3-A – Records for voter verification
The voting system must provide individual voters the opportunity to verify that the voting system correctly interpreted their ballot selections.

Discussion
Precinct-based voting systems are the only way to meet this requirement. Entirely separate voting channels, such as remote postal voting, do not offer this opportunity to the voter.

Applies to: Vote Capture Devices

9.1.3-B – Identification of errors
The voting system must offer voters the opportunity to identify ballot errors before it is cast.

Applies to: Paper-based system architectures

Cryptographic E2E system architectures

9.1.3-C – Ballot error correction
The voting system must allow a voter to restart a voting session if a ballot is deemed unacceptable.

Applies to: Paper-based system architectures

9.1.3-D – Voter reported errors
Voting system documentation must describe a method, either through procedural or technical means, for voters to report detected errors or incorrect results.

Discussion
This can include a voter alerting an election worker or pressing a button on the machine to report detected errors or incorrect results.

9.1.4 – Auditable

9.1.4-A – Auditor verification
Voting systems must generate records that would enable external auditors to verify that cast ballots were correctly tabulated.

Discussion
The voting systems themselves cannot make records available to the public. The manner and decision to make these records available is made by a state and or local jurisdiction. This requirement only ensures that the records themselves are generated and can be easily accessed without additional software or assistance from the voting system manufacturer. This requirement is meant to enable external auditors to perform their own count of the election results.

Applies to: Voting Device  
Related Requirements: Principle 1 – High Quality Design

**9.1.4-B – Auditable with compromised software, firmware, or hardware**

The voting system must enable a meaningful audit in the presence of:

1. compromised or malicious software resident on the system
2. compromised or malicious hardware components
3. faults or errors in software components
4. faults or errors in hardware components

**Discussion**

The production of tamper evidence records protects against this scenario.

**9.1.4-C – Documented procedure**

The voting system manufacturer must provide a documented procedure to verify that cast ballots were correctly tabulated.

**Discussion**

This documentation includes procedures and technical practices that verify the results post-election.

**9.1.5 – Paper records**

**9.1.5-A – Paper record production**

The voting system must produce an independently verifiable paper record of the voter’s ballot selections.

**Discussion**

Voting systems that use independent voter-verifiable records can satisfy the software independence requirement and achieve conformance to the VVSG.

Applies to: Paper-based system architectures
9.1.5-B – Paper record retention
The voting system must retain a paper record of the voter’s ballot selections.

Applies to: Paper-based system architectures

9.1.5-C – Paper record intelligibility
The recorded ballot selection must be presented in a way the voter can understand.

Applies to: Paper-based system architectures

9.1.5-D – Matching selections
All representations of a voter’s ballot selections produced by the voting system must agree with the selections made by the voter.

Applies to: Paper-based system architectures

9.1.5-E – Paper record transparency and interoperability
All representations of a voter’s ballot selections must use an open and interoperable format.

Applies to: Paper-based system architectures

9.1.5-F – Unique identifier
Each paper ballot that is counted may contain a unique identifier, which can be printed on the ballot or affixed by some other external mechanism.

Discussion
Voting systems are not required to affix a unique identifier to ballots, but all voting systems that are certified with risk-limiting audit (RLA) capabilities need to be able to affix a ballot identifier.

Applies to: Paper-based system architectures
Related requirements: 9.4-B – Efficient risk limiting audit

9.1.6 – E2E Cryptography

9.1.6-A – Cryptographic E2E transparency
The cryptographic E2E protocol used in the voting system must be publicly available, without an explicit request, for open review for 2 years before it enters the voting system certification process.

Applies to: Cryptographic E2E system architectures
9.1.6-B – Cryptographic verification
Individual voters must have the opportunity to confirm that the voting system correctly interpreted their ballot selections.

Applies to: Cryptographic E2E system architectures

9.1.6-C – Ballot receipt
After casting, the voter must receive a receipt that allows them to verify that their ballot has been correctly recorded and tallied by the system. These receipts

1. do not display any ballot selections made by the voter
2. do not enable the voter to prove their selections on the cast ballot to others
3. are represented in an open and interoperable format
4. contain a unique identifier

Applies to: Cryptographic E2E system architectures
Related Requirements: Principle 10 - Ballot Secrecy
Principle 4 - Interoperable

9.1.6-D – Receipt export
The voting system must be capable of exporting receipt batches in an open format.

Discussion
Voting systems are not required to affix a unique identifier to ballots, but all voting systems that are certified with risk-limiting audit (RLA) capabilities need to be able to affix a ballot identifier.

Applies to: Cryptographic E2E system architectures
Related Requirements: Principle 10 - Transparency

9.1.6-E – Mandatory ballot availability
The voting system must make available all encoded ballots for public posting.

Applies to: Cryptographic E2E system architectures

9.1.6-F – Verification of encoded votes
Voters must have the opportunity to verify that their ballots are included within the tabulation results.
9.1.6-G – Sufficient information for verification
The receipt must provide sufficient information for voters to verify that their cast ballots are uniquely contained within the publicly available list of encoded ballots.

9.1.7 – Audit support

9.1.7-A – Number of ballots to check
A voting system manufacturer must document the procedure to determine the number of ballots which need to be checked to reach an election-official-specified margin of error for a given contest.

Discussion
To ensure that the election outcome is correct within a specified margin of error, a minimum number of ballots will be checked. This can be performing with paper records in paper-based system architectures which are checked by election officials or checks by voters in cryptographic E2E system architectures. This is important to understanding how efficient the system is at detecting changes due to an error or fault.

9.1.7-B – No fixed margin of error
The voting system must allow election officials to determine the margin of error used to determine the number of ballots to check.

Discussion
This requires the documentation of the margins to be specified as an equation rather than having specific margins built into the system. Additional inputs such as margin of victory, total number of voters, number of voters for each candidate, actual ballots, or an audit trail, may be needed to determine the number of ballots needed.

9.1.7-C – Random number generation
If a voting system generates random or pseudo-random numbers, the manufacturer must document the method used to obtain the numbers and how the random numbers are used within the voting system.

Discussion
Various systems used to implement software independence require random numbers, whether for ballot selection for audits or cryptographic purposes.

The most important reason for this requirement is to ensure that cryptographic protocols requiring random numbers use a true random number generator (TRNG) or a cryptographically secure pseudo-random number generator (CSPRNG) as required. For additional information, see NIST SP 800-90A Rev 1 - Recommendation for Random Number Generation Using Deterministic Random Bit Generators.

External reference

NIST SP 800-90A Rev 1
9.2 - The voting system produces readily available records that provide the ability to check whether the election outcome is correct and, to the extent possible, identify the root cause of any irregularities.

9.2-A – Compliance audit procedures
The voting system documentation must specify the election procedures necessary to perform a compliance audit.

Discussion
A compliance audit ensures that the election audit trail is sufficiently accurate to reconstruct the outcome according to how voters cast their ballots. Compliance audits provide assurance that a full hand count of the election audit trail shows the outcome according to how the voters really voted.

External references: Evidence-Based Elections by P.B. Stark and D.A. Wagner
Related requirements: 3.1.3-D – Audit Procedures

9.2-B – General post-election audit procedures
The voting system documentation must specify the election procedures necessary to perform a post-election audit.

9.2-C – Generating CVRs
The voting system must be capable of recording and reporting a cast vote record for each ballot.

9.2-D – Reporting intermediate results
The voting system must be able to report intermediate results as the audit is being conducted.

9.2-E – Reporting unusual audit events
The voting system must be capable of reporting problems as they arise (for example, matching failures).

9.2-F – Reporting format
The voting system manufacturer must document the intermediate and final election audit results in an open format.
9.2-G – Ballot count
Voting systems must count and report the number of ballots cast.

Discussion
This needs to be granular enough to have voting devices and tabulators count and report the number of ballots cast.
9.3 - Voting system records are resilient in the presence of intentional forms of tampering and accidental errors.

9.3-A – Data protection requirements for audit records
All voting systems must meet the requirements listed under Principles 13.1 and 13.2

Related requirements 13.1 and 13.2
9.4 - The voting system supports efficient audits.

9.4-A – Efficient compliance audit
The voting system must produce records to enable an efficient compliance audit.

Discussion
Voting systems need to provide information that will assist election officials in conducting compliance audits, whenever possible. While compliance audits check that procedures are followed, voting systems can provide information that aids in conducting this audit. For example, inspection of event logs is much more efficient if the logs are available in human readable text format. Using event codes in logs, which requires manual decoding, is an example of a record which impairs the efficiency of compliance audits.

9.4-B – Efficient risk-limiting audit
A voting system must produce paper records that allow election officials to conduct an efficient risk-limiting audit.

Discussion
Voting systems contain information which enables election officials to conduct efficient risk limiting audits. For example, by providing a human readable ballot manifest, the voting system makes the process of ballot sampling more efficient.

Applies to: Optical scanners, BMDs

9.4-C – Unique ballot identifiers
The voting system must enable election auditors to uniquely address individual ballots.

Discussion
This capability is needed to support RLAs.

Applies to: Auditing system

9.4-D – Multipage ballots
The voting system must be able to appropriately manage multipage ballots during an audit.

Applies to: Auditing system
Principle 10
Ballot Secrecy

The voting system protects the secrecy of voters’ ballot selections.

10.1 - Ballot secrecy is maintained throughout the voting process.

10.2 - The voting system does not contain nor produce records, notifications, information about the voter or other election artifacts that can be used to associate the voter’s identity with the voter’s intent, choices, or selections.
Principle 10
Ballot Secrecy
The voting system protects the secrecy of voters’ ballot selections.

The requirements for Principle 10 include ensuring ballot secrecy and ensuring that nothing is produced that would associate the voter’s identity with their votes. A related topic, Principle 6: Voter Privacy, covers voter privacy during voting.

10.1 - Use of voter information covers the requirement that ballot secrecy is maintained throughout the voting process.

10.2 - No association of the voter’s choices with the voter’s identity. The sections in Guideline 10.2 cover:

1 – Voter associations requires that there be no direct or indirect association between the voter’s identity and their ballot, with the exception of certain instances when used in end-to-end (E2E) voting systems. It covers how election workers can select the indirect association option and how these ballots are to be stored separately from cast ballots. It also requires encryption of ballots not cast that contain an indirect association.

2 – Identification in vote records covers the use of identifiers for tying CVRs and ballot images to paper ballots and the need for them to be distinct from identifiers used for indirect associations. The voting system cannot allow for any information that could be used to determine the order in which votes are cast or include any information identifying a voter. Aggregate and final totals also will not allow identification of a voter.

3 – Access to cast vote records covers the need to limit information about and access to the storage location for CVRs, ballot images and ballot selections. Any such access needs to be authorized and logged in.

4 – Voter information in other devices and artifacts explains that receipts produced by a voting system cannot contain voter information. At the same time, the voting system needs to ensure ballot secrecy for any receipts it does issue. No part of the audit trail can contain individual or aggregate selections and nor can activation devices create or retain information that can be used to identify a voter’s ballot.
**10.1 - Ballot secrecy is maintained throughout the voting process.**

**10.1-A – System use of voter information**

The voting system must be incapable of accepting, processing, storing, and reporting identifying information about a specific voter, with the exception of blank ballot distribution and online ballot marking systems.

**Discussion**

Examples include first name, last name, address, driver’s license, and voter registration number. The voting system cannot prevent a voter from self-identifying within write-in fields.
10.2 - The voting system does not contain nor produce records, notifications, information about the voter, or other election artifacts that can be used to associate the voter’s identity with the voter’s intent, choices, or selections.

10.2.1 – Voter associations

10.2.1-A – Direct voter associations
The voting system must not create or store direct associations between a voter’s identity and their ballot.

Discussion
A direct voter association would be the voting system storing that John Smith voted for George Washington. Other examples of a direct association would include tying ballot selections to a social security number, voter identification number, or driver’s license number. (This is not an exhaustive list of direct voter association examples.)

10.2.1-B – Indirect voter associations
Only paperless systems may use indirect associations; other systems must not.

Discussion
Certain channels of voting require indirect associations so that ballots can be removed before the ballot is read and counted. Some reasons include signature mismatch or death of a voter. Once a ballot is read and counted, the ballot is permanently stripped of its identifier. The most common example of indirect association would be a randomly generated number. Ballots with indirect associations are not considered read or counted until the association is removed.

This requirement only applies to paperless voting systems that also meet the requirements under guideline 9.1, which state that the voting system must be software independent. During the writing of these requirements, cryptographic E2E verifiable voting systems are a potential paperless and software independent system that could be applicable for this requirement.

Applies to: E2E voting system architectures

10.2.1-C – Use of indirect voter associations
The voting system must only use indirect associations for situations when a voter needs to fill out a ballot before their eligibility is determined.
**Discussion**

Certain channels of voting require indirect associations so that ballots can be removed before casting for a variety of reasons including signature mismatch or death of a voter. The act of casting the ballot permanently strips it of an identifier.

The most common example of indirect association would be a randomly generated number. Ballots with indirect associations are not considered cast until the association is removed. Best practice would ensure that indirect voter associations are only available to authorized election personnel.

**Applies to:** E2E voting system architectures

10.2.1-D – Election worker selection of indirect associations

When the use of an indirect association is needed, an election worker must select the option for using an indirect association at the beginning of each new voting session.

**Applies to:** E2E voting system architectures

10.2.1-E – Isolated storage location

Ballots that are not cast and contain an indirect association must be stored in separate storage locations from cast ballots.

**Discussion**

Ballots that contain an indirect association are not considered cast. Cast ballots and ballots having their eligibility considered need to be kept separate from each other. Although not the only way of meeting this requirement, one example would be storing cast ballots in a different directory from ballots not yet cast.

**Applies to:** E2E voting system architectures

10.2.1-F – Confidentiality for indirect association

Ballots that are not cast and contain an indirect association must be encrypted.

**Discussion**

Encryption of the ballot preserves the confidentiality of the voter’s ballot selections while the ballot is tied to an indirect association to the voter.

**Applies to:** E2E voting system architectures

**Related requirements:** Data Protection
10.2.2 – Identification in vote records

10.2.2-A – Identifiers used for audits
Identifiers used for tying a cast vote record (CVR) and ballot images to physical paper ballots must be distinct from identifiers used for indirect associations.

Discussion
For the purpose of these requirements, associations between physical ballots and CVRs are not considered direct or indirect identifiers.

Related requirements: Auditability

10.2.2-B – No voter record order information
The voting system must not contain data or metadata associated with the CVR and ballot image files that can be used to determine the order in which votes are cast.

10.2.2-C – Identifying information in voter record file names
CVR and ballot image file names must not include any information identifying a voter.

Discussion
This helps to ensure that information that could accidentally be used to reference a voter is not used within a file name.

10.2.2-D – Non-memorable identifiers and associations
Unique identifiers and associations must not be displayed in a way that is easily remembered by the voter.

Discussion
Unique identifiers on the paper record are displayed or formatted in such a way that they are not easily remembered by voters, such as by obscuring them in other characters.

Related requirements: 9.4 Efficiency

10.2.2-E – Aggregating and ordering
Aggregated and final totals:

1. must not contain voter specific information, and
2. must not be able to recreate the order in which the ballots were cast.
10.2.3 – Access to cast vote records (CVR)

10.2.3-A – Least privilege access to store
The directory or storage location of CVRs, ballot images, and ballot selections on the voting system must be subject to the principle of least privilege.

**Discussion**

NIST SP 800-12 defines “least privilege” as, “The security objective of granting users only those accesses they need to perform their official duties.”
Nieles, Dempsey, and Pilliteri, *Special Publication (SP) 800-12 Revision 1, An Introduction to Information Security*, National Institute of Standards & Technology (NIST), Gaithersburg, Maryland, June, 2017.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

**External references:** NIS SP800-12 Revision 1
**Related requirements:** Access Control

10.2.3-B – Limited access
Permission to access the directory or storage location for CVRs, ballot images, and ballot selections must be assigned to as few entities as possible.

**Discussion**

Entities include people and applications or processes running on the voting system.

**Related requirements:** Access Control

10.2.3-C – Authorized access
Permissions to access the directory or storage location for CVRs, ballot images, and ballot selections must be validated and explicitly authorized before access is given.

**Discussion**

Modern operating systems often have sufficient mechanisms in place to accomplish this, but these security capabilities need to be configured and enforced.

**Related requirements:** Access Control
10.2.3-D – Digital voter record access log
The voting system must log all access to the directory or storage location for CVRs, ballot images, and ballot selections in addition to logging access to all actions occurring within the system.

**Discussion**
This ensures that any person, process, or other entity reading, writing, or performing other actions to the electronic audit trail is properly logged.

*Related requirements*  
Access Control, Auditing

10.2.4 – Voter information in other devices and artifacts

10.2.4-A – Voting information in receipts
Receipts produced by a voting system must not contain voter information.

10.2.4-B – Ballot secrecy for receipts
The voting system must not issue a receipt to the voter that would provide proof to another of how the voter voted.

*Applies to:*  
E2E voting system architectures

*Prior VVSG source:*  
2007 Vol 1: 3.2.3.1-A.4

10.2.4-C – Logging of ballot selections
Logs and other portions of the audit trail must not contain individual or aggregate ballot selections.

**Discussion**

The voting system needs to be constructed so that the security of the system does not rely upon the secrecy of the event logs. It will be considered routine for event logs to be made available to election officials, and possibly even to the public, if election officials so desire. The system will be designed to permit the election officials to access event logs without fear of negative consequences to the security and integrity of the election. For example, cryptographic secret keys or passwords will not be logged in event log records.
10.2.4-D – Activation device records

Activation devices must not create or retain information that can be used to identify a voter’s ballot, including the order and time at which a voter uses the voting system.

Discussion

Information such as the time the voter arrived at the polls or the specific vote-capture device used by the voter may be used to link a voter with their specific ballot and violates the principle of ballot secrecy.
Principle 11
Access Control

The voting system authenticates administrators, users, devices, and services before granting access to sensitive functions.

11.1 - The voting system enables logging, monitoring, reviewing, and modifying of access privileges, accounts, activities, and authorizations.

11.2 - The voting system limits the access of users, roles, and processes to the specific functions and data to which each entity holds authorized access.

11.3 - The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations.

11.4 - The voting system’s default access control policies enforce the principles of least privilege and separation of duties.

11.5 - Logical access to voting system assets are revoked when no longer required.
Principle 11
Access Control

The voting system authenticates administrators, users, devices, and services before granting access to sensitive functions.

The requirements for Principle 11 covers how the voting system secures and limits access to only those who are authorized.

11.1 – Access privileges, accounts, activities and authorizations are logged, monitored, and reviewed and modified as needed ensures there are records in case there are errors or incidents that need to be accounted for. The system also prevents logging any voter ID information and prevents the logging capability from becoming disabled or the log entries from being modified. The system provides administrators access to logs, allowing for continuous monitoring and periodic review.

11.2 – Voting system limits the access of users and processes to the specific functions and data to which each entity holds authorized access

1 – Authorized access ensures that only authorized users can access the voting system, and only administrators can create or modify authorized users, configure permissions and create or assign groups or roles. Control mechanisms distinguish at least four voting stages: Pre-voting, activated, suspended, and post-voting.

2 – Role-based access control standard relates to the requirement that voting systems that implement role-based access control support the ANSI Core Role Based Access Control (RBAC) recommendations. Systems that implement RBAC define groups or roles. Voting systems use the groups and stages described above to assign minimum permissions to authorized users.

11.3 – Voting system supports strong, configurable authentication mechanisms

1 – Access control mechanisms either permit authorized access or prevent unauthorized access to the voting system. This includes the capability to use multi-factor authentication to verify a user’s authorized access to perform critical operations. It also authenticates the administrator with a multi-factor authentication mechanism.

2 – User name and password covers the requirement that only the administrator can specify and enforce password strength, histories, and expiration, when that authentication method is used. The system will also compare all passwords against a manufacturer-specified list of well-known weak words, and will ensure that the username is not used in the password.

11.4 – Default access control policies enforce the principles of lease privilege and separation of duties.
11.5 – Logical access to voting system assets are revoked when no longer required. The voting system only allows users access within the time period specified by the administrator. The system locks out roles or individuals after a specified number of consecutive failed attempts, and it allows only an administrator to define the lockout duration.
11.1 - The voting system enables logging, monitoring, reviewing, and modifying of access privileges, accounts, activities, and authorizations.

11.1-A – Logging activities and resource access
The voting system must log any access to, and activities performed on, the voting system, including:

1. timestamps for all log entries
2. all failed and successful attempts to access the voting system
3. all events which change the access control system including policies, privileges, accounts, users, groups or roles, and authentication methods.

Discussion
In the event of an error or incident, the user access log can assist in narrowing down the reason for the incident or error.

- Timestamped log entries will allow for easy auditing and review of access to the voting system.
- Access control logging supports accountability of actions by identifying and authenticating users.
- Groups are a collection of users that are assigned a specific set of permissions. Roles are an identity that is given specific permissions and can be assigned to a user. Any changes to the permissions assigned to groups and roles should be logged to identify updates to a user’s privileges.

Prior VVSG source: 2007 VVSG 4.2.1-A

11.1-B – Voter information in log files
The voting system must prevent the logging of any voter identifying information.

Discussion
The logging and storing of voter identifying information after a ballot is cast violates voter privacy.

Related requirements 10.2.4-C Logging of ballot selections

11.1-C – No disabling logging
The voting system must prevent:

1. the logging capability from being disabled, and
2. the log entries from being modified.
**Discussion**

This requirement promotes the integrity of the information logged by ensuring all activities are logged. Additionally, it prevents these abilities from being an option within the user interface.

This requirement promotes the integrity of the information logged by ensuring all activities are not modifiable.

**11.1-D – On-demand access to logs**

The voting system must provide administrators access to logs on demand, allowing for continuous monitoring and periodic review.

**Discussion**

Enabling administrators to export and review the logs is a useful feature. Continuous monitoring and review of access control logs gives the administrator the opportunity to analyze and make changes to permissions and privileges, and quickly identify issues.

Prior VVSG source: 2007 VVSG 4.2.1-A
11.2 - The voting system limits the access of users, roles, and processes to the specific functions and data to which each entity holds authorized access.

11.2.1 – Authorized access

11.2.1-A – Ensuring authorized access
The voting system must allow only authorized users to access the voting system.

Discussion
Authorized users include voters, election officials, and election workers.

11.2.1-B – Modifying authorized user lists
The voting system must allow only an administrator to create or modify the list of authorized users.

Discussion
This requirement assists with ensuring only authorized users are given access to the voting system.

11.2.1-C – Access control by voting stage
The voting system access control mechanisms must distinguish at least the following voting stages from Table 11-1:

1. Pre-voting
2. Activated
3. Suspended
4. Post-voting

Table 11-1 – Voting stage descriptions

<table>
<thead>
<tr>
<th>Stage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-voting</td>
<td>Powering-on, loading, and configuring device software, maintenance, loading election-specific files, preparing for election day usage</td>
</tr>
<tr>
<td>Activated</td>
<td>Activating the ballot, printing, casting, spoiling the ballot</td>
</tr>
<tr>
<td>Suspended</td>
<td>Occurring when an election official suspends voting</td>
</tr>
<tr>
<td>Post-voting</td>
<td>Closing polls, tabulating votes, printing records, powering-off</td>
</tr>
</tbody>
</table>
11.2.1-D – Access control configuration
The voting system must allow only an administrator to configure the permissions and functionality for each identity, group or role, or process to include account and group or role creation, modification, disablement, and deletion.

Discussion
For vote-capture devices, it is possible for each group or role to have (or not have) permissions for every voting stage. Additionally, the permissions that a group or role has for a voting stage can be restricted to certain functions. Table 3 shows an example matrix of group/role to system to voting state access rights; the table is not meant to include all activities. This requirement extends [VVSG2005] I.7.2.1.1-a by allowing configuration flexibility for permissions and functionality for each identity or group/role.

Privileged accounts include any accounts within the operating system, voting device software, or other third-party software with elevated privileges such as administrator, root, and maintenance accounts. This requirement extends [VVSG2005] I.7.2.1.2 by allowing the creation and disabling of privileged accounts.

The administrator is the only user authorized to make major changes within a voting system. Administrators are given this group or role to ensure all other users have proper access to the information necessary to perform their duties.

11.2.1-E – Administrator modified permissions
The voting system must allow only an administrator to create or modify permissions assigned to specific groups or roles.

Discussion
The administrator’s authority to create or modify permissions restricts users from gaining unauthorized permissions.
11.2.1-F – Authorized assigning groups or roles
The voting system must allow only an administrator to create or assign the groups or roles.

Discussion
Table 2 is a list of groups or roles that need to be included within the voting system.

| Related requirements: | 11.2.2-B – Minimum groups or roles |

11.2.2 – Role-based access control

11.2.2-A – Role-based access control standard
Voting systems that implement role-based access control must support the recommendations for Core Role Based Access Control (RBAC) in the ANSI INCITS 359-2004 American National Standard for Information Technology – Role Based Access Control document.

Discussion
This requirement extends [VVSG2005] I. 7.2.1.1-a by requiring role-based methods to follow ANSI INCITS 359-2004.

| External references: | ANSI INCIS 359-2004 |
| Prior VVSG source: | VVSG 1.0 I.7.2.1.1 |

11.2.2-B – Minimum groups or roles
At minimum, voting systems that implement RBAC must define the following groups or roles within Table 11-2.

Table 11-2 – Minimum Voting System Groups or Roles for RBAC

<table>
<thead>
<tr>
<th>Group or role</th>
<th>Role description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Can update and configure the voting devices and troubleshoots system problems.</td>
</tr>
<tr>
<td>Voter</td>
<td>A restricted process in the vote-capture device. It allows the vote-capture device to enter the Activated state for voting activities.</td>
</tr>
<tr>
<td>Election Judge</td>
<td>Has the ability to open the polls, close the polls, recover from errors, and generate reports.</td>
</tr>
<tr>
<td>Election Worker</td>
<td>Checks in voters and activates the ballot style.</td>
</tr>
<tr>
<td>Central Election Official</td>
<td>Loads ballot definition files.</td>
</tr>
</tbody>
</table>
Discussion
Table 11-2 is a baseline list of groups or roles to be included in the voting system.

11.2.2-C – Minimum group or role permissions
At minimum, the voting system must use the groups or roles from Table 11-2 and the voting stages from Table 11-1, to assign the minimum permissions in Table 11-3.

Discussion
Table 11-3 defines the minimum functions according to user, voting stage, and system. Other capabilities can be defined as needed by jurisdiction.

Table 11-3 - Minimum permissions for each group or role

<table>
<thead>
<tr>
<th>Group/Role</th>
<th>System</th>
<th>Pre-Voting</th>
<th>Activated</th>
<th>Suspended</th>
<th>Post-Voting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>EMS</td>
<td>Full Access</td>
<td>Full Access</td>
<td>Full Access</td>
<td>Full Access</td>
</tr>
<tr>
<td></td>
<td>BMD/Electronic</td>
<td>Full Access</td>
<td>Full Access</td>
<td>Full Access</td>
<td>Full Access</td>
</tr>
<tr>
<td></td>
<td>PCOS</td>
<td>Full Access</td>
<td>Full Access</td>
<td>Full Access</td>
<td>Full Access</td>
</tr>
<tr>
<td>Voter</td>
<td>EMS</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td></td>
<td>BMD/Electronic</td>
<td>---</td>
<td>Vote and cast ballots</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td></td>
<td>PCOS</td>
<td>---</td>
<td>Ballot Submission</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Election Judge/Precinct Captain</td>
<td>EMS</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td></td>
<td>BMD/Electronic</td>
<td>Open polls, L&amp;A</td>
<td>Close or suspend polls, Recover from errors</td>
<td>Exit suspended state</td>
<td>Generate reports</td>
</tr>
<tr>
<td></td>
<td>PCOS</td>
<td>Open polls, L&amp;A</td>
<td>Recover from errors</td>
<td>Exit suspended state</td>
<td>Generate reports</td>
</tr>
<tr>
<td>Election Worker</td>
<td>EMS</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td></td>
<td>BMD/Electronic</td>
<td>---</td>
<td>Activate ballot and cancel ballots</td>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>
11.2.2-D – Applying permissions

The voting system must be capable of applying assigned groups or roles and permissions to authorized users.

**Discussion**

Once the user is assigned a group or role, the voting system needs to be capable of making the necessary changes to the user’s permissions. The permissions are changed based on the assigned group or role.
11.3 - The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations.

### 11.3.1 – Access control mechanism

#### 11.3.1-A – Access control mechanism application

The voting system must use access control mechanisms to permit authorized access or prevent unauthorized access to the voting system.

**Discussion**

Access controls support the following concepts:

- Limiting the actions of users, groups or roles, and processes to those that are authorized.
- Limiting entities to the functions for which they are authorized.
- Limiting entities to the data for which they are authorized.
- Accountability of actions by identifying and authenticating users.

Most modern operating systems natively provide configurable access control mechanisms that the voting system application can use.

Prior VVSG Source: VVSG 1.1 I.7.2.1.2-1, I.7.2.1.2-2

#### 11.3.1-B – Multi-factor authentication for critical operations

The voting system must be capable of using multi-factor authentication to verify a user has authorized access to perform critical operations, including:

1. Software updates to the certified voting system
2. Aggregation and tabulation
3. Enabling network functions, wireless, and use of telecommunications
4. Changing device states, including opening and closing the polls
5. Deleting or modifying the audit trail
6. Modifying authentication mechanisms

**Discussion**

NIST SP 800-63-3 Digital Identity Guidelines provides additional information useful in meeting this requirement. NIST SP 800-63-3 defines Multi-factor authentication (MFA) as follows:
“An authentication system that requires more than one distinct authentication factor for successful authentication. Multi-factor authentication can be performed using a multi-factor authenticator or by a combination of authenticators that provide different factors.

The three authentication factors are something you know, something you have, and something you are.

Multifactor authenticators include, but are not limited to the following:

- Username & password
- Smartcard (for example, voter access card)
- iButton
- Biometric authentication (for example, fingerprint)

External reference: NIST SP 800-63-3 Digital Identity Guidelines

11.3.1-C – Multi-factor authentication for administrators
The voting system must authenticate the administrator with a multi-factor authentication mechanism.

Discussion
This requirement extends [VVSG2005] I.7.2.1.2-e by requiring multi-factor authentication for the voting system administrator group or role.

Prior VVSG source: VVSG 1.1 I.7.2.1.2-e

11.3.2 – Username and password

11.3.2-A – Username and password management
If the voting system uses a user name and password authentication method, the voting system must allow only the administrator to enforce password strength, histories, and expiration.

Discussion
This requirement extends [VVSG2005] I.7.2.1.2-e by requiring strong passwords, password histories, and password expiration.

Prior VVSG source: VVSG 1.1 I.7.2.1.2-1
11.3.2-B – Password complexity
The voting system must allow only the administrator to specify password strength for all accounts including minimum password length per NIST 800-63B Digital Identity Guidelines standards.

Discussion
This requirement extends [VVSG2005] I.7.2.1.2-e by allowing the administrator flexibility in configuring password strength. It also requires the use of NIST 800-63B standards.

Prior VVSG source: VVSG 1.1 I.7.2.1.2-1

11.3.2-C – Minimum password complexity
The voting system must compare all passwords against a manufacturer-specified list of well-known weak passwords.

Discussion
Examples of common weak passwords include 0000, 1111, 1234.

Prior VVSG source: VVSG 1.1 I.7.2.1.2-1

11.3.2-D – Usernames within passwords
The voting system must ensure that the username is not used in the password.

Discussion
This requirement extends [VVSG2005] I.7.2.1.2-e by restricting the use of usernames and related information in passwords.

Prior VVSG source: VVSG 1.1 I.7.2.1.2-e
11.4 - The voting system’s default access control policies enforce the principles of least privilege and separation of duties.

11.4-A – Least privilege for access policies
By default, the voting system must implement the principle of least privilege including denying access to functions and data unless explicitly permitted.

**Discussion**
This requirement extends [VVSG2005] I.7.2.1.2-a by requiring explicit authorization of subjects based on access control policies.

Prior VVSG source: VVSG 1.1 I.7.2.1.2-1

11.4-B – Separation of duties
Voting system documentation must include suggested practices for dispersing critical operations across multiple groups or roles.

**Discussion**
Guidance for implementing separation of duties within the voting system is imperative to implement the separation of duties principle. Separation of duties is meant to divide user functions and roles so that there is no conflict of interest.
11.5 - Logical access to voting system assets are revoked when no longer required.

11.5-A – Access time period
The voting system must only allow users authorized access within a time period specified by the administrator.

Discussion
After authentication, a user’s access to a voting system will time-out after a specified period of time. This will avoid unauthorized access to the voting system by unauthorized users. Once a user’s access has timed-out, the user will have to re-authenticate to continue using the voting system.

11.5-B – Account lockout
The voting system must lockout roles or individuals after an administrator-specified number of consecutive failed authentications attempts.

Discussion
This requirement prevents certain classes of password guessing attacks. This requirement can be implemented using a technique such as exponential backoff. Exponential backoff requires that after each unsuccessful authentication attempt, the time period before another authentication attempt can be made grows exponentially. For instance:

- The wait after 1 unsuccessful authentication attempt is 0 seconds
- The wait after 2 unsuccessful attempts is 2 seconds
- The wait after 3 unsuccessful attempts is 4 seconds, and so on

Prior VVSG source: VVSG 1.1 I.7.2.1.2-1

11.5-C – Lockout time duration
The voting system must allow only an administrator to define the lockout duration.

Discussion
This requirement extends [VVSG2005] I.7.2.1.2 by allowing the administrator flexibility in configuring the account lockout policy. The lockout policy should not lockout voters.

Prior VVSG source: VVSG 1.1 I.7.2.1.2-1
Principle 12
Physical Security

The voting system prevents or detects attempts to tamper with voting system hardware.

12.1 - The voting system supports mechanisms to detect unauthorized physical access.

12.2 - The voting system only exposes physical ports and access points that are essential to voting operations.
Principle 12
Physical Security
The voting system prevents or detects attempts to tamper with voting system hardware.

The requirements for Principle 12 cover the mechanisms that will ensure the safety of the voting system.

12.1 – Mechanisms to detect unauthorized physical access deals with the requirement that unauthorized physical access leave physical evidence, including access to containers holding voting system records. Devices need to produce an alarm if access to a restricted voting device component is detected or if a connected component is physically disconnected during the activated state. The voting system needs to log when a device or component is connected or disconnected during an activated state and log the status of physical access points when the system is booted.

Locks installed in voting devices for security will be evaluated and meet certain requirements along with being designed with countermeasures to indicate unauthorized attempts have been made to gain access to the voting device. Locking systems will be flexible enough to support different keying schemes. Backup power for power-reliant countermeasures is also required.

12.2 – Physical ports and access points essential to voting operations covers the requirement that voting devices have only those physical ports and access points that are essential to voting operation, testing, and auditing. If a physical connection between components is broken during an activated or suspended state, the affected voting device port will be automatically disabled. Voting system will restrict physical access to any port that accommodates removable media, except for ports that activate a voting session. Devices need to allow authorized administrators to put physical ports into a disabled state. An event entry log that identifies the name of the affected device will be generated when physical ports are enable or disabled.
12.1 - The voting system supports mechanisms to detect unauthorized physical access.

12.1-A – Unauthorized physical access
Any unauthorized physical access must leave physical evidence that an unauthorized event has taken place.

Discussion
Access points such as covers and panels need to be secured by locks or other mechanisms that leave physical evidence in case of tampering or unauthorized access. Manufacturers can provide for and recommend a combination of procedures and physical measures that allow election officials to differentiate authorized from unauthorized access during all modes of operation, such as a system that relies on tamper evident tape, seals, or tags coded with consecutive serial numbers. Other systems might use seals incorporating radio frequency identification devices with physically unclonable functions or other technology in the future.

This requirement extends [VVSG2005] I.7.3.1 by requiring that any tampering with a device leave physical evidence. [VVSG2005] I.7.3.1 states that any tampering should be detectable using manufacturer-specified procedures and measures.

Prior VVSG Source: VVSG 1.0 7.3.1

12.1-B – Unauthorized physical access alarm
Voting devices must produce an alarm if access to a restricted voting device component is detected during the activated state.

Discussion
This alarm is meant to call attention to election workers in the polling place.

12.1-C – Disconnecting a physical device
The voting device must produce an alarm if a connected component is physically disconnected during the Activated state.

Discussion
Examples of connected components include printers, removable storage devices, and mechanisms used for networking. If a token is necessary for normal operation, such as a memory card or other device granting a voter access to the voting system, it is not necessary to trigger the alarm.
12.1-D – Logging of physical connections and disconnections
The voting system must log when a voting device or component is connected or disconnected during the Activated state.

**Discussion**
Logging of the devices is vital for determining cause and providing incident information if a physical security event occurs.

Related requirement: Aligns with 15.1, Detection and Monitoring

12.1-E – Logging door cover and panel status
The voting system must log the status (for example, open, closed) of physical access points, such as covers and panels, upon boot of the system.

**Discussion**
This ensures system owners can monitor access to voting device components whenever they are being used on election day. The status of the open physical access points can be externally monitored and communicated to the voting device itself.

Related requirement: Aligns with 15.1, Detection and Monitoring

12.1-F – Secure containers
Unauthorized physical access to a container holding voting system records must result in physical evidence that an unauthorized event has taken place.

**Discussion**
The goal is to ensure that election workers or observers would easily notice if someone has tampered with the container. This requirement can be achieved through locks or seals as a part of tamper evidence and tamper resistance countermeasures described by the use procedures and supplied by the manufacturer.

Additionally, to support the auditable principle, containers which hold either paper or electronic voting system records needed for audits need to be secure against physical access.

12.1-G – Secure physical locks
Locks installed in voting devices for security purposes must be:

1. evaluated and meet or exceed requirements of UL 437 for door locks and locking cylinders.
2. designed with countermeasures that give a physical indication that unauthorized attempts have been made to defeat the lock and gain access to the voting device.

Discussion
See [UL03] for UL listing requirements.

External source: UL 437

12.1-H – Secure locking system key
The voting system must support locking systems for securing voting devices that are flexible enough to support different keying schemes, including a scheme that can make use of keys that are unique to each owner.

Discussion
The use of a single key used to unlock thousands of precinct-based voting devices makes for a challenging security situation, as copies of this single key design are distributed to a large number of individuals. This creates a situation in which the key can be easily lost or stolen, and subsequently copied. At the same time, this situation does make key management significantly easier for election officials. To alleviate this situation, election officials might want keying schemes that are more or less restrictive in accordance with their election management practices and needs. This system can make use of replicable locks or cylinders, mechanisms which allow for rekeying of locks, or other technologies. The requirement does not mandate a unique key for each piece of voting equipment, but requires manufacturers to be able to provide unique keys for the voting equipment if requested by election officials. System owners need to establish procedures for issues such as key reproduction, use, and storage.

12.1-I – Backup power for power-reliant countermeasures
Any physical security countermeasure that requires power must have a backup power supply. In addition, switching from primary power supply to backup power supply:

1. produces an alarm, and
2. generates an event log entry.

Discussion
This ensures that the countermeasure isn’t disabled or intentionally circumvented by a power failure.

Switching to the backup power supply triggers an alarm that alerts an election worker to the issue so that any problem can be further diagnosed and eventually resolved. The alarm can be visible and audible.
The log entry information is security relevant, especially once a security incident has occurred, and would be useful when determining cause. Alternatively, the voting system should log when there is a switch from backup power to the primary power supply.

Applies to: Voting Device, EMS
Prior VVSG Source: VVSG 2007 5.8.9-A, VVSG 2007 5.8.9-B
Related requirement: Aligns with 15.1, Detection and Monitoring
12.2 - The voting system only exposes physical ports and access points that are essential to voting operations.

12.2-A – Physical port and access least functionality
The voting device must only have physical ports and access points that are essential to voting operations, testing, and auditing.

Discussion
Examples of ports are USB and RJ45 physical network interfaces. Examples of access points are doors, panels, and vents. Voting operations include voting device upgrades and maintenance.

Prior VVSG Source: VVSG 2007 5.6.3-C

12.2-B – Physical port auto-disable
If a physical connection between voting system components is broken during an activated or suspended state, the affected voting device port must be automatically disabled.

Discussion
Automatically disabling will require an election worker’s attention to re-enable and re-attach any network or power cabling. Under ideal circumstances, the specific election worker performing maintenance is uniquely identified within the logs, but this is not required.

12.2-C - Physical port restriction
Voting systems must restrict physical access to voting machine ports that accommodate removable media, with the exception of ports used to activate a voting session.

Discussion
Although voting systems can have ports dedicated to voting operations outside of election day activities, those ports need not be exposed while balloting is in progress. Removable media (such as Floppy, CD or DVD drives, thumb drives, and memory cards) might be essential to voting operations during pre-voting and post-voting phases of the voting cycle, such as machine upgrade, maintenance, and testing. Therefore, all removable media should be accessible only to authorized personnel. They should not be accessible to voters during activated and suspended phases of the voting cycle. It is essential that any removable drives, whether or not they are used by the system, are not accessed without detection.

Related requirements: Aligns with 14.2, System Integrity
12.2-D – Disabling ports
Voting devices must allow authorized administrators to be able to put physical ports into a disabled state.

Discussion
Logically disabling ports prevents unused ports from being used as a staging point for an attack on the voting system.

Applies to: Voting Device, EMS
Related requirements: Aligns with 14.2, System integrity

12.2-E – Logging enabled and disabled ports
An event log entry that identifies the name of the affected device must be generated when physical ports are enabled or disabled.

Discussion
Whether a port is disabled or not is security relevant, especially once a security incident has occurred, and this information would be useful when determining cause. 12.2-D applies to physical restrictions, whereas 12.2-F discusses logical disabling of ports.

Applies to: Voting Device, EMS
Related requirements: Aligns with 9.3, Access Control and 15.1, Detection and Monitoring
Principle 13
Data Protection

The voting system protects data from unauthorized access, modification, or deletion.

13.1 – The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records.

13.2 - The source and integrity of electronic tabulation reports are verifiable.

13.3 - All cryptographic algorithms are public, well-vetted, and standardized.

13.4 - The voting system protects the integrity, authenticity, and confidentiality of sensitive data transmitted over all networks.
Principle 13
Data Protection
The voting system protects data from unauthorized access, modification, or deletion.

The requirements for Principle 13 include ensuring that the voting system prevents unauthorized access to or manipulation of data and records and that the source and integrity of electronic tabulation reports are verifiable. It details cryptographic standards and ensure that the system protects sensitive data that is transmitted over all networks. The sections in Guideline 13.1 cover:

1 – Configuration file which deals with the requirement that the system allow only authenticated system administrators to access and modify voting device configuration files. In addition, the election management system (EMS) will uniquely authenticate individuals associated with the role of system administrator before they can access and modify EMS configuration files. Network appliances will uniquely authenticate individuals before allowing them to access and modify configuration files.

2 – Elections records deals with the need for the vote capture and tabulation system and the EMS to integrity protect the cast vote record (CVR) and ballot images when they are stored in the voting device.

13.2 – Source and integrity of electronic tabulation reports are verifiable covers the requirement that cast vote records and ballot images be digitally signed both when stored and before being transmitted. The EMS needs to be able to cryptographically certify all electronic voting records.

13.3 – Cryptographic algorithms are public, well-vetted, and standardized deals with the requirements that cryptographic functionality be implemented in a FIPS 140-2 validated cryptographic module operating in FIPS mode. In addition, cryptographic functions specific to E2E cryptographic voting protocols adhere to requirements set by the certification authority and are omitted from FIPS 140-2 validation. Devices using cryptography need to employ NIST approved algorithms, and the key used with Message Authentication Codes needs to have a specific security strength. Voting system documentation describes how key management is to be performed.

13.4 – Protecting sensitive data transmitted over all networks deals with the requirement that data be transmitted by a mutually authenticated connection. Voting systems transmitting data need to cryptographically protect the confidentiality and integrity of data sent over a network. A receiving voting system will adhere to requirements on verifying and logging data received and presenting any verification errors immediately.
13.1 - The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records.

13.1.1 – Configuration file

13.1.1-A – Authentication to access configuration file
The voting system must allow only authenticated system administrators to access and modify voting device configuration files.

Discussion
Voting system configuration files can include operating system and voting system application configuration files. These files can have a large impact on how the voting system functions and what election logic is being used. Therefore, accidental or malicious modification can have a large impact on the system and access to these files should be restricted to authorized individuals.

Prior VVSG source: 2007 VVSG 5.3-H
Related requirements: 13.2-A, 13.2-B
Applies to: Vote capture and tabulation system

13.1.1-B – Authentication to access configuration file on EMS
The EMS must uniquely authenticate individuals associated with the role of system administrator before allowing them to access and modify EMS configuration files.

Discussion
EMS configuration files can include operating system and voting system application configuration files. These files can have a large impact on how an EMS tabulates and reports election results. Therefore, accidental or malicious modification can have a large impact on the system and access to these files should be restricted to authorized individuals.

Prior VVSG source: 2007 VVSG 5.3-H.1
Related requirements: Access Control
Applies to: EMS workstation

13.1.1-C – Authentication to access configuration file for network appliances
Network appliances must uniquely authenticate individuals before allowing them to access and modify configuration files.
Discussion

Network appliances, such as firewalls, routers, switches, and VPN gateways are generally configurable. Individually authenticating users to the device, in lieu of using a shared password, is a standard practice for restricting access to these devices.

Related requirements: Access Control
Applies to: Network appliance

13.1.2 – Election records

13.1.2-A – Integrity protection for election records
The vote capture and tabulation system must integrity protect the CVR and ballot images when they are stored in the voting device.

13.1.2-B – EMS integrity protection for election records
The EMS must integrity protect the CVR and ballot images when they are stored in the device.

13.2 – The source and integrity of electronic tabulation reports are verifiable.

13.2-A – Signing stored electronic voting records
Cast vote records and ballot images must be digitally signed when stored.

Discussion

Digital signatures address the threat that the records might be tampered with when stored. Cryptographic hashes do not sufficiently mitigate this threat, as election records could be altered and then re-hashed.

Prior VVSG Source: 2007 VVSG 4.3.1-C

13.2-B – Signing electronic voting records prior to transmission
Cast vote records and ballot images must be digitally signed before being transmitted.

Discussion
Digital signatures address the threat that the records might be tampered with when transmitted. Cryptographic hashes do not sufficiently mitigate this threat, as hashed election records could be altered and then the hash could be recomputed.

Prior VVSG Source: 2007 VVSG 4.3.1-C

**13.2-C – Cryptographic verification of electronic voting records**

The EMS must be able to cryptographically verify all electronic voting records.

**Discussion**

Verifying the authenticity and integrity record can mitigate attacks that could modify the ballot in transit and allow unauthorized ballots to be counted. This does not solely apply to transmitted records.

Applies to: Vote capture and tabulation system, EMS

**13.3 - All cryptographic algorithms are public, well-vetted, and standardized.**

**13.3-A – Cryptographic module validation**

Cryptographic functionality must be implemented in a cryptographic module that meets or exceeds FIPS 140-2 validation, operating in FIPS mode.

This applies to:

1. A software cryptographic module
2. A hardware cryptographic module

**Discussion**

Use of validated cryptographic modules ensures that the cryptographic algorithms used are secure and their correct implementation has been validated. It also ensures that the security module security requirements have been validated to a specified security level. The current version of FIPS 140 and information about the NIST Cryptographic Module Verification Program are available at: http://csrc.nist.gov/cryptval/. Note that a voting device can use more than one cryptographic module, and quite commonly can use a software module for some functions and a hardware module for other functions. This only applies to the software module – the underlying hardware platform is omitted from this requirement.

External references: FIPS 140
NIST Cryptographic Module Verification Program

Prior VVSG source: 2007 VVSG 5.1.1-A
13.3-B – E2E cryptographic voting protocols
Cryptographic functions specific to E2E cryptographic voting protocols must adhere to requirements set by the certification authority and are omitted from FIPS 140-2 validation.

Discussion
Commonplace cryptographic operations used within E2E systems, such as encryption, decryption, and hashing, are not subject to the FIPS 140-2 validation requirement.

These new types of systems might need additional requirements to be deployed in a secure manner.

External references: FIPS 140-2
Prior VVSG source: 2007 VVSG 5.1.1-A
Applies to: E2E voting systems

13.3-C – Cryptographic strength
Devices using cryptography must employ NIST approved algorithms with a security strength of at least 112-bits

Discussion
At the time of this writing, NIST specifies the security strength of algorithms in SP 800-57, Part 1 <http://csrc.nist.gov/publications/nistpubs/index.html>. This NIST recommendation will be revised or updated as new algorithms are added, and if cryptographic analysis indicates that some algorithms are weaker than presently believed. The security strengths of SP 800-57 are based on estimates of the amount of computation required to successfully attack the particular algorithm. The specified strength should be sufficient for several decades.

This requirement is not intended to forbid all incidental use of non-approved algorithms by OS software or standardized network security protocols.

External references: SP 800-57, Part 1
Prior VVSG source: 2007 VVSG 5.1.1-B

13.3-D – MAC cryptographic strength
The key used with Message Authentication Codes must also have a security strength of at least 112 bits and use a 96-bit tag length.
Discussion
Message Authentication Codes of 96-bits are conventional in standardized secure communications protocols, and acceptable to protect voting records and systems.

Prior VVSG Source: 2007 VVSG 5.1.1-B

13.3-E – Key management documentation
The voting system documentation must describe how key management is to be performed.

Discussion
This document provides procedural steps that can be taken to ease the burden of key management and safely perform these operations.

13.4 - The voting system protects the integrity, authenticity, and confidentiality of sensitive data transmitted over all networks

13.4-A – Mutual authentication of endpoints
Data must only be transmitted by a mutually authenticated connection.

Discussion
Mutual authentication provides assurance that each electronic device is legitimate. Mutual authentication can be performed using various protocols, such as IPsec and SSL/TLS.

Prior VVSG source: 2007 VVSG 5.6.3-B
Related requirements: Access Control, Detection & Monitoring
Applies to: Voting systems with networking capabilities

13.4-B – Confidentiality protection for transmitted data
A voting system transmitting data must cryptographically protect the confidentiality of all data sent over a network at the transport layer or higher.

Discussion
This does not prevent the use of “double encrypted” connections employing cryptography at multiple layers of the network stack.
13.4-C – Integrity protection for transmitted data
A voting system transmitting data must cryptographically protect the integrity of all election data sent over the network.

Discussion
Integrity protection ensures that any inadvertent or intentional alterations to data are detected by the recipient. Integrity protection for data in transit can be provided through the use of various protocols, such as IPsec VPNs and SSL/TLS.

Applies to: EMS, Vote capture and tabulation system

13.4-D – Verification of election data
A receiving voting system must...

1. Cryptographically verify the integrity and authenticity of all election data received.
2. Immediately log onscreen any verification error of received election results.
3. Immediately present on-screen any verification errors.
4. Not tabulating or aggregating any data that fails verification.

Discussion
This information is a first line of defense against accidental errors or a malicious incident regarding modified or false election records.

This prevents the use of election results that did not pass cryptographic verification.

Applies to: EMS, Vote capture and tabulation system
Principle 14
System Integrity

The voting system performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

14.1 - The voting system uses multiple layers of controls to provide resiliency against security failures or vulnerabilities.

14.2 - The voting system limits its attack surface by avoiding unnecessary code, data paths, connectivity, and physical ports, and by using other technical controls.

14.3 - The voting system maintains and verifies the integrity of software, firmware, and other critical components.

14.4 - Voting system software updates are authorized by an administrator prior to installation.
Principle 14
System Integrity
The voting system performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

The requirements for Principle 14 include ensuring that the voting system provides redundancy against security failures, limits its attack surface, maintains and verifies the integrity of all critical components, and authorizes all software updates before they are installed.

14.1 – Voting system provides redundancy against security failures or vulnerabilities covers the requirement that the system’s documentation contains a risk assessment which provides technical controls or a notation showing the acceptable risk for each documented threat to system integrity. This document will describe how all controls work together to prevent, mitigate, and respond to attacks on the system. The system will also document necessary processes that need to occur to ensure integrity of the system.

14.2 – Voting system limits its attack surface by meeting the following requirements. The system will prevent extraneous processes and services from being installed or executed, and will disable networking and non-essential features. The system will visually show an indicator when networking functionality is enabled and disabled and will follow a secure configuration guide for all underlying operating systems and other voting system components.

The system documentation will include the guidance used to ensure the system is securely configured. The system application will not contain unused or dead code. The system’s underlying platform will provide and make use of modern exploit mitigation technologies.

The system application will not import entire software libraries where individual functions are more practical. The voting system will have the capability to restrict access to physical ports that are to be used solely by election judges and administrators.

The underlying system platform generally needs to be free of well-known vulnerabilities before certification, unless the certification authority allows it. In that case, a list of these vulnerabilities will be provided to the certification authorities before it is certified.

14.3 – Voting system maintains and verifies the integrity of all critical components covers the requirement that a voting system’s documentation contain

- a supply chain risk management strategy
- a list of critical components defined by criticality analysis, and
- hardware and software information for the critical components defined in 14.3-B
1 – **Boot integrity** deals with the requirement that the voting system cryptographically verifies system integrity before the operating system is loaded into memory. If the system fails boot validation, it will not boot, will provide an onscreen alert, and log this failure along with any information necessary to understand the failure.

2 – **Software integrity** states that the voting system will only allow digitally signed software and firmware to be installed. The system cryptographically verifies the digital signature before installation and whitelists all application running in userspace. It will also protect the integrity and authenticity of the whitelist configuration files.

14.4 – **Software updates are authorized prior to installation** covers the requirement that the voting system authenticates administrators:

- before an operating system update
- before a software update to the system application and related hardware
- before a firmware or driver update

**14.1 - The voting system uses multiple layers of controls to provide resiliency against security failures or vulnerabilities.**

**14.1-A – Risk assessment documentation**
The voting system’s documentation must contain a risk assessment

**Discussion**
Risk assessments are a foundation of effective risk management. Additionally, they help to facilitate decision making at the organization, business process, and information system levels. Many methods of conducting risk assessments exist, including NIST SP 800-30-1: Guide for Conducting Risk Assessments or ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management.

- External references: NIST SP 800-30-1: Guide for Conducting Risk Assessments

- Related requirements: 3.1.3-E – Risk Analysis

**14.1-B – Addressing and accepting risk**
The voting system’s risk assessment documentation must provide technical controls or a notation showing the acceptance of risk for each documented threat to voting system integrity.
Discussion
Assigning controls or accepting risk is a key part of the risk assessment process.

Related requirements: 3.1.3-E – Risk Analysis

14.1-C – System security architecture description
The voting system’s risk assessment documentation must describe how physical, technical, and operational controls work together to prevent, mitigate, and respond to attacks on the voting system. This includes the use of:

1. Cryptography
2. Malware protection
3. Firewall access control lists, rules, and configurations
4. System configurations

Discussion
Risk assessments can be large, complicated documents. This requirement ensures that a single narrative exists to explain to election officials and other system owners how the overall security operates for the voting system.

Related requirements: 3.1.3-C – Physical security

14.1-D – Procedural and operational security
The voting system must document necessary procedural and operational processes that need to occur to ensure integrity of the system.

Discussion
Procedural and operational security processes play a key role in overall system security. If any of these procedures are necessary to ensure system integrity or system security, these practices need to be well documented and explained.
14.2 - The voting system limits its attack surface by avoiding unnecessary code, data paths, connectivity, and physical ports, and by using other technical controls.

14.2-A – Extraneous processes and services
The voting system must prevent extraneous processes and services from being installed or executed.

**Discussion**
Attack surface mitigation limits the voting system’s exposure to malicious activity. The presence of non-essential programs or network services severely increases attack surface. This can include network services, superfluous userspace processes, integrated development environment, and compilers.

14.2-B – Non-essential features
The voting system must disable networking and other features that are non-essential to the function of the voting system by default.

**Discussion**
When the voting system is booted, networking and other functions are prohibited from running. For instance, networking interfaces such as eth, wlan, and hci should be off.

By disabling features that are non-essential to the voting system, this decreases the attack surface by limiting the functionality and decreasing the entry points that may be accessed by unauthorized users.

14.2-C – Network status indicator
The voting system application must visually show an indicator within the management interface when networking functionality is enabled and disabled.

**Discussion**
This helps to ensure that network functionality is not enabled by accident.

14.2-D – Wireless network status indicator
If a voting system has network functionality, the voting system application must visually show an indicator within the management interface when wireless networking functionality is enabled and disabled.
Discussion
Note that this is in addition to the networking identifier.

Wireless is a significant avenue for system compromise. This indicator ensures that wireless functionality is not enabled by accident.

14.2-E – Secure configuration and hardening
The voting system must follow a secure configuration guide for all underlying operating systems and other voting system components, with any deviations from best practice documented and justified.

Discussion
Properly configuring an operating system is a difficult and complex task, with small settings potentially causing a large impact. Industry, NIST, and various agencies within the DoD offer guidance for specific operating systems, as do OS and component manufacturers.

Documenting deviations ensures that important settings are not overlooked and decisions to deviate are properly considered.

14.2-F – Secure configuration and hardening documentation
The voting system documentation must include the guidance used to securely configure the voting system.

Discussion
Access to the guidance used for secure configuration provides a reference to ensure the voting system is securely configured.

14.2-G – Unused code
The voting system application must not contain unused, or dead code.

Discussion
An attacker may be able to take advantage of the unused code and introduce software bugs/exploits that can be used to make the voting system vulnerable.

Dead code is source code that can never be executed in a running program. The surrounding code makes it impossible for a section of code to ever be executed [See MITRE CWE-561-https://cwe.mitre.org/data/definitions/561.html]. Software with dead code is considered poor quality and reduces maintainability.
14.2-H – Exploit mitigation technologies within platform
The underlying platform of the voting system must provide modern exploit mitigation technologies such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR).

Discussion
DEP and ASLR are commonplace exploit mitigation technologies that can help prevent a variety of vulnerability types, including memory corruption errors like buffer overflows.

14.2-I – Application use of exploit mitigation technologies
The underlying platform of the voting system must make use of the exploit mitigation technologies provided by the underlying system.

Discussion
Applications need to be written and compiled in such a way as to make use of underlying exploit mitigation technologies.

14.2-J – Importing software libraries
The voting system application must not import entire software libraries where individual functions are more practical.

Discussion
Importing entire software libraries significantly increases the attack surface of the software. Importing only the functions needed is a useful attack surface minimization strategy. Not all 3rd party libraries are easily modifiable, making this attack surface reduction strategy impractical.

Applies to: Voting System Application

14.2-K – Physical port restriction
The voting system must have the capability to restrict access to physical ports that are meant to be used solely by election judges and administrators.

Discussion
Physical port access needs to be restricted when not in use. This requirement is not meant to impede the use of accessible technology.

Related requirements: Physical Security
14.2-L – Known vulnerabilities
The underlying voting system platform must be free of well-known vulnerabilities before certification, unless otherwise noted by the certification authority.

Discussion
Vulnerability scanning tools can be used to identify known vulnerabilities in software and firmware. The U.S. National Vulnerability Database (NVD) is one resource that can be useful for identifying known vulnerabilities. Other vulnerability databases also exist and can be leveraged for full vulnerability coverage that might not be identified by automated scanning tools.

14.2-M – List of known vulnerabilities
If the certification authority allows certification of the voting system with known vulnerabilities, a list of these vulnerabilities must be provided to the certification authority before it is certified.

Discussion
Certain information can also be included for each vulnerability, such as any severity, impact, or exploitability scores.

14.3 - The voting system maintains and verifies the integrity of software, firmware, and other critical components.

14.3-A – Supply chain risk management strategy
The voting system’s documentation must contain a supply chain risk management strategy that at minimum includes the following:

1. A reference to the template or standard used, if any, to develop the supply chain risk management strategy
2. Identification and prioritization of the critical systems, components and services
3. The contract language that requires suppliers and partners to provide the appropriate information to meet the assurance requirements of the supply chain risk management strategy. This includes the products or services acquired from the suppliers/partners and any evidence or artifacts that attest to the required level of assurance.
4. The plan for reviewing and auditing suppliers and partners
5. The response and recovery plan for a supply chain risk incident
**Discussion**
Supply chain risks may include insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices in the technology supply chain. These risks are associated with an organization’s decreased visibility into, and understanding of, how the technology that they acquire is developed, integrated, and deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services. These risks can be managed by...

- Utilizing the NIST Cybersecurity Framework version 1.1. by referencing the Supply Chain Risk Management category and subcategory
- Referencing the relevant security controls for supply chain in NIST SP 800-53 Rev. 5 *Security and Privacy Controls for Information Systems and Organizations*

**External references:**
- NIST Cybersecurity Framework Version 1.1
- NIST SP 800-53 Rev. 5

### 14.3-B – Criticality analysis
The voting system’s documentation must include a list of critical components defined by a criticality analysis.

**Discussion**
Defining the critical components of the voting system can assist in prioritizing their importance to the voting process and identifying the impact to security, privacy and performance for failure or compromise.

This can be supplemented by following NISTIR 8179 *Criticality Analysis Process Model - Prioritizing Systems and Components.*

**External references:**
- NISTIR 8179 – Criticality Analysis Process Model – Prioritizing Systems and Components
14.3-B.1 – Bill of Materials

The voting system’s documentation must include the hardware and software information for the critical components defined in the 14.3-B and at minimum list the following information for each component:

1. Component name
2. Manufacturer
3. Model or Version
4. Applicable platform for software (e.g., Windows or Linux)

Discussion

This requirement will use the critical components defined in the critical analysis of 14.3-B.

This is a common practice when providing a hardware bill of materials. It is not as common to produce a bill of materials for software and as standards/best practices are developed, they should be considered for inclusion in the software bill of materials.

External references: SAFECODE - Security Risks Inherent in the Use of Third-party Components

14.3.1 – Boot integrity

14.3.1-A – Cryptographic boot verification

The voting system must cryptographically verify system integrity before the operating system is loaded into memory.

Discussion

This requirement does not mandate hardware support. This requirement could be met by trusted boot, but other software-based solutions exist. This includes a software bootloader cryptographically verifying the OS prior to execution. Verifying the bootloader itself is excluded from this requirement, but not prohibited.

Applies to: Vote capture and tabulation device, EMS

14.3.1-B – Preventing of boot on error

If the voting system fails boot validation, the voting system must not boot and provide an onscreen alert.
Discussion
System users need to be notified when the voting system is either corrupted or has been maliciously modified.

Boot validation prevents unauthorized operating systems and software from being installed or run on a system.

Applies to: Vote capture and tabulation device, EMS

### 14.3.1-C – Logging of verification failure

The voting system must log if the voting system does not pass boot validation and include any other necessary information to understand the failure.

**Discussion**
Failure of boot validation needs to be logged so these errors can be further analyzed when needed.

Applies to: Vote capture and tabulation device, EMS

### 14.3.2 – Software integrity

#### 14.3.2-A – Installing software

The voting system must only allow digitally signed software and firmware to be installed.

**Discussion**
Signed software and firmware ensures that it is not modified before installation, and that it is being distributed by the proper entity.

#### 14.3.2-B – Software verification for installation

The voting system must cryptographically verify the digital signature of software and firmware before it is installed.

**Discussion**
The security properties of integrity and authenticity are not achieved unless the digital signature for the signed software and firmware is cryptographically verified.

#### 14.3.2-C – Software whitelisting

The voting system must whitelist all applications running in userspace.

**Discussion**
This is the principle malware prevention mechanism on the voting system. One method of achieving
this is cryptographically verifying the digital signatures of all applications before they are run on the voting system.

Applies to: Vote Capture Device

14.3.2-D – Integrity protection for software whitelists
The voting system must protect the integrity and authenticity of the whitelist configuration files.

Discussion
If the whitelist is improperly modified, the software whitelisting mitigation can be defeated. The most common way of providing whitelist configuration file protection could be a digital signature.

Applies to: Vote Capture Device

14.4 - Voting system software updates are authorized by an administrator prior to installation.

14.4-A – Authenticated operating system updates
The voting system must authenticate administrators before an operating system update is performed.

Discussion
Administrators are required to be authenticated before they can update the voting system, regardless of whether the update is done by a networked method or performed using physical media.

Related requirements: Access Control
Applies to: Vote Capture Device

14.4-B – Authenticated application updates
The voting system must authenticate administrators before a software update to the voting system application and related software.

Discussion
Administrators are required to be authenticated before they can update the voting system, whether the update is applied by a network method or physical media.

Related requirements: Access Control
Applies to: Vote capture and tabulation device, Network appliances, EMS
14.4-C – Authenticated firmware updates
The voting system must authenticate administrators before a firmware or driver update.

Discussion
Administrators are required to be authenticated before they can update the voting system, regardless if network enabled update is performed or via physical media.

Related requirements: Access Control
Applies to: Vote Capture Device
Principle 15
Detection and Monitoring

The voting system provides mechanisms to detect anomalous or malicious behavior.

15.1 - Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing.

15.2 - The voting system generates, stores, and reports all error messages as they occur.

15.3 - The voting system is designed to protect against malware.

15.4 - A voting system with networking capabilities employs appropriate, well-vetted modern defenses against network-based attacks, commensurate with current best practice.
Principle 15
Detection and Monitoring
The voting system provides mechanisms to detect anomalous or malicious behavior.

The requirements for Principle 15 include ensuring that voting system equipment records important activities through event logging, and generates and reports all error messages as they occur. The system employs mechanisms to protect against malware. Systems with networking capabilities employ defenses against network-based attacks.

15.1 – Voting system equipment records important activities through event logging mechanisms covers the requirements that the system be capable of logging events that occur in a voting system and of exporting those logs. The system will not log any information identifying a specific voter or connecting a voter to a specific ballot. At a minimum, the system will log events including:

- general system functions
- networking
- software
- voting functions

In addition, when a system administrator is accessing a configuration file, the system needs to log identifying information about the individual and group or role accessing that file.

15.2 – Voting system generates, stores, and reports all error messages as they occur covers the requirement that systems provide immediate notification to the user when an error occurs and that system documents include procedures for handling errors, including logging all errors and creating error reports.

15.3 – Voting system employs mechanisms to protect against malware deals with the requirement that vote capture and tabulation devices verify software using digital signatures or application whitelisting. The sections in 15.3.1 cover requirement specific to malware protection mechanisms.

1 – Malware protection mechanisms deals with the need for COTS devices that provide EMS functionality to:

- deploy mechanisms to protect against malware
- promptly notify an election official when malware is detected
- provide notification upon the removal or remediation of malware

The system’s malware protection mechanisms need to be updatable and the documentation needs to include the process and procedures for performing the updates. The voting system will log instances when it detects malware along with malware remediation activities.
15.4 – Voting system with networking capabilities employs appropriate defenses against network-based attacks deals with the requirement for system documentation to include the network architecture of any internal network used by any portion of the voting system. Voting system documentation includes how any public telecommunications networks are used by any portion of the system. Documentation also lists security relevant configurations and is accompanied by network security best practices. The system includes a firewall or intrusion detection system (IDS). Default configurations for the system implement the principle of least privilege. In addition, the system needs to be capable of updating rules and policies for firewalls and other network appliances.

15.1 - Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing.

15.1-A – Event logging
The voting system must be capable of logging events that occur in a voting system.

Discussion
The ability to log events within a system allows for continuous monitoring of the voting system. These logs provide a way for administrators to analyze the voting system’s activities, diagnose issues, and perform necessary recovery and remediation actions.

15.1-B – Exporting logs
The voting system must be capable of exporting logs.

Discussion
Exporting logs offers the opportunity for external review, clearing storage, and a method to compare with future logs.

15.1-C – Logging voter information
The voting system must not log any information:

1. identifying a specific voter
2. connecting a voter to a specific ballot

Discussion
No voter information is stored anywhere within voting system logs. This would violate voter ballot secrecy because it can link a voter to their ballot selections.

Related requirements: 11.1-B and Ballot secrecy

15.1-D – Logging event types

At minimum, the voting system must log the events included in Table 15-1.

**Discussion**

Table 15-1 provides a list of events that will be included in the voting system event logs. The voting system is not limited to the events in the table.

Related requirements Access Control, System Integrity, Data Protection

**Table 15-1 – System events to log**

<table>
<thead>
<tr>
<th>System Event</th>
<th>Description</th>
<th>Applies To</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General system functions</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Device generated error and exception messages | Includes but is not limited to:  
- The source and disposition of system interrupts resulting in entry into exception handling routines.  
- Messages generated by exception handlers.  
- The identification code and number of occurrences for each hardware and software error or failure.  
- Notification of physical violations of security.  
- Other exception events such as power failures, failure of critical hardware components, data transmission errors, or other types of operating anomalies.  
- All faults and the recovery actions taken.  

Device generated error and exception messages such as ordinary timer system interrupts and normal I/O system interrupts do not need to be logged. | Programmed device |
| **Critical system status messages** | Critical system status messages other than information messages displayed by the device during the course of normal operations. Includes but is not limited to:  
- Diagnostic and status messages upon startup  
- The “zero totals” check conducted before opening the polling place or counting a precinct centrally | Programmed device |
<table>
<thead>
<tr>
<th>Event Type</th>
<th>Description</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>For paper-based systems, the initiation or</td>
<td>For paper-based systems, the initiation or termination of scanner and</td>
<td>Programmed device</td>
</tr>
<tr>
<td>termination of scanner and communications</td>
<td>termination of scanner and communications equipment operation</td>
<td></td>
</tr>
<tr>
<td>equipment operation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Printer errors</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detection or remediation of malware or other</td>
<td>Detection or remediation of malware or other malicious software</td>
<td></td>
</tr>
<tr>
<td>malicious software</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cryptographic boot validation success/failure</td>
<td>Cryptographic boot validation success/failure</td>
<td></td>
</tr>
</tbody>
</table>

| Non-critical status messages                  | Non-critical status messages that are generated by the device’s data        | Programmed device             |
|                                               | quality monitor or by software and hardware condition monitors.              |                               |

| Events that require election official         | Events that require election official intervention, so that each election   | Programmed device             |
| intervention                                  | official access can be monitored, and access sequence can be constructed.   |                               |

| Device shutdown and restarts                  | Both normal and abnormal device shutdowns and restarts.                     | Programmed device             |

| Changes to system configuration settings      | Configuration settings include but are not limited to registry keys, kernel  | Programmed device             |
|                                               | settings, logging settings, and other voting device configuration settings.   |                               |

| Integrity checks for executables,            | Integrity checks that can indicate possible tampering with files and data.   | Programmed device             |
| configuration files, data, and logs.          |                                                                             | with file systems              |

| The addition and deletion of files.          | Files that are added or deleted from the voting device.                      | Programmed device             |
|                                               |                                                                             | with file systems              |

| System readiness results                     | Includes but is not limited to:                                             | Programmed device             |
|                                               | • System pass or fail of hardware and software test for system readiness    |                               |
|                                               | • Identification of the software release, identification of the election to|                               |
|                                               | be processed, polling place identification, and the results of the software  |                               |
|                                               | and hardware diagnostic tests                                              |                               |
|                                               | • Pass or fail of ballot style compatibility and integrity test             |                               |
|                                               | • Pass or fail of system test data removal                                 |                               |
|                                               | • Zero totals of data paths and memory locations for vote recording        |                               |

| Removable media events                        | Removable media that is inserted into or removed from the voting device.    | Programmed device             |

| Backup and restore                            | Successful and failed attempts to perform backups and restores.             | Election Management Systems   |

**Authentication and Access Control**
<table>
<thead>
<tr>
<th>Authentication related events</th>
<th>Includes but is not limited to:</th>
<th>Programmed device</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Login/logoff events (both successful and failed attempts)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Account lockout events</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Password changes</td>
<td></td>
</tr>
<tr>
<td>Access control related events</td>
<td>Includes but is not limited to:</td>
<td>Programmed device</td>
</tr>
<tr>
<td></td>
<td>• Use of privileges (such as a user running a process as an administrator)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Attempts to exceed privileges</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• All access attempts to application and underlying system resources</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Changes to the access control configuration of the voting device</td>
<td></td>
</tr>
<tr>
<td>User account and role (or groups) management activity</td>
<td>Includes but is not limited to:</td>
<td>Programmed device</td>
</tr>
<tr>
<td></td>
<td>• Addition and deletion of user accounts and roles</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• User account and role suspension and reactivation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Changes to account or role security attributes such as password length, access levels, login restrictions, and permissions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Administrator account and role password resets</td>
<td></td>
</tr>
<tr>
<td>Networking</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enabling or disabling networking functionality</td>
<td>Includes but is not limited to:</td>
<td>Programmed device</td>
</tr>
<tr>
<td></td>
<td>• Wired networking</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Wireless networking</td>
<td></td>
</tr>
<tr>
<td>Software</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Installing, upgrading, patching, or modifying software or firmware</td>
<td>Logging for installation, upgrading, patching, or modifying software or firmware include logging what was installed, upgraded, or modified as well as a cryptographic hash or other secure identifier of the old and new versions of the data.</td>
<td>Programmed device</td>
</tr>
<tr>
<td>Changes to configuration settings</td>
<td>Includes but is not limited to:</td>
<td>Programmed device</td>
</tr>
<tr>
<td></td>
<td>• Changes to critical function settings. At a minimum, critical function settings include location of election definition file, contents of the election definition file, vote reporting, location of logs, and voting device configuration settings.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Changes to device settings including, but not limited to, enabling and disabling services.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Starting and stopping processes.</td>
<td></td>
</tr>
<tr>
<td>Abnormal process exits</td>
<td>All abnormal process exits.</td>
<td>Programmed device</td>
</tr>
<tr>
<td>Successful and failed database connection attempts (if a database is used)</td>
<td>All database connection attempts.</td>
<td>Programmed device with database capabilities</td>
</tr>
</tbody>
</table>
### Cryptographic Functions

<table>
<thead>
<tr>
<th>Changes to cryptographic keys</th>
<th>At a minimum, critical cryptographic settings include key addition, key removal, and re-keying.</th>
<th>Programmed device</th>
</tr>
</thead>
</table>

#### Voting Functions

| Ballot definition and modification | During election definition and ballot preparation, the device can provide logging information for preparing the baseline ballot formats and modifications to them, including a description of the modification and corresponding dates. Includes but is not limited to:  
- The account name that made the modifications.  
- A description of what was modified including the file name, location, and the content changed.  
- The date and time of the modification. | Programmed device |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------|-------------------|

| Voting events | Includes:  
- Opening and closing polls  
- Casting a vote  
- Canceling a vote during verification  
- Success or failure of log and election results exportation  
- Note: for paper-based devices, these requirements might need to be met procedurally | Programmed device |
|----------------|-------------------------------------------------------------------------------------------------------------------|-------------------|

#### 15.1-E – Configuration file access log

When a system administrator is accessing a configuration file, the voting system must log identifying information of the individual and group or role accessing that file.

**Discussion**

A record of who modified a configuration file is important for auditing and accountability. The identifying information should include the username or the name of the user.
15.2 - The voting system generates, stores, and reports all error messages as they occur.

15.2-A – Presentation of errors
The voting system must provide immediate notification to the user when an error occurs.

Discussion
Immediate notification of an issue or an error allows for prompt recovery and remediation.

15.2-B – Documenting error handling
The voting system documentation must include procedures for handling errors.

Discussion
Documentation will assist election officials with steps to properly address errors.

15.2-C – Logging errors
The voting system must log all errors.

15.2-D – Creating error reports
The voting system must be capable of creating error reports.

Discussion
Error reports allow system administrators to easily analyze the errors that occurred within a system.

15.3 - The voting system is designed to protect against malware.

15.3-A – Software verification
Vote capture and tabulation devices must verify software using digital signatures, application whitelisting, or some combination of the two.

Discussion
Digital signatures and whitelists assist in ensuring the vote capture and tabulation devices are using the correct software. If unauthorized software is found on the device, the appropriate malware remediation and response procedures will be implemented.

Related requirements: System Integrity, Data Protection
Applies to: Vote capture and tabulation devices

15.3.1 – Malware protection

15.3.1-A – Malware protection mechanisms
COTS devices providing EMS functionality must deploy mechanisms to protect against malware.

Discussion
NIST SP 800-83 Revision 1 Guide to Malware Incident Prevention and Handling for Desktops and Laptops might be useful as supplemental guidance for protecting against malware. Digital signatures and whitelists can also be useful protection mechanisms.

External reference: NIST SP 800-83 Revision 1 Guide to Malware Incident Prevention and Handling for Desktops and Laptops

Applies to: EMS Workstations

15.3.1-B – Updatable malware protection mechanisms
The voting system’s malware protection mechanisms must be updatable.

Discussion
Malware protection mechanisms typically use software signatures to identify malware. As new malware signatures are received, the malware protection mechanism needs to be updated with the new signatures to ensure it is identifying all known malware.

Applies to: EMS Workstations, vote capture and tabulation devices

15.3.1-C – Documenting malware protection mechanisms
The voting system documentation must include the process and procedures for updating malware protection mechanisms.

Discussion
Providing documentation of the procedures to configure the malware protection mechanisms assists with ensuring the malware protection mechanisms are properly updated to meet 15.3.1-B- Updatable malware protection mechanisms.

Applies to: EMS Workstations, vote capture and tabulation devices
15.3.1-D – Notification of malware detection
COTS devices providing EMS functionality must promptly notify an election official when malware is detected.

Discussion
Malware on an EMS device can disrupt the integrity of the data on the EMS device. Notification of malware detection allows election officials to promptly take the proper action to avoid data integrity issues.

Applies to: EMS Workstations

15.3.1-E – Logging malware detection
The voting system must log instances of detecting malware.

15.3.1-F – Notification of malware remediation
COTS devices providing EMS functionality must provide a notification upon the removal or remediation of malware.

Discussion
Once malware it is identified on a device, operations can cease until the malware is remediated. This notification allows administrators and officials to know when it is safe to resume normal operations.

Applies to: EMS Workstation

15.3.1-G – Logging malware remediation
The voting system must log malware remediation activities.

15.4 - A voting system with networking capabilities employs appropriate, well-vetted modern defenses against network-based attacks, commensurate with current best practice.

15.4-A – Network architecture documentation
The voting system documentation must include the network architecture of any internal network used by any portion of the voting system.

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

Applies to: Voting systems with networking capabilities

15.4-B – Telecommunications documentation

The voting system documentation must include how any public telecommunications networks are used by any portion of the voting system, including vote capture devices and EMS workstations.

Applies to: Voting systems with networking capabilities

Discussion

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

Applies to: Voting systems with networking capabilities

15.4-C – Secure configuration documentation

The voting system documentation must list security relevant configurations and be accompanied by network security best practices.

If outside manufacturers provide guidance and best practices exist, these need to be documented and used to the extent practical.

Discussion

A variety of documentation providing secure configurations for network devices is publicly available from the US government.

External network services need to be documented.

Applies to: Voting systems with networking capabilities

15.4-D – Firewall and IDS

The voting system must include a firewall or intrusion detection system (IDS).

Discussion

This requirement does not include point-to-point networks which do not typically use network appliances.

Applies to: Voting systems with networking capabilities
15.4-E – Least privilege
Default configurations for the voting system must implement the principle of least privilege.

**Discussion**

Network access is only as much as is necessary to perform the desired function.

<table>
<thead>
<tr>
<th>Related requirements</th>
<th>Applies to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>Voting systems with networking capabilities</td>
</tr>
</tbody>
</table>

15.4-F – Rule and policy updates
The voting system must be capable of regularly updating rules and policies for firewalls and other network appliances.

**Discussion**

Network appliances and the voting system are constantly receiving improvements and information related to current threats. As this information is released, rules and policies might need to be modified to adjust to new capabilities.

| Applies to: | Voting systems with networking capabilities |
Appendix A
Glossary of Terms
Glossary

A:

absentee ballot

Ballot used for absentee voting.

absentee voting

Voting that can occur unsupervised at a location chosen by the voter either before or on election day.

acceptance testing

Examination of a voting system and by the purchasing election jurisdiction to validate:

- the performance of delivered devices to ensure they meet procurement requirements, and
- that the delivered system is, in fact, the certified system purchased.

This usually happens in a simulated-use environment.

access control

The process of granting or denying specific requests to:

- obtain and use information and related information processing services; and
- enter specific physical facilities.

accessibility

Measurable characteristics that indicate the degree to which a system is available to, and usable by, individuals with disabilities. The most common disabilities include those associated with vision, hearing, mobility, and cognition.
accreditation

Formal recognition that a laboratory is competent to carry out specific tests or calibrations.

accreditation body

1. Authoritative body that provides accreditation.
2. Independent organization responsible for
   • assessing the performance of other organizations against a recognized standard, and
   • formally confirming the status of those that meet the standard.

activation device

Programmed device that creates credentials necessary to begin a voting session using a specific ballot style. Examples include electronic poll books and card activators that contain credential information necessary to determine the appropriate ballot style for the voter.

active period

Span of time during which a vote-capture device either is ready to begin a voting session or is in use during a voting session.

adjudication

Process of resolving flagged cast ballots to reflect voter intent. Common reasons for flagging include:

- write-ins,
- overvotes,
- marginal marks,
- having no contest selections marked on the entire ballot, or
- the ballot being unreadable by a scanner.

adjudication-required ballot

A ballot that contains contest selections that require adjudication.

air gap

A physical separation between systems that requires data to be moved by some external, manual procedure.
alert time

The amount of time that a voting device will wait for detectible voter activity after issuing an alert, before going into an inactive state requiring election worker intervention.

alternative format

The ballot or accompanying information is said to be in an alternative format if it is presented in non-standard ballot language and format. Examples include, but are not limited to, languages other than English, Braille, ASCII text, large print, recorded audio.

appropriate mark

An expected mark made according to the ballot instructions.

approval voting

A vote variation used for elections in which each voter may "approve" of (that is, select) any number of candidates. Typically, the winner is the most-approved candidate.

archival media

Storage media that is designed to preserve content for an extended period of time with minimal data corruption or loss.

assistive technology

A device that improves or maintains the capabilities of people with disabilities (such as no vision, low vision, mobility, or cognitive). These devices include headsets, keypads, software, sip-and-puff, and voice synthesizers.

asymmetric cryptography

Encryption system that uses a public and private key pair for cryptographic operation. The private key is generally stored in a user's digital certificate and used typically to encrypt or digitally sign data. The public key is used typically to decrypt the data or verify its digital signatures. The keys could be used interchangeably as needed, that is, a public key can be used to encrypt data and the private key can be used to decrypt the data.
audio format

A ballot display format in which contest options and other information are communicated through sound and speech.

audit

1. Systematic, independent, documented process for obtaining records, statements of fact, or other relevant information and assessing them objectively to determine the extent to which specified requirements are fulfilled.
2. Verification of statistical or exact agreement of records from different processes or subsystems of a voting system.
3. A review of a system and its controls to determine its operational status and the accuracy of its outputs.

audit device

Voting device dedicated exclusively to independently verifying or assessing the voting system's performance.

audit trail

Information recorded during election activities to reconstruct steps followed or to later verify actions taken with respect to the voting system.

authentication

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. Audit trails may include event logs, paper records, error messages, and reports.
B:

ballot

Presentation of the contest options for a particular voter.

ballot counting logic

The software logic that:

- defines the combinations of contest selections that are valid and invalid on a given ballot and,
- determines how the contest selections are totaled in a given election.

ballot data

A list of contests and associated options that may appear on a ballot for a particular election.

ballot display format

The concrete presentation of the contents of a ballot appropriate to the particular voting technology being used. The contents may be rendered using various methods of presentation (visual or audio), language, or graphics.

ballot image

Electronically produced record of all votes cast by a single voter. A ballot image might be a transient logical representation of the votes or an archival record (a cast vote record).

ballot instructions

Information provided to the voter that describes the procedure for marking the ballot. This information may appear directly on the paper or electronic ballot or may be provided separately.

ballot manifest

A catalog prepared by election officials listing all the physical paper ballots and their locations in sequence.
ballot marking device

A **device** that:

- permits **contest options** to be reviewed on an electronic interface,
- produces a human-readable **paper ballot**, and
- does not make any other lasting **record** of the **voter**'s selections.

ballot measure

A question that appears on a **ballot** with options, usually in the form of an approval or rejection.

ballot measure option

A **contest option** that specifies a response to a **ballot measure**.

ballot on demand®

A process that produces a **paper ballot** of the required **ballot style** that meets a specific **voter**'s needs. The use of this process requires:

- a system with a printer that can create a tabulatable paper ballot; and
- a **device** driving the printer that has all the data needed to print each ballot style and allows selection of the needed style.

Note: "ballot on demand" is a registered trademark of ES&S.

ballot production

Process of generating **ballots** for presentation to **voters**, for example, printing **paper ballots** or configuring the ballot presentation for an electronic display.

ballot rotation

The process of varying the order of listed **candidates** within a **contest**. This allows each candidate to appear first on the list of candidates an approximately equal number of times across different **ballot styles** or **election districts**.

ballot style

**Ballot data** that has been put into **contest** order for a particular **precinct** and considers a particular set of **voter** situations. Voter situations include party affiliation (for **closed primaries**),
and age of the voter (in states that permit 17-year-olds to vote in primary elections), among others.

**barcode**

An optical, machine-readable representation of data as a sequence of bars and spaces that conform to accepted standards. Linear (1d) barcode standards include UPC, EAN and 128. QR is an example of a 2d barcode standard.

**barcode reader**

*Device* used to scan *barcodes* and convert the encoded information into a usable format. Barcode readers are used to scan codes on a variety of *election* materials including *ballots*, driver’s licenses, voter ID cards, voter information packets, envelopes, and other election documents.

**batch**

A collection of *paper ballots* gathered as a group for tabulation or for auditing.

**batch fed scanner**

An electronic *voting device* that:

- accepts stacks of hand-marked or BMD-produced *paper ballots* and automatically processes them until the stack is empty;
- is usually used at an *election jurisdiction*’s central location;
- is mostly commonly used to process absentee or mail *ballots*;
- usually has input and output hoppers for ballots;
- scans a ballot and rejects it if either unreadable or un-processable;
- detects, interprets, and validates *contest selections*;
- detects and sorts (either digitally or physically) ballots that are unreadable or un-processable, or that contain undeterminable selections, marking exceptions, or write-ins; and
- **tabulates** and **reports contest** results as required. This unit was previously referred to as central count optical scanner or CCOS.

**benchmark**

Quantitative point of reference to which the measured performance of a system or *device* may be compared.
blank ballot

An issued ballot without any selections made.
Callable Unit

(Of a software program or logical design) Function, method, operation, subroutine, procedure, or analogous structural unit that appears within a module.

Candidate

Person contending in a contest for office. A candidate may be explicitly presented as one of the contest options or may be a write-in candidate.

Candidate Option

A contest option that is associated with a candidate.

Canvass

The process of compiling, reviewing, and validating election returns that forms the basis of the official results by a political subdivision.

Cast

(v) The final action a voter takes in selecting contest options and irrevocably confirming their intent to vote as selected.

Cast Ballot

Ballot in which the voter has taken final action in selecting contest options and irrevocably confirmed their intent to vote as selected.

Cast Vote Record

Archival tabulatable record of all votes produced by a single voter from a given ballot.

Central Reporting Device

Electronic voting device that consolidates and reports vote totals from multiple precincts at a central location.
certification testing

Testing of a voting system performed by a testing authority (such as the EAC or a state) to ensure that the system meets the requirements defined in the standards being tested against in the manner specified in its product documentation.

Ciphertext

Data or information in its encrypted form.

closed primary

Partisan primary election in which the voter receives a ballot containing only those party-specific contests pertaining to the political party with which the voter is affiliated, along with non-party-specific contests presented at the same election. Unaffiliated voters may be permitted to vote only on non-party-specific contests.

combined precinct

Two or more precincts treated as a single precinct for a specific election.

commercial-off-the-shelf

Hardware or software components that are widely available for purchase and can be integrated into special-purpose systems.

Common Data Format

Standard and practice of creating and storing data in a common, described format that can be read by other systems.

Common Industry Format

Format used for usability test reporting. The format is described in ISO/IEC 25062:2006 "Common Industry Format (CIF) for Usability Test Reports," one of a group of usability standards. CIF is the format required for usability test reporting.

component

Element within a larger voting system.
confidentiality

Prevention of unauthorized disclosure of information.

configuration management

A continuous process of recording and maintaining consistent and reliable records pertaining to an organization's hardware and software composition, including software version control and hardware updates.

conformance

Fulfilling specified requirements by a product, process, or service.

conformance testing

Process of testing device or system of devices against the requirements specified in one or more standards. The outcomes of a conformance test are generally a pass or fail result, possibly including reports of problems encountered during the execution.

contest

A single decision or set of associated decisions being put before the voters (for example, the option of candidates to fill a particular public office or the approval or disapproval of a constitutional amendment). This term encompasses other terms such as "race," "question," and "issue" that are sometimes used to refer to specific kinds of contests. It does not refer to the legal challenge of an election outcome.

contest option

A votable choice that appears under a contest.

contest option position

A specified area on a ballot where a voter's selection in a particular contest can be indicated.

contest option vote

Vote that will be counted for a particular contest option. This term was previously referred to as valid vote.
contest selection

A selection made on the ballot by a voter with respect to a specific single contest (for example, a candidate, the value "Yes" or "Approve").

core logic

Subset of application logic that is responsible for vote recording and tabulation.

corrective action

Action taken to eliminate the causes of an existing deficiency or other undesirable situation in order to prevent it from recurring.

counted ballot

A read ballot that has been processed and whose votes are included in the vote totals.

cross-party endorsement

Endorsement of a single candidate or slate of candidates by more than one political party. The candidate or slate appears on the ballot representing each endorsing political party.

cryptographic end-to-end voting system

A voting system that supports both voter verification and election verification.

cryptographic hash

A cryptographic algorithm that computes a numerical value based on a data file or electronic message. The numerical value is used to represent that file or message, and depends on the entire contents of the file or message. A hash function can be considered to be a fingerprint of the file or message. Colloquially known as a hash, hash function, or digital fingerprint. Hashes provide integrity protection.

cryptographic key

A numeric value used as input to cryptographic operations, such as decryption, encryption, signature generation, or verification of a digital signature.
cryptography

Discipline that embodies the principles, means, and methods for transforming data to hide their semantic content, prevent their unauthorized use, prevent their undetected modification, or establish their authenticity.

cumulative voting

A vote variation used in multi-seat contests where a voter is permitted to distribute allowed selections to 1 or more candidates in whole vote increments.
cybersecurity

Measures taken to protect computer systems and data from attack and unauthorized access or use.
D:

decertification
Revocation of national or state certification of a voting system or any of its components.

decryption
Cryptographic process of transforming encrypted data back into its pre-encryption form.

defense-in-depth
Also called the "Castle" approach. Multiple levels of logical and physical security measures that deny a single point of security failure in a system. Examples include the combined use of passwords, encryption, lock-and-key access, security seals, and logs.

device
Physical apparatus and any supporting supplies, materials, and logic that together form a functional unit that performs assigned tasks as an integrated whole.

digital certificate
A data set used to identify the holder of the certification and to verify, using a PKI, the authenticity of the certificate. It typically includes the holder's private key and is used for cryptographic operations such as digitally signing or encrypting data.

digital signature
A cryptographic operation where the private key is used to digitally sign an electronic document and the public key is used to verify the signature. Digital signatures provide data authentication and integrity protection.

direct recording electronic voting machine
A vote-capture device that allows:

- electronic presentation of a ballot,
- electronic selection of valid contest options, and
- electronic storage of contest selections as individual records. It also provides a summary of these contest selections.

**dynamic password**

A password that changes at a defined interval or event.
E:

EAC

Election Assistance Commission, created by the Help America Vote Act (HAVA) to assist the states regarding HAVA compliance and to distribute HAVA funds to the states. The EAC is also charged with creating voting system guidelines and operating the federal government's first voting system certification program. The EAC is also responsible for maintaining the National Voter Registration form, conducting research, and administering a national clearinghouse on elections that includes shared practices, information for voters, and other resources to improve elections.

early voting

Voting that occurs prior to election day under the supervision of election workers.

early voting center

Physical location where individuals may cast a ballot before election day under the supervision of election workers.

elected office

An office that is filled primarily or exclusively via election.

election

A formal process in which qualified voters select candidates to fill seats in one or more offices and/or vote on one or more proposed ballot measures.

election certification

The act of confirming the final official results of a jurisdiction's election. This event occurs after results from valid ballots are tallied from all sources (election day, absentee voting, early voting, provisional ballots, etc.) and results are validated and approved by those legally responsible.
**election day**

The last day on which *voters* may **cast a ballot**. *Absentee ballots* and **early voting** ballots may be cast in advance of election day.

**election definition**

Data used in defining an **election**, including *election districts*, *contests*, *candidates*, and **ballot style** information.

**election definition medium**

Programmed memory *device* containing all applicable **election definition** data required by the **election system component** where the device will be used.

**election district**

Administrative area in which *voters* are entitled to **vote in contests** that are specific to that area.

**election jurisdiction**

A geographical area to which a practical authority has been granted to administer **elections** for political or administrative *offices*. Areas of jurisdiction apply to local, state, and federal levels. States, counties, cities, **towns**, and **townships** are all examples of jurisdictions.

**election management system**

Set of processing functions and databases within a **voting system** typically used to:

- develop and maintain **election definition** data,
- perform **ballot** layout functions,
- create ballot presentation templates for ballot printers or **devices** used by *voters* for ballot markup,
- count **votes**,
- consolidate and **report** results, and
- maintain **audit trails**.

**election official**

Any person who is involved with administering or conducting an **election**, including government personnel and temporary **election workers**. This may include any county clerk and recorder,
election judge, member of a canvassing board, central election official, election day worker, member of a board of county commissioners, member or secretary of a board of directors authorized to conduct public elections, representative of a governing body, or other person engaged in the performance of election duties as required by the election code.

election programming

Process by which election officials or their designees use voting system software to create the election definition and configure all election definition medium for use in a specific election.

election results report

A tabulation report produced after the closing of polls for the purpose of publicizing the vote counts.

Election Results Reporting System

A system that:

- aggregates and displays election results across the election jurisdiction,
- can be real-time or near real-time,
- can provide a variety of formats for displaying election results, and
- may provide direct feeds for the media.

election system

1. A technology-based system that is used to collect, process, and store data related to elections and election administration. In addition to voter registration systems and public election websites, election systems include voting systems, vote tabulation systems, electronic poll books, election results reporting systems, and auditing devices.
2. Entire array of procedures, people, resources, equipment, and locations associated with conducting elections.

election worker

Any person who interacts with those coming to vote. This includes any poll worker, election day worker, early voting worker, or other temporary staff engaged in supporting the voting or vote counting process.
electronic ballot delivery

The delivery of ballot and voter information packets electronically. The 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 election office to the registered UOCAVA voter.

electronic ballot interface

Subsystem within a voting system which communicates ballot information to a voter in video, audio, or other alternative format which allows the voter to select contest options using vocalization or physical actions.

electronic ballot return

The return of a voted ballot or voter information packet using electronic means. This can be by fax, email, or through the use of an Internet supported application. Sometimes referred to as "Internet Voting."

electronic device

Device that uses electronic or electromechanical components.

electronic poll book

Device that partially automates the process of checking in voters, assigning them the correct ballot style, and marking voters who have been issued a ballot. May be used in place of a traditional paper poll book. E-poll books can be stand alone at the precinct with a separate copy of the registration list or can be networked into a central voter registration system. They can check and update voter records in real time.

electronic voter interface

Component of an electronic vote-capture device that communicates ballot information to the voter and accepts contest selection input from the voter.

eligible voters

The universe of all voters who, if they cast a ballot, would have the legal right to have eligible contests on that ballot counted. This would include those who do not appear in the list of eligible voters because they live in a same-day registration or no registration state and did not or could not register ahead of time.
encryption

Cryptographic process of transforming data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used. Encryption provides confidentiality protection.

endorsement

Approval by a political party, for example, as the candidate that the party fields in a particular contest or as the candidate that should receive straight party votes. In some states, more than one party may endorse a candidate or contest option.

enhanced visual format

An alternative visual display format supporting personal choices such as text size, color contrast, and preferred language.

error correction code

Coding system that allows data being read or transmitted to be checked for errors and, when detected, corrects those errors.

error rate

Ratio of the number of errors that occur to the volume of data processed.

escalation of privilege

An attack on a system where the attacker is using some means to bypass security controls in order to attain a higher privilege level on the target system.

exhausted ballot

Refers to processing a ranked choice voting contest on a cast ballot, when that ballot becomes inactive and cannot be advanced in the tabulation for a contest because there are no further valid rankings on the ballot for continuing contest options.

expected mark

Mark that falls wholly or partially inside a contest option position.
Extensible Markup Language

A text-based language used to organize and present information on the World Wide Web.

extraneous mark

A mark on a paper ballot that appears to be unrelated to the act of indicating a voter's selection. Examples include: a mark made unintentionally by a voter that is obviously not related to making a selection; a hesitation mark, a dot within or outside of the target area made by resting a pen or pencil on the ballot; written notes or identifying information not related to indication of the voter's selection; or printing defects.
failure

Looking at voting system reliability, a failure is an event that results in:

- loss of one or more functions,
- degradation of performance resulting in a device that is unable to perform its intended function for longer than 10 seconds,
- automatic reset, restart, or reboot of the voting device, operating system or application software, requiring an unanticipated intervention by a person in the role of election worker or technician before normal operation can continue, or
- error messages or audit log entries indicating that a failure has occurred.

failure rate

Ratio of the number of failures that occur to the volume of data processed.

fault

Flaw in design or implementation that may result in the qualities or behavior of the voting system deviating from the qualities or behavior that are anticipated, including those specified in the VVSG or in manufacturer-provided documentation.

fault-tolerant

A system that continues to operate after the failure of a computer or network component.

Federal Information Processing Standards

Standards for federal computer systems developed by NIST. These standards are developed when there are no existing industry standards to address federal requirements for system interoperability, portability of data and software, and computer security.

finding

(n) Result of a formal evaluation by a test lab or accredited expert.
**firewall**

A gateway system designed to prevent unauthorized access to a private network or intranet that is connected to the internet. A firewall can be implemented in either hardware or software, or a combination of both.

**firmware**

A specific class of software encoded directly into a hardware device that controls its defined functions and provides the low-level control for the computer's specific hardware (such as the firmware that initially boots an operating system).

**Functional Configuration Audit**


**functional test**

Test performed to verify or validate the accomplishment of one or more functions.
**G:**

general election

Election in which all eligible voters, regardless of party affiliation, are permitted to select candidates to fill public office and/or vote on ballot measures.

Geographical Information System

A system designed to capture, store, manipulate, analyze, manage, and present all types of spatial or geographical data. GIS systems are used to validate voting district boundaries and may be integrated with the voter registration system.

Geopolitical Unit

Describes units of geopolitical geography so that they can be associated with contests, offices, ballot styles, and election results.
H:

hardware

The physical, tangible, mechanical, or electromechanical components of a system.

Help America Vote Act

Act passed by the U.S. Congress in 2002 to make sweeping reforms to the nation's voting process. HAVA addresses improvements to voting systems and voter access that were identified following the 2000 election.
implementation statement

Statement by a manufacturer indicating the capabilities, features, and optional functions as well as extensions that have been implemented. Also known as implementation conformance statement.

in-person voting

Voting that occurs in an official location under the supervision of election workers.

independently

Without assistance from an election worker or other person.

indirect selection

The mechanism by which a selection for a specific contest option automatically selects other linked contest options. An example is a straight party selection that causes indirect selections for all contest options of the identified party.

information security

Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.

inspection

Examination of a product design, product, process, or installation and determination of its conformity with specific requirements.

interaction mode

A specific combination of display format and control or navigation options that enable voters to perceive and interact with the voting system.
interoperability

The extent to which systems from different manufacturers and devices with different system configurations can communicate with each other.

Intrusion Detection System

A hardware or software application that detects and reports a suspected security breach, policy violation, or other compromise that may adversely affect the network.

Intrusion Prevention System

A hardware or software application that detects and blocks a suspected security breach, policy violation or other compromise that may adversely affect the network.
K:

key management

Activities involving handling of cryptographic keys and other related security parameters (such as passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, zeroization, and revocation.
L:

life cycle

Systems engineering concept that identifies the phases that a system passes through, from concept to retirement. There are different concerns and activities associated with each phase of the life cycle.

locality

Generic term used in election contexts to signify a town, village or city contained within an election jurisdiction, such as a county.

logic and accuracy testing

Equipment and system readiness tests whose purpose is to detect malfunctioning devices and improper election-specific setup before the equipment or systems are used in an election. Election officials conduct L&A tests prior to the start of an election as part of the process of setting up the system and the devices for an election according to jurisdiction practices and conforming to any state laws.

logic defect

Fault in software, firmware, or hardwired logic.

logical correctness

Condition signifying that, for a given input, a computer program will satisfy the program specification and produce the required output.
M:

machine unreadable mark
Mark in a contest selection position of a paper ballot that cannot be detected as readable or marginal by a scanner, and may require human adjudication.

machine-readable mark
Mark in a contest selection position of a paper ballot that meets requirements for detection by a scanner.

majority voting
A vote variation which requires the winning candidate to receive more than half of the votes cast. If no candidate wins an outright majority, a run-off election may be held between the top two vote-getters.

malware
Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of a system. For example, a virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malware.

manually-marked paper ballot
Paper ballot marked by a voter using a writing utensil. The paper ballot is the independent voter verifiable record.

manufacturer
Entity with ownership and control over a voting system submitted for testing.

marginally machine-readable mark
An intentional mark in a contest selection position of a paper ballot that does not meet the requirements for a reliably detectable selection, and therefore requires human adjudication. A marginal mark may be determined to indicate a selection, depending on state law.
marked ballot

**Ballot** that contains all of a **voter**'s selections.

military voter

A member of a uniformed service in active service, including army, navy, air force, marine corps, coast guard and merchant marine, and their spouses and dependents.

misfeed rate

Ratio of the misfeed total to the total **ballot** volume.

module

A structural unit of a software program that serves a specific function for the program or that serves to make the program modular in structure for the purposes of easier understanding and maintenance.

multi-factor authentication

**Authentication** mechanism requiring two or more of the following:

- something you know (such as a password),
- something you have (such as a **token**),
- something you are (for example, biometric authentication).

multi-seat contest

**Contest** in which multiple **candidates** are elected to fill a specified number of **seats**.

municipality

Term as used in **election** contexts to signify a jurisdiction such as city, **town**, or village that has some form of local government for which elections are generally conducted.
N:

N-of-M voting

Vote variation in which the voter is entitled to allocate a fixed number of votes (N) over a list of M contest options or write-in options, with the constraint that at most 1 vote may be allocated to a given contest option. This usually occurs when multiple seats are concurrently being filled in a governing body such as a city council or school board where candidates contend for at-large seats. The voter is not obliged to allocate all N votes. 1-of-M is N-of-M voting where N = 1.

national certification test report

Report of the results of independent testing of a voting system by a Voting System Test Lab (VSTL) delivered to the EAC with a recommendation about granting a certification number.

National Institute of Standards and Technology

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 EAC in developing testable standards for voting systems.

non-party-specific contest

Contest where eligibility to vote in that contest is independent of political party affiliation.

non-user-serviceable failure

Functional failure that requires the manufacturer or highly trained personnel to repair.

nonpartisan office

Elected office for which candidates appear on the ballot without political party designation.

nonpartisan primary

Primary election held to narrow the field of candidates in non-party-specific contests.

nonvolatile memory

Memory in which information can be stored indefinitely with no external power applied.
notice of clarification

Document providing further guidance and explanation on the requirements and procedures of the EAC’s Voting System Certification or Voting System Testing Lab (VSTL) programs. NOCs may be issued in response to a clarification request from a Voting System Test Lab or an EAC registered manufacturer. EAC may also issue NOCs when it determines general clarifications are necessary.
observational test

Operational test conducted on voting devices during an election by real voters to establish confidence that the voter verifiable paper record is produced correctly when assistive technology is used. Devices subjected to observational testing are used for normal collection of votes; the votes collected are included in the election tally.

office

A position established by law with certain associated rights and duties.

open primary

Partisan primary election in which the voter may choose a political party at the time of voting and vote in party-specific contests associated with that party, along with non-party-specific contests presented at the same election. Some states require voters to publicly declare their choice of party at the polling place, after which the election worker provides or activates the appropriate ballot. Other states allow the voters to make their choice of party within the privacy of the voting booth.

open source

Computer software with its source code (human readable code) made available with a license in which the copyright holder provides the rights to study, change, and distribute the software to anyone and for any purpose. Open source software may:

- be developed in a collaborative public manner;
- be reviewed by multiple professional and amateur programmers;
- require a fee and be licensed like other software;
- be fully open source or may have only a portion of the software open source.

optical scan

Voting system that counts votes marked in contest option positions on the surface of a paper ballot.
overseas voter

A U.S. citizen who is living outside of the United States and is eligible to vote in their last place of residence in the United States.

overvote

Occurs when the number of selections made by a voter in a contest is more than the maximum number allowed.
P:

paper ballot
A piece of paper, or multiple sheets of paper, on which all contest options of a given ballot style are printed.

paper ballot sheet
A single piece of paper that forms part of a paper ballot. Paper ballots may contain multiple sheets.

paper ballot side
The face of a paper ballot sheet. A paper ballot may have two sides.

partisan office
Elected office for which candidates may appear on the ballot with a political party designation.

partisan primary
Primary election held to narrow the field of candidates in party-specific contests.

party-specific contest
Contest where eligibility to vote in that contest is restricted based on political party affiliation or lack of any affiliation. The affiliation might be the registered affiliation of the voter or it might be an affiliation declared at the time of voting.

pattern voting
Selecting contest options across multiple contests in a predetermined pattern intending to signal one's identity to someone else. The possibility of pattern voting can be an issue for publishing Cast Vote Records (CVR) because it may compromise voter privacy if there are enough selections in each published CVR to make it likely a selection pattern might be unique.

penetration testing
An evaluation method that enables researchers to search for vulnerabilities in a system.
personal assistive device

Assistive technology belonging to voters rather than any supplied with the voting system.

Personal Identifiable Information

Any information about an individual maintained by an agency, including:

- information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and
- any other information that can be linked to an individual, such as medical, educational, financial, and employment information.

Physical Configuration Audit

Inspection by a voting system test lab (VSTL) that compares the voting system components submitted for certification testing to the manufacturer's technical documentation and confirms that the documentation submitted meets the national certification requirements. Includes witnessing the executable system being built to ensure that the certified release is built from the tested components.

plurality voting

A vote variation in which the candidate with the most votes wins, without necessarily receiving a majority of votes.

political party

An association of individuals under whose name a candidate may appear on a ballot. # political subdivision Any unit of government, such as counties, cities, school districts, and water and conservation districts having authority to hold elections for public offices or on ballot measures.

polling location

Physical address of a polling place.

polling place

Location at which voters may cast in-person ballots under the supervision of election workers during one or more specific time periods.
post-election audit

Hand-counting votes on paper records, then comparing those counts to the corresponding vote totals originally reported:

- as a check on the accuracy of election results, and
- to resolve discrepancies using accurate hand counts of the paper records as the benchmark.

precinct

Election administration division corresponding to a geographic area that is the basis for determining which contests the voters legally residing in that area are eligible to vote on.

precinct count

Counting ballots in the same precinct in which those ballots have been cast.

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.

presentable ballot style

Ballot style that includes all presentational details required to generate a ballot. This may include language, ordering of contests and candidates, and structural content such as headers.

presidential primary election

Primary election in which voters choose the delegates to the presidential nominating conventions allotted to their states by the national party committees.

primary election

Election held to determine which candidates qualify to appear as contest options in subsequent elections.

privacy (for voters)

A property of a voting system that is designed and deployed to enable voters to obtain a ballot, and mark, verify, and cast it without revealing their ballot selections or selections of language,
display and **interaction modes** to anyone else. This does not preclude the ability of a voter to request assistance under state law.

**private key**

The secret part of an asymmetric key pair that is typically used to verify, digitally sign, or decrypt data.

**product standard**

**Standard** that specifies requirements to be fulfilled by a product or a group of products, to confirm it can perform its intended task.

**programmed device**

**Electronic device** that includes software. Most electronic **voting devices** include application logic (software) and are, therefore, programmed devices.

**proportional voting**

A **vote variation** used in **multi-seat contests** where the **votes** allowed in the **contest** are distributed to the selected **candidates** proportionally depending on the number of selections. This may result in candidates receiving fractional votes.

**provisional ballot**

A failsafe **ballot** provided to a **voter** whose eligibility for a regular ballot cannot be immediately determined. The ballot may be counted or further processed depending on state law.

**public key**

Public part of an asymmetric key pair that is typically used to verify **digital signatures** or encrypt data.

**Public Key Infrastructure**

A set of roles, policies, and procedures used to establish greater trust in the authenticity of a **digital certificate** and for use in creating, managing, distributing, using, storing, and revoking digital certificates.
public test

An abbreviated logic and accuracy test of voting equipment, pre-announced in public media and open to public attendance, usually in conformance with specific election calendar timing.
QR Code

Quick Response Code. A 2-D, trademarked bar code. Some voting systems will encode the voter's selections in a QR Code that can be read on a scanner in the precinct and converted to a printed ballot.


**R:**

range voting

A *vote variation* for single-seat *contests*, in which *voters* give each *candidate* a score, the scores are added (or averaged), and the candidate with the highest total is elected.

ranked choice voting

A *vote variation*:

- which allows each *voter* to rank *contest options* in order of the voter's preference,
- in which *votes* are counted in rounds using a series of runoff tabulations to defeat contest options with the fewest votes, and,
- which elects a winner with a majority of final round votes in a single-winner *contest* and provides proportional representation in multi-winner contests.

read ballot

*Cast ballot* that has been successfully accepted and initially processed.

recall issue with options

*Vote variation* that allows *voters* to remove elected representatives from *office* before their terms of office expire. The recall may involve not only the question of whether a particular officer should be removed, but also the question of naming a successor in the event that there is an affirmative *vote* for the recall.

recallable ballot

*Recorded ballot* that can be individually retrieved and included or excluded from further processing.

recertification

Re-examination, and possibly retesting, of a *voting system* that was modified after being previously certified. The object of recertification is to determine if the system as modified still conforms to the requirements.
record

(n) Preserved evidence of activities performed or results achieved (for example, forms, reports, test results).

(o) To create a record.

recorded ballot

A ballot for which there is an associated cast vote record.

recount

Repeat tabulation of votes cast in an election, whether manually or electronically, that is used to determine the accuracy of an initial count.

report

Self-contained, time-stamped, archival record, such as a printout or analogous electronic file that is produced at a specific time and subsequently protected from modification.

report total error rate

Ratio of the report total error to the report total volume.

reporting unit

Geographical area in which reported totals or counts are reported (for example, an election jurisdiction, precinct, or election district).

reproducibility

Ability to obtain the same test results by using the same test method on identical test items in different testing laboratories with different operators using different equipment.

residual vote

Vote that could not be allocated to a specific contest due to an undervote or overvote.

reviewed ballot

Ballot that has been reviewed (either electronically or by the voter) before it is cast, to determine what contest selections it contains.
risk assessment

The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and safeguards that would mitigate this impact.

risk-limiting audit

Procedure for checking a sample of ballots (or voter verifiable records) that is guaranteed to have a large, pre-specified chance of correcting the reported outcome if the reported outcome is wrong (that is, if a full hand count would reveal an outcome different from the reported outcome).

runoff election

\textbf{Election} to select a winner following a primary election or a general election, in which no candidate in the contest received the required minimum percentage of the votes cast. The two candidates receiving the most votes for the contest in question proceed to a runoff election.
S:

seat

An elected office position that a single officeholder may occupy for a term of office.

second chance voting

Feature of a voter facing scanner that reviews the ballot for possible marking mistakes, informs the voter, and presents an opportunity to cast as-is or return the ballot.

security analysis

An inquiry into the potential existence of security flaws in a voting system. Includes an analysis of the system's software, firmware, and hardware, as well as the procedures associated with system development, deployment, operation, and management.

security controls

Management, operational, and technical controls (that is, safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

security strength

A metric associated with the amount of work (that is, the number of operations) that is required to break a cryptographic algorithm or system.

software independence

Quality of a voting system or voting device where a previously undetected change or fault in software cannot cause an undetectable change or error in election outcome.

source code

Human readable computer instructions that, when compiled or interpreted, define the functionality of a programmed device. Source code can be written by humans or by computers.
spear phishing

A targeted attack by hackers, using bogus emails, that attempts to get the victim to provide login information or personal information to the hackers. Spear Phishing attempts may appear to originate from legitimate, known sources, such as organizational IT or known vendors.

special election

Primary election or general election that is not regularly scheduled. A special election may be combined with a scheduled election.

spoil

(A ballot) To mark or otherwise alter a ballot so it indicates in a human-readable manner that the ballot is not to be cast.

spoiled ballot

A ballot that has been issued to a voter but will not be cast, usually because it has been incorrectly marked or impaired in some way.

standard

A document that provides requirements, specifications, guidelines, or characteristics that can be used consistently to ensure that materials, products, processes, and services are fit for their purpose.

straight party override

Explicit voter selection that overrides or supplements the vote selections made by a straight party voting option. Straight party overrides may be subject to state election rules for how they work or whether they are allowed.

straight party voting

Mechanism that allows voters to cast a single vote to select all candidates on the ballot from a single political party.

street segment data

The portion of a street between two consecutive cross streets that can be assigned to a precinct.
support software

Software that aids in developing, maintaining, or using other software, for example, compilers, loaders and other utilities.

symmetric cryptography

Encryption system that uses the same key for encryption and decryption. This key must be kept secret.

system extent

Administrative unit that is the entire scope within which the voting system is used (for example, a county). The system extent corresponds to the top-level reporting context for which the system generates reports.
**t**:  

**t-coil**  
Inductive coil used in some hearing aids to allow reception of an audio band magnetic field signal instead of an acoustic signal. The magnetic or inductive mode of reception is commonly used in conjunction with telephones, auditorium loop systems, and other systems that provide the required magnetic field output.

**tabulate**  
Process of totaling votes.

**tabulation report**  
A report containing the counts associated with ballots tabulated for a given election district.

**tactile controls**  
Tactile controls are discernable or perceptible by touch using hands, feet, or other parts of the body. (Does not include touch screens.) Dual switches are a form of tactile controls that can be used by voters with minimal use of their hands.

**technical data package**  
Manufacturer documentation relating to the voting system, which can include manuals, description of components, and details of architectural and engineering design.

**test**  
Procedure used to determine one or more characteristics of a given product, process, or service according to a specified procedure for conformity assessment. A test may be an operational test or a non-operating test (for example, an inspection).

**test deck**  
A set of marked ballots with a predetermined outcome. Used for logic and accuracy testing of a voting system.
test method

Specified technical procedure for performing a test, procedures by which tests are derived, or a combination of these.

test plan

Document created prior to testing that outlines the scope and nature of testing, items to be tested, test approach, resources needed to perform testing, test tasks, risks, and schedule.

test suite

Implementation of a set of operational tests for a particular object (such as a specific voting system) or class of objects (such as all voting systems that can interpret the language in which the test data are expressed).

third-party logic

Software, firmware, or hardwired logic that is neither application logic nor COTS. This includes, for example, general-purpose software developed by a third party that is either customized (for example, ported to a new platform, as is Windows Embedded Compact), not widely used, or source-code generated by a COTS package.

token

Something a user possesses and controls, typically a key or password, that is used to authenticate an identity.

touch screen voting machine

A vote-capture device that utilizes a computer screen to display the ballot and allows the voter to indicate their selections by touching designated locations on the screen.

town

An urban area that has a name, defined boundaries, and local government, and that is generally larger than a village and smaller than a city. Term used in New England, New York, and Wisconsin to refer to the equivalent of the civil township in these states.
township

A widely used unit of local government in the United States, subordinate to a county, with some form of local government for which it generally conducts elections.

U:

undervote

Occurs when the number of voter selections in a contest is less than the maximum number allowed for that contest or when no selection is made. The number of undervotes is equal to the number of votes lost, for example, if no selection is made in a vote for two contest the number of votes lost is two.

Uniformed and Overseas Citizens Absentee Voting Act

Act of Congress in 1986 requiring that the states and territories allow certain groups of citizens to register and vote absentee in elections for Federal offices.

UOCAVA voter

An overseas voter or an active duty member of the U.S. military, either within or outside the United States, including any accompanying spouse and family members who are eligible to vote in their last place of residence in the United States. The Uniformed and Overseas Citizens Absentee Voting Act is commonly referred to as UOCAVA.

usability

Effectiveness, efficiency, and satisfaction with which a specified set of users can achieve a specified set of tasks in a particular environment. Usability in the context of voting refers to voters being able to cast valid votes as they intended quickly, without errors, and with confidence that their contest selections were recorded correctly. It also refers to the usability of the setup and operation of voting equipment in the polling place.

usability testing

Testing that encompasses a range of methods that examine how users in the target audience actually interact with a system, in contrast to analytic techniques such as usability inspection.
user-serviceable failure

Functional failure that can be remedied by a troubleshooter or election official using only knowledge found in voting equipment user documentation.
V:

valid vote

See contest option vote.

validation

Process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements.

visual format

A display format in which contest options and other information are displayed on screen or paper for perception using sight.

vote

Indication of support for a particular contest option.

vote center

A physical location where voters from multiple precincts may cast their ballots.

vote for N of M

A multi-seat contest in which voters are allowed to vote for a specified number ("N") of candidates.

vote variation

Voting style or feature, including but not limited to the following: approval voting, borda count, cumulative voting, n-of-m voting, plurality voting, proportional voting, range voting, ranked choice voting and super majority voting.

vote-by-mail

Method of voting by which eligible voters are mailed ballots and information packets by the local election jurisdiction. Voters may be able to return their marked ballots by mail, bring them to an election office, or drop them off in secure drop boxes.
vote-capture device

An electronic voting device that is used directly by a voter to make selections on a ballot.

voter

Person permitted to cast a ballot.

voter facing scanner

An electronic voting device that:

• accepts hand-marked or BMD-produced paper ballots one sheet at a time;
• is usually used for in-person voting;
• permits election workers to open and close the polls;
• scans a ballot and rejects it if either unreadable or un-processable;
• detects, interprets and validates contest selections;
• notifies the voter of voting exceptions (such as undervotes or overvotes) or unreadable marks;
• stores accepted ballots in a secure container;
• sorts or otherwise marks ballots or ballot images that need subsequent human review;
• and tabulates and reports contest results after polls are closed.

This unit was previously referred to as precinct count optical scanner or PCOS.

voter intent

A cognitive construct, formed by the voter, that they attempt to express through actions taken to mark, verify, and cast the issued ballot.

voter intent standard

A standard for counting ballots that aims to ensure that ballots are counted in accordance with the goals of the voter, using written rules for both human processes and machine algorithms to ensure that all ballots marked in a similar way are counted in the same way.

voter verifiable

A voting system feature that provides the voter an opportunity to verify that their contest selections are being recorded correctly before the ballot is cast.
voter verified paper audit trail

A paper document that the voter can review before officially casting their ballot.

voting device

Device that is part of the voting system.

voting process

Entire array of procedures, people, resources, equipment, and locations associated with conducting elections.

voting session

A collection of activities including ballot issuance, voter interaction with the vote-capture device, voting, verification, and casting.

voting station

The location within a polling place where voters may record their votes. A voting station includes the area, location, booth, or enclosure where voting takes place.

voting system

Equipment (including hardware, firmware, and software), materials, and documentation used to define elections and ballot styles, configure voting equipment, identify and validate voting equipment configurations, perform logic and accuracy tests, activate ballots, capture votes, count votes, reconcile ballots needing special treatment, generate reports, transmit election data, archive election data, and audit elections.

voting system software

The executable code and associated configuration files needed for the proper operation of the voting system.

Voting System Test Lab

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 (NIST).
W:

white box testing

*Testing* based on an analysis of the internal structure of the *component* or system.

Wi-Fi

A *wireless* networking technology that uses radio waves to provide high-speed Internet network connections.

Wide Area Network

A network that connects computers across metropolitan, regional, and national boundaries. The internet is an example of a WAN.

wireless

Network connectivity using radio waves instead of wire connections.

write-in option

A type of *contest option* that allows a *voter* to specify a *candidate*, usually not already listed as a contest option. Depending on *election jurisdiction* rules, in some cases only previously approved names will be considered as valid write-in *contest selections*. 
Z:

zero report

A tabulation report produced at the opening of polls to check that there are no stored votes.
Appendix B
Requirements Listing
Appendix B: Requirements Listing

The VVSG 2.0 - Principles and Guidelines

Principle 1: High Quality Design
Principle 2: High Quality Implementation
Principle 3: Transparent
Principle 4: Interoperable
Principle 5: Equivalent and Consistent Voter Access
Principle 6: Voter Privacy
Principle 7: Marked, Verified, and Cast as Intended

Principle 8: Robust, Safe, Usable, and Accessible
Principle 9: Auditable
Principle 10: Ballot Secrecy
Principle 11: Access Control
Principle 12: Physical Security
Principle 13: Data Protection
Principle 14: System Integrity
Principle 15: Detection and Monitoring
Principle 1: High Quality Design

The voting system is designed to accurately, completely, and robustly carry out election processes.

1.1 – The voting system is designed using commonly-accepted election process specifications.

1.1.1 – Election definition
  1.1.1-A – Election definition
  1.1.1-B – Election definition details
  1.1.1-C – Define political geographies
  1.1.1-D – Serve multiple or split precincts and election districts
  1.1.1-E – Identifiers
  1.1.1-F – Definition of parties and contests
  1.1.1-G – Voting methods
  1.1.1-H – Election definition accuracy
  1.1.1-I – Voting options accuracy
  1.1.1-J – Confirm recording of election definition
  1.1.1-K – Election definition distribution
  1.1.1-L – Define ballot styles
  1.1.1-M – Auto-format
  1.1.1-N – Include contests
  1.1.1-O – Exclude contests
  1.1.1-P – Nonpartisan formatting
  1.1.1-Q – Jurisdiction-dependent content
  1.1.1-R – Primary elections, associate contests with parties
  1.1.1-S – Ballot rotation
  1.1.1-T – Ballot configuration in combined or split precincts
  1.1.1-U – No advertising
  1.1.1-V – Ballot style distribution
  1.1.1-W – Ballot style identification
  1.1.1-X – Retaining, modifying, reusing definitions
  1.1.1-Y – Ballot style protection
  1.1.1-Z – Data inputs and outputs

1.1.2 – Equipment setup
  1.1.2-A – Equipment setup
  1.1.2-B – Built-in self-test and diagnostics
  1.1.2-C – Verify proper preparation of ballot styles
  1.1.2-D – Verify proper installation of ballot styles
  1.1.2-E – Verify compatibility between software and ballot styles
  1.1.2-F – Test ballots
  1.1.2-G – Test all ballot positions
  1.1.2-H – Test Cast Vote Records
  1.1.2-I – Test codes and images
  1.1.2-J – Testing calibration
  1.1.2-K – Ballot marker readiness
  1.1.2-L – L&A testing, no side-effects
  1.1.2-M – Status and readiness reports
  1.1.2-N – Pre-election reports
  1.1.2-O – Readiness reports for each polling place
  1.1.2-P – Readiness reports, precinct tabulation
  1.1.2-Q – Readiness reports, central tabulation
  1.1.2-R – Readiness reports, public network test ballots

1.1.3 – Opening the Polls
  1.1.3-A – Opening the polls
  1.1.3-B – Verify L&A performed
  1.1.3-C – Prevent opening the polls
  1.1.3-D – Non-zero totals
  1.1.3-E – Scanners and ballot marking devices - verify activation
  1.1.3-F – Scanners and ballot marking devices - enter voting mode

1.1.4 - Ballot Activation
  1.1.4-A – Ballot activation
  1.1.4-A.1 – One cast ballot per session
  1.1.4-A.2 – Contemporaneous record
  1.1.4-A.3 – Control ballot configuration

1.1.5 - Casting
  1.1.5-A – Voting methods when casting
  1.1.5-B – N-of-M voting
  1.1.5-C – Yes/no measures and multiple-choice measures
  1.1.5-D – Indicate party affiliations and endorsements
  1.1.5-E – Closed primaries
  1.1.5-F – Open primaries
  1.1.5-G – Write-ins
  1.1.5-H – Write-in reconciliation
  1.1.5-I – Ballot rotation for contest options
  1.1.5-J – Straight party voting
  1.1.5-K – Cross-party endorsement
  1.1.5-L – Precinct splits
  1.1.5-M – Cumulative voting
  1.1.5-N – Ranked choice voting
  1.1.5-O – Recallable ballots
1.2 – The voting system is designed to function correctly under real-world operating conditions.

1.2-A – Assessment of accuracy
1.2-A.1 – Minimum ballot positions
1.2-A.2 – Ballot position distribution

1.2-B – Assessment of reliability
1.2-B.1 – Continuous operation – typical environmental conditions
1.2-B.2 – Continuous operation – varied environmental conditions
1.2-B.3 – Failure Modes and Effect Analysis (FEMA)
1.2-C – No single point of failure

1.2-D – Protect against failure of input and storage devices
1.2-E – Reliably detectable marks
1.2-F – Misfeed rate benchmark
1.2-G – Respond gracefully to stress of system limits
1.2-H – Handle realistic volume

1.3 – Voting system design supports evaluation methods enabling testers to clearly distinguish systems that correctly implement specified properties from those that do not.

1.3-A – Identifiability of basic and compound system components
1.3-B – Comprehensible processes that form system configurations
1.3-C – Observable configurations via plausible observation methods

1.3-D – Identifiable resolution limits for observation methods
1.3-E – Description of observational noise and consequences for observational methods
1.3-F – Explicitly-stated performance criteria
1.3-G – Creation and execution of evaluation methods
Principle 2: High Quality Implementation

The voting system is implemented using high quality best practices.

2.1 - The voting system software is implemented using trustworthy materials and best practices in software development.

2.1-A – Acceptable programming languages
2.1-B – COTS language extensions are acceptable
2.1-C – Acceptable coding conventions
2.1-D – Records last at least 22 months

2.1.1 – Workmanship

2.1.1-A – General build quality
2.1.1-B – High quality products
2.1.1-C – High quality parts

2.1.2 – Maintainability

2.1.2-A – Electronic device maintainability
2.1.2-B – System maintainability
2.1.2-C – Nameplate and labels

2.2 – The voting system is implemented using best practice user-centered design methods that consider a wide range of representative voters, including those with and without disabilities, and election workers.

2.2-A – User-centered design process

2.3 - Voting system logic is clear, meaningful, and well-structured.

2.3-A – Block-structured exception handling
2.3-B – Legacy library units
2.3-C – Separation of code and data
2.3-D – Hard-coded passwords and keys

2.3.1 – Software flow

2.3.1-A – Unstructured control flow
2.3.1-B – Goto
2.3.1-C – Intentional exceptions
2.3.1-D – Unstructured exception handling

2.4 - Voting system structure is modular, scalable, and robust.

2.4-A – Modularity
2.4-B – Module testability

2.4-C – Module size and identification
2.4-D – Lookup tables in separate files

2.5 - The voting system supports system processes and data with integrity.

2.5-A – Self-modifying code
2.5-B – Unsafe concurrency

2.5.1 – Code integrity

2.5.1-A – COTS compilers
2.5.1-B – Interpreted code, specific COTS interpreter
2.5.1-C – Prevent tampering with code
2.5.1-D – Prevent tampering with data

2.5.2 – Input/output errors

2.5.2-A – Monitoring and defending for I/O errors

2.5.2-B – Validate and filter input
2.5.2-C – Detect garbage input
2.5.2-D – Defend against garbage input

2.5.3 – Output protection

2.5.3-A – Escaping and encoding output
2.5.3-B – Sanitize output
2.5.3-C – Stored injection

2.5.4 – Error handling

2.5.4-A – Mandatory internal error checking
2.5.4-B – Array overflows
2.5.4-C – Buffer overflows
2.5.4-D – CPU traps
2.5.4-E – Garbage input parameters
2.5.4-F – Numeric overflows
2.5.4-G – Uncontrolled format strings
2.5.4-H – Recommended internal error checking
2.5.4-I – Pointers
2.5.4-J – Memory mismanagement
2.5.4-K – Nullify freed pointers
2.5.4-L – React to errors detected
2.5.4-M – Election integrity monitoring
2.5.4-N – SQL injection
2.5.4-O – Parameterized queries

2.6 - The voting system handles errors robustly and gracefully recovers from failure.
2.6-A – Surviving device failure
2.6-B – No compromising voting or audit data
2.6-C – Surviving component failure
2.6-D – Controlled recovery
2.6-E – Nested error conditions
2.6-F – Reset CPU error states
2.6-G – Coherent checkpoints

2.7 - The voting system performs reliably in anticipated physical environments.
2.7-A – Ability to function in physical environment (non-operating)
2.7-B – Ability to support maintenance and repair physical environment conditions
2.7-C – Ability to support transport and storage physical environment conditions
2.7-D – Ability to support storage temperatures in physical environment
2.7-E – Ability to support storage humidity levels in physical environment
2.7-F – Ability to operate as intended in physical environment
2.7-G – Ability to operate as intended at low and high temperatures
2.7-H – Ability to operate as intended at specified humidity conditions
2.7.1 – Ability to withstand electrical disturbances
2.7.1-A – Electrical disturbances
2.7.1-B – FCC Part 15 Class A and B conformance
2.7.1-C – Power supply from energy service provider
2.7.1-D – Power port connection to the facility power supply
2.7.1-E – Leakage from grounding port
2.7.1-F – Outages, sags, and swells
2.7.1-G – Withstand conducted electrical disturbances
2.7.1-H – Emissions from other connected equipment
2.7.1-I – Electrostatic discharge immunity
2.7.1-J – Radiated radio frequency emissions
Principle 3: Transparent

The voting system and voting processes are designed to provide transparency.

3.1 – The documentation describing the voting system design, operation, accessibility features, security measures, and other aspects of the voting system can be read and understood.

3.1.1 – System overview
   3.1.1-A – System overview documentation
   3.1.1-B – System overview, functional diagram
   3.1.1-C – System description
   3.1.1-D – Identify software and firmware by origin
   3.1.1-E – Traceability of procured software

3.1.2 – System performance
   3.1.2-A – System performance
   3.1.2-B – Maximum tabulation rate
   3.1.2-C – Reliably detectable marks
   3.1.2-D – Processing capabilities

3.1.3 – System security documentation
   3.1.3-A – System security
   3.1.3-B – Access control implementation
   3.1.3-C – Physical security
   3.1.3-D – Audit Procedures
   3.1.3-E – Risk Analysis

3.1.4 – Software Installation
   3.1.4-A – Software installation
   3.1.4-B – Software information
   3.1.4-C – Software location information
   3.1.4-D – Election specific software identification
   3.1.4-E – Installation software and hardware
   3.1.4-F – Software installation procedure
   3.1.4-G – Compiler installation prohibited
   3.1.4-H – Baseline binary image creation
   3.1.4-I – Programmed device configuration replication
   3.1.4-J – Software installation record creation
   3.1.4-K – Procurement of voting system software
   3.1.4-L – Open market procurement of COTS software
   3.1.4-M – Erasable storage media preparation
   3.1.4-N – Unalterable storage media

3.1.5 – System operations
   3.1.5-A – Operations manual
   3.1.5-B – Support training
   3.1.5-C – Functions and modes
   3.1.5-D – Roles
   3.1.5-E – Conditional actions
   3.1.5-F – References
   3.1.5-G – Operational environment
   3.1.5-H – Readiness testing
   3.1.5-I – Features
   3.1.5-J – Operating procedures
   3.1.5-K – Support
   3.1.5-L – Transportation

3.1.6 – System Maintenance
   3.1.6-A – System maintenance manual
   3.1.6-B – General contents
   3.1.6-C – Maintenance viewpoint
   3.1.6-D – Equipment overview details
   3.1.6-E – Maintenance procedures
3.1.6-F – Preventive maintenance procedures
3.1.6-G – Troubleshooting procedures
3.1.6-H – Troubleshooting procedure details
3.1.6-I – Special equipment
3.1.6-J – Parts and materials
3.1.6-K – Approved parts list
3.1.6-L – Marking devices
3.1.6-M – Approved manufacturers
3.1.6-N – Ballot stock specification
3.1.6-O – Ballot stock specification criteria
3.1.6-P – Printer paper specification
3.1.6-Q – System maintenance, maintenance environment
3.1.6-R – System maintenance, maintenance support and spares

3.1.7 – Training material
3.1.7-A – Training requirements
3.1.7-B – Personnel
3.1.7-B – User functions versus manufacturer functions
3.1.7-C – Training requirements

3.2 – The processes and transactions, both physical and digital, associated with the voting system are readily available for inspection.
3.2-A – Setup inspection process
3.2-B – Minimum properties included in the setup inspection process
3.2-C – Setup inspection record generation
3.2-D – Installed software identification procedure
3.2-E – Software integrity verification procedure
3.2-F – Election information value
3.2-G – Maximum and minimum values of election information storage locations
3.2-H – Variable value inspection procedure
3.2-I – Backup power operational range
3.2-J – Backup power inspection procedure
3.2-K – Cabling connectivity inspection procedure
3.2-L – Communications operational status inspection procedure
3.2-M – Communications on/off status inspection procedure
3.2-N – Quantity of voting equipment
3.2-O – Consumable inspection procedure
3.2-P – Calibration of voting device components
3.2-Q – Checklist of properties to be inspected

3.3 – The public can understand and verify the operations of the voting system throughout the entirety of the election.
3.3-A – System security, system event logging
3.3-B – Specification of common data format usage
3.3-C Bar and other codes
3.3-D Encodings
3.3-E Audit
Principle 4: Interoperable

The voting system is designed to support interoperability in its interfaces to external systems, its interfaces to internal components, its data, and its peripherals.

4.1 – Voting system data that is imported, exported, or otherwise reported, is in an interoperable format.

4.1-A – Data export and exchange format
4.1-B – Election programming data input and output
4.1-C – Tabulator report data
4.1-D – Exchange of cast vote records (CVRs)

4.1-E – Exchange of voting device election event logs
4.1-F – Voting device event code documentation
4.1-G – Specification of common format usage

4.2 - Standard, publicly-available formats for other types of data not addressed by NIST CDF specifications are used.

4.2-A – Standard formats
4.2-B – Public documented manufacturer formats

4.3 - Widely-used hardware interfaces and communications protocols are used.

4.3-A – Standard device interfaces

4.4 - Commercial-off-the-shelf (COTS) devices can be used if they meet all applicable VVSG requirements.

4.4-A – COTS devices meet applicable requirements
Principle 5: Equivalent and Consistent

All voters can access and use the voting system regardless of their abilities, without discrimination.

5.1 – Voters have a consistent experience throughout the voting process within any method of voting.

5.1-A – Interaction modes
5.1-B – Languages
5.1-C – Vote records

5.1-D – Accessibility features
5.1-E – Reading paper ballots
5.1-F – Accessibility documentation

5.2 – Voters receive equivalent information and options in all modes of voting.

5.2-A – No bias
5.2-B – Presenting content in all languages
5.2-C – Information in all modes

5.2-D – Audio synchronized
5.2-E – Sound cues
5.2-F – Preserving votes
Principle 6: Voter Privacy

_Voters can mark, verify, and cast their ballot privately and independently._

6.1 - The voting process preserves the privacy of the voter’s interaction with the ballot, modes of voting, and vote selections.

- 6.1-A – Preserving privacy for voters
- 6.1-B – Warnings
- 6.1-C – Enabling or disabling output
- 6.1.D – Audio privacy

6.2 - Voters can mark, verify, and cast their ballot or other associated cast vote record without assistance from others.

- 6.2-A - Voter Independence
Principle 7: Marked, Verified, and Cast as Intended

Ballots and vote selections are presented in a perceivable, operable, and understandable way and can be marked, verified, and cast by all voters.

7.1 – The default voting system settings present a ballot usable for the widest range of voters, and voters can adjust settings and preferences to meet their needs.

7.1-A – Reset to default settings
7.1-B – Reset by voter
7.1-C – Default contrast
7.1-D – Contrast options
7.1-E – Color conventions
7.1-F – Using color
7.1-G – Text size (electronic display)
7.1-H – Scaling and zooming (electronic display)
7.1-I – Text size (paper)
7.1-J – Sans-serif font
7.1-K – Audio settings
7.1-L – Speech frequencies
7.1-M – Audio comprehension
7.1-N – Tactile keys
7.1-O – Toggle keys
7.1-P – Identifying controls

7.2 – Voters and election workers can use all controls accurately, and voters have direct control of all ballot changes.

7.2-A – Display and interaction options
7.2-B – Navigation between contests
7.2-C – Voter control
7.2-D – Scrolling
7.2-E – Touchscreen gestures
7.2-F – Voter speech
7.2-G – Voter control of audio
7.2-H – Accidental activation
7.2-I – Touch area size
7.2-J – Paper ballot target areas
7.2-K – Key operability
7.2-L – Bodily contact
7.2-M – No repetitive activation
7.2-N – System response time
7.2-O – Inactivity alerts
7.2-P – Floor space
7.2-Q – Physical dimensions
7.2-R – Control labels visible

7.3 – Voters can understand all information as it is presented, including instructions, messages from the system, and error messages.

7.3-A – System-related errors
7.3-B – No split contests
7.3-C – Contest information
7.3-D – Consistent relationship
7.3-E – Feedback
7.3-F – Correcting the ballot
7.3-G – Full ballot selections review
7.3-H – Overvotes
7.3-I – Undervotes
7.3-J – Notification of casting
7.3-K – Warnings, alerts, and instructions
7.3-L – Icon labels
7.3-M – Identifying languages
7.3-N – Instructions for voters
7.3-O – Instructions for election workers
7.3-P – Plain language
Principle 8: Robust, Safe, Usable, and Accessible

The voting system and voting processes provide a robust, safe, usable, and accessible experience.

8.1 – The voting system’s hardware, software, and accessories are robust and do not expose users to harmful conditions.

8.1-A – Electronic display screens
8.1-B – Flashing
8.1-C – Personal Assistive Technology (PAT)
8.1-D – Secondary ID and biometrics
8.1-E – Standard audio connectors
8.1-F – Discernable audio jacks
8.1-G – Telephone style handset
8.1-H – Sanitized headphones
8.1-I – Standard PAT jacks
8.1-J – Hearing aids
8.1-K – Eliminating hazards

8.2 – The voting system meets currently accepted federal standards for accessibility.

8.2-A – Federal standards for accessibility

8.3 – The voting system is evaluated with a wide range of representative voters, including those with and without disabilities, for effectiveness, efficiency, and satisfaction.

8.3-A – Usability tests with voters

8.4 – The voting system is evaluated for usability by election workers.

8.4-A – Usability tests with election workers
Principle 9: Auditable

The voting system is auditable and enables evidence-based elections.

9.1 - An error or fault in the voting system software or hardware cannot cause an undetectable change in election results.

9.1.1 – Software independence
9.1.1-A – Software independent
9.1.1-B – Paper-based or cryptographic E2E system
9.1.1-C – Mechanism documentation

9.1.2 – Tamper evidence
9.1.2-A – Tamper evident records
9.1.2-B – Tamper-evident record creation

9.1.3 – Voter verification
9.1.3-A – Records for voter verification
9.1.3-B – Identification of errors
9.1.3-C – Ballot error correction
9.1.3-D – Voter reported errors

9.1.4 – Auditable
9.1.4-A – Auditor verification
9.1.4-B – Auditable with compromised software, firmware, or hardware
9.1.4-C – Documented procedure

9.1.5 – Paper records
9.1.5-A – Paper record production
9.1.5-B – Paper record retention
9.1.5-C – Paper record intelligibility
9.1.5-D – Matching selections
9.1.5-E – Paper record transparency and interoperability

9.1.6 – E2E Cryptography
9.1.6-A – Cryptographic E2E transparency
9.1.6-B – Cryptographic verification
9.1.6-C – Ballot receipt
9.1.6-D – Receipt export
9.1.6-E – Mandatory ballot availability
9.1.6-F – Verification of encoded votes
9.1.6-G – Sufficient information for verification

9.1.7 – Audit support
9.1.7-A – Number of ballots to check
9.1.7-B – No fixed margin of error
9.1.7-C – Random number generation

9.2 - The voting system produces readily available records that provide the ability to check whether the election outcome is correct and, to the extent possible, identify the root cause of any irregularities.

9.2-A – Compliance audit procedures
9.2-B – General post-election audit procedures
9.2-C – Generating CVRs
9.2-D – Reporting intermediate results
9.2-E – Reporting unusual audit events
9.2-F – Reporting format
9.2-G – Ballot count

9.3 - Voting system records are resilient in the presence of intentional forms of tampering and accidental errors.

9.3-A – Data protection requirements for audit records

9.4 - The voting system supports efficient audits.

9.4-A – Efficient compliance audit
9.4-B – Efficient risk-limiting audit
9.4-C – Unique ballot identifiers
9.4-D – Multipage ballots
Principle 10: Ballot Secrecy

The voting system protects the secrecy of voters’ ballot selections.

10.1 - Ballot secrecy is maintained throughout the voting process.

10.1-A – System use of voter information

10.2 - The voting system does not contain nor produce records, notifications, information about the voter, or other election artifacts that can be used to associate the voter’s identity with the voter’s intent, choices, or selections.

10.2.1 – Voter associations
   10.2.1-A – Direct voter associations
   10.2.1-B – Indirect voter associations
   10.2.1-C – Use of indirect voter associations
   10.2.1-D – Election worker selection of indirect associations
   10.2.1-E – Isolated storage location
   10.2.1-F – Confidentiality for indirect association

10.2.2 – Identification in vote records
   10.2.2-A – Identifiers used for audits
   10.2.2-B – No voter record order information
   10.2.2-C – Identifying information in voter record file names
   10.2.2-D – Non-memorable identifiers and associations
   10.2.2-E – Aggregating and ordering

10.2.3 – Access to cast vote records (CVR)
   10.2.3-A – Least privilege access to store
   10.2.3-B – Limited access
   10.2.3-C – Authorized access
   10.2.3-D – Digital voter record access log

10.2.4 – Voter information in other devices and artifacts
   10.2.4-A – Voting information in receipts
   10.2.4-B – Ballot secrecy for receipts
   10.2.4-C – Logging of ballot selections
   10.2.4-D – Activation device records
Principle 11: Access Control

The voting system authenticates administrators, users, devices, and services before granting access to sensitive functions.

11.1 - The voting system enables logging, monitoring, reviewing, and modifying of access privileges, accounts, activities, and authorizations.

11.1-A – Logging activities and resource access 11.1-C – No disabling logging
11.1-B – Voter information in log files 11.1-D – On-demand access to logs

11.2 - The voting system limits the access of users, roles, and processes to the specific functions and data to which each entity holds authorized access.

11.2.1 – Authorized access
11.2.1-A – Ensuring authorized access
11.2.1-B – Modifying authorized user lists
11.2.1-C – Access control by voting stage
11.2.1-D – Access control configuration
11.2.1-E – Administrator modified permissions
11.2.1-F – Authorized assigning groups or roles

11.2.2 – Role-based access control
11.2.2-A – Role-based access control standard
11.2.2-B – Minimum groups or roles
11.2.2-C – Minimum group or role permissions
11.2.2-D – Applying permissions

11.3 - The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations.

11.3.1 – Access control mechanism
11.3.1-A – Access control mechanism application
11.3.1-B – Multi-factor authentication for critical operations
11.3.1-C – Multi-factor authentication for administrators
11.3.2 – Username and password
11.3.2-A – Username and password management
11.3.2-B – Password complexity
11.3.2-C – Minimum password complexity
11.3.2-D – Usernames within passwords

11.4 - The voting system’s default access control policies enforce the principles of least privilege and separation of duties.

11.4-A – Least privilege for access policies 11.4-B – Separation of duties

11.5 - Logical access to voting system assets are revoked when no longer required.

11.5-A – Access time period 11.5-C – Lockout time duration
11.5-B – Account lockout
**Principle 12: Physical Security**

*The voting system prevents or detects attempts to tamper with voting system hardware.*

**12.1 - The voting system supports mechanisms to detect unauthorized physical access.**

12.1-A – Unauthorized physical access  
12.1-B – Unauthorized physical access alarm  
12.1-C – Disconnecting a physical device  
12.1-D – Logging of physical connections and disconnections  
12.1-E – Logging door cover and panel status

12.1-F – Secure containers  
12.1-G – Secure physical locks  
12.1-H – Secure locking system key  
12.1-I – Backup power for power-reliant countermeasures

**12.2 - The voting system only exposes physical ports and access points that are essential to voting operations.**

12.2-A – Physical port and access least functionality  
12.2-B – Physical port auto-disable

12.2-C - Physical port restriction  
12.2-D – Disabling ports  
12.2-E – Logging enabled and disabled ports
Principle 13: Data Protection

The voting system protects data from unauthorized access, modification, or deletion.

13.1 - The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records.

13.1.1 – Configuration file
   13.1.1-A – Authentication to access configuration file
   13.1.1-B – Authentication to access configuration file on EMS
   13.1.1-C – Authentication to access configuration file for network appliances

13.1.2 – Election records
   13.1.2-A – Integrity protection for election records
   13.1.2-B – EMS integrity protection for election records

13.2 – The source and integrity of electronic tabulation reports are verifiable.

13.2-A – Signing stored electronic voting records
13.2-B – Signing electronic voting records prior to transmission
13.2-C – Cryptographic verification of electronic voting records

13.3 - All cryptographic algorithms are public, well-vetted, and standardized.

13.3-A – Cryptographic module validation
13.3-B – E2E cryptographic voting protocols
13.3-C – Cryptographic strength
13.3-D – MAC cryptographic strength
13.3-E – Key management documentation

13.4 - The voting system protects the integrity, authenticity, and confidentiality of sensitive data transmitted over all networks

13.4-A – Mutual authentication of endpoints
13.4-B – Confidentiality protection for transmitted data
13.4-C – Integrity protection for transmitted data
13.4-D – Verification of election data
Principle 14: System Integrity

The voting system performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

14.1 - The voting system uses multiple layers of controls to provide resiliency against security failures or vulnerabilities.

14.1-A – Risk assessment documentation
14.1-B – Addressing and accepting risk
14.1-C – System security architecture description
14.1-D – Procedural and operational security

14.2 - The voting system limits its attack surface by avoiding unnecessary code, data paths, connectivity, and physical ports, and by using other technical controls.

14.2-A – Extraneous processes and services
14.2-B – Non-essential features
14.2-C – Network status indicator
14.2-D – Wireless network status indicator
14.2-E – Secure configuration and hardening
14.2-F – Secure configuration and hardening documentation
14.2-G – Unused code
14.2-H – Exploit mitigation technologies within platform
14.2-I – Application use of exploit mitigation technologies
14.2-J – Importing software libraries
14.2-K – Physical port restriction
14.2-L – Known vulnerabilities
14.2-M – List of known vulnerabilities

14.3 - The voting system maintains and verifies the integrity of software, firmware, and other critical components.

14.3-A – Supply chain risk management strategy
14.3-B – Criticality analysis
14.3-1 – Bill of Materials
14.3.1-A – Cryptographic boot verification
14.3.1-B – Preventing of boot on error
14.3.1-C – Logging of verification failure
14.3.2 – Software integrity
14.3.2-A – Installing software
14.3.2-B – Software verification for installation
14.3.2-C – Software whitelisting
14.3.2-D – Integrity protection for software whitelists

14.4 - Voting system software updates are authorized by an administrator prior to installation.

14.4-A – Authenticated operating system updates
14.4-B – Authenticated application updates
14.4-C – Authenticated firmware updates
Principle 15: Detection and Monitoring

The voting system provides mechanisms to detect anomalous or malicious behavior.

15.1 - Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing.

15.1-A – Event logging
15.1-B – Exporting logs
15.1-C – Logging voter information
15.1-D – Logging event types
15.1-E – Configuration file access log

15.2 - The voting system generates, stores, and reports all error messages as they occur.

15.2-A – Presentation of errors
15.2-B – Documenting error handling
15.2-C – Logging errors
15.2-D – Creating error reports

15.3 - The voting system is designed to protect against malware.

15.3-A – Software verification
15.3.1 – Malware protection
15.3.1-A – Malware protection mechanisms
15.3.1-B – Updatable malware protection mechanisms
15.3.1-C – Documenting malware protection mechanisms
15.3.1-D – Notification of malware detection
15.3.1-E – Logging malware detection
15.3.1-F – Notification of malware remediation
15.3.1-G – Logging malware remediation

15.4 - A voting system with networking capabilities employs appropriate, well-vetted modern defenses against network-based attacks, commensurate with current best practice.

15.4-A – Network architecture documentation
15.4-B – Telecommunications documentation
15.4-C – Secure configuration documentation
15.4-D – Firewall and IDS
15.4-E – Least privilege
15.4-F – Rule and policy updates
## Appendix C: References

<table>
<thead>
<tr>
<th>Reference</th>
<th>Citation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANSI15a:</td>
<td>CISPR 22 Ed. 5.2 b: 2015 RLV, Information technology equipment - Radio disturbance characteristics - Limits and methods of measurement.</td>
</tr>
<tr>
<td>FCC19b:</td>
<td>Title 47, Part 68, Rules and Regulations of the Federal Communications Commission, Connection of Terminal Equipment to the Telephone.</td>
</tr>
<tr>
<td>Reference</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Reference</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>RM</td>
<td>ISO/IEC 23270:2006, Information technology—Programming languages—C#.</td>
</tr>
<tr>
<td>ISO19a</td>
<td>ISO/IEC PRF TR 24772-1 PROGRAMMING LANGUAGES -- GUIDANCE TO AVOIDING VULNERABILITIES IN PROGRAMMING LANGUAGES -- PART 1: LANGUAGE INDEPENDENT.</td>
</tr>
<tr>
<td>Reference</td>
<td>Details</td>
</tr>
<tr>
<td>-----------</td>
<td>---------</td>
</tr>
<tr>
<td>MISRA18:</td>
<td>Roberto Bagnara, Abramo Bagnara, and Patricia M. Hill, “The MISRA C Coding Standard and its Role in</td>
</tr>
<tr>
<td>Reference</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Reference</td>
<td>Description and Available Links</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Source</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>