Voluntary Voting System Guidelines VVSG 2.0

Requirements for the Voluntary Voting System Guidelines 2.0

February 10, 2021

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 Elections
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

Diane Golden
Accessibility Expert
Grain Valley, MO

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 Election Process Working Groups: Pre-Election, Election, and Post-Election Process Working Groups** performed a great deal of up-front work to collect locale-specific election process information and, from that, to create coherent process models.
- **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.

Executive Summary

The United States Congress passed the *Help America Vote Act of 2002 (HAVA) [HAVA02]* to modernize the administration of federal elections and to establish the U.S. Election Assistance Commission (EAC) to provide guidance to the states in their efforts to comply with the HAVA administrative requirements. *Section 202* of HAVA directs the EAC to adopt voluntary voting system guidelines, and to provide for the testing, certification, decertification, and recertification of voting system hardware and software.

The purpose of the guidelines is to provide a set of specifications and requirements against which voting systems can be tested to determine if they provide all the basic functionality, accessibility, and security capabilities required of voting systems. This document, the **Voluntary *Voting System Guidelines Version 2.0*** (referred to herein as the Guidelines or *VVSG 2.0*), is the fifth iteration of national level voting system standards. The Federal Election Commission published the first two sets of federal standards in 1990 *[VSS1990]* and 2002 *[VSS2000]*. The EAC then adopted Version 1.0 of the VVSG *(VVSG 1.0) [VVSG2005]* on December 13, 2005. In an effort to update and improve Version 1.0 of the VVSG, on March 31, 2015, the EAC commissioners unanimously approved *VVSG 1.1 [VVSG2015]*.

The *VVSG 2.0* is a departure from past versions in that a set of principles and associated guidelines were first developed to describe how, at a high-level, voting systems should be designed, developed, and how they should operate. The *VVSG 2.0* requirements were then derived from those principles and guidelines. The *VVSG 2.0* requirements fit within a framework of documents under the EAC Voting System Certification Program that include:

- VVSG 2.0 Principles and Guidelines
- VVSG 2.0 Requirements
- VVSG 2.0 Testing and Certification Program Manual

The Guidelines were designed to meet the challenges ahead, to replace decade's old voting machines, to improve the voter experience, and provide necessary safeguards to protect the integrity of the voting process. All sections of the prior VVSG versions have been reviewed, re-evaluated, and updated to meet modern expectations, which address how voters should interact with the voting system and how voting systems should be designed and developed. The *VVSG 2.0* requirements represent the latest in both industry and technology best practices, requiring significant updates in many aspects of voting systems.

The Guidelines allow for an improved and consistent voter experience, enabling all voters to vote privately and independently, ensuring votes are marked, verified and cast as intended, and that the final count represents the true will of the voters. *Section 508 Information and Communication Technology (ICT) Final Standards and Guidelines [USAB18]*, and *Web Content Accessibility Guidelines (WCAG) [W3C10]* are referenced and highlighted. Voter interface requirements have been updated to incorporate recent usability research and interactions that result from modern devices and now fully support accessibility throughout the voting process.

The cybersecurity of voting systems has never been more important. Indeed, attacks from nation state actors on our elections infrastructure in 2016 led to a critical infrastructure designation. To limit the attack surface on voting systems, the Guidelines require that any election system, such as an e-pollbook or election reporting system, be air-gapped from the voting system. To ensure the integrity of the voting process, methods have been implemented to detect errors through the combined use of an evidence trail and regular audits, including risk-limiting audits (RLAs), compliance audits, and ballot-level audits. There is a dedicated section on ballot secrecy, preventing voter information from being carried through to the voting system, and two-factor authentication is now mandated for critical voting operations. Cryptographic protection of data and new system integrity requirements ensure that security protections developed by industry over the past decade are built into the voting system. These include risk assessment and supply chain risk management, secure configurations and system hardening, exploit mitigation, sandboxing and runtime integrity.

The *VVSG 2.0* requires the voting system to include the capability of using common data formats defined by the National Institute of Standards and Technology (NIST) and public working groups. The common data formats were created to make election data more transparent and interoperable. These formats can be used in addition to any native formats used by the manufacturer. Defensive coding practices, reliability and electrical requirements were reviewed, updated, and streamlined. Finally, guidance relevant to testing and certification has been moved to the EAC's testing and certification manual.

This document was produced by the EAC's Technical Guidelines Development Committee (TGDC) working in conjunction with NIST to aid in developing guidelines for voting equipment and technologies for making accessible, accurate and secure elections possible.

EAC staff must annually review the VVSG for proposed revisions. Determinations must be sent to the EAC's Executive Director (or a person operating in that capacity) to begin the review process required by HAVA (review by the TGDC, Board of Advisors, Standards Board, and public comment review) to ensure timely adoption of revisions. Under the direction of the Executive Director, EAC staff in consultation with NIST staff may make minor technical changes to the requirements in a timely manner. This process may include, but is not limited to, the development of an appeals process for such minor technical changes. EAC staff is responsible for updating the test assertions and issuing requests for interpretation or notices of clarification, as needed, to ensure efficiency in the process.

Table of Contents

Introduction

This document, the *Voluntary Voting System Guidelines 2.0* (*VVSG 2.0*), is the third version of national level voting system standards. Adherence to the Guidelines is governed by state and territory-specific laws and procedures.

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.

This version offers a new approach to the organization of the guidelines. It is a complete re-write of the *Voluntary Voting System Guidelines 1.1 (VVSG 1.1) [VVSG2015]* and contains new and expanded material in many areas, including reliability, usability, accessibility, and security.

The requirements of the *VVSG 2.0* are more precise, more detailed, and written to be clearer to voting system manufacturers and test labs. 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.

The *VVSG 2.0* requirements were derived from the *VVSG 2.0 Principles and Guidelines*, which contain 15 major principles and 63 associated guidelines that cover voting system design, development, and operations.

How the VVSG is to be Used

This document will be used primarily by voting system manufacturers and voting system test laboratories as a baseline set of requirements for voting systems to which states will add their state-specific requirements as necessary. This audience includes:

- Manufacturers, who will use the requirements when they design and build new voting systems as information about how voting systems should perform or be used in certain types of elections and voting environments.
- Test labs who will refer to this document when they develop test plans for the analysis and testing of voting systems as part of the national certification process and state certification testing to verifying whether the voting systems have satisfied the *VVSG 2.0* requirements.

This document, therefore, serves as an important, foundational tool that defines a baseline set or requirements necessary for ensuring that the voting systems used in U.S. elections will be secure, reliable, and easy for all voters to use accurately.

Scope

The scope of the *VVSG 2.0* is limited to equipment acquired by states and certified by the EAC. The *VVSG 2.0* covers pre-voting, voting, and post-voting operations consistent with the definition of a ***voting system*** in the *Help America Vote Act (HAVA) Section 301 [HAVA02]*, which 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.

The ***voting system*** as defined in the *VVSG 2.0* is:

Equipment (including hardware, firmware, and software), materials, and documentation used to enact the following functions of an election:

1. *define elections and ballot styles,*
2. *configure voting equipment,*
3. *identify and validate voting equipment configurations,*
4. *perform logic and accuracy tests,*
5. *activate ballots for voters,*
6. *record votes cast by voters,*
7. *count votes,*
8. *label ballots needing special treatment,*
9. *generate reports,*
10. *export election data including election results,*
11. *archive election data, and*
12. *produce records in support of audits.*

As part of the voting system scope, *HAVA Section 301 [HAVA02]* mandates five additional functional 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, which are reflected in the *VVSG 2.0* requirements:

1. Permit the voter to verify (in a private and independent manner) their choices before their ballot is cast and counted.
2. Provide the voter with the opportunity (in a private and independent manner) to change their choices or correct any error before their ballot is cast and counted.
3. 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 their ballot before it is cast and counted.
4. Be accessible for individuals with disabilities in a manner that provides the same opportunity for access and participation (including privacy and independence) as for all voters.

5. Provide alternative language accessibility pursuant to *Section 203* of the *Voting Rights Act [VRA65]*.

Section 301(a)(3)(B) [HAVA02] also states that there should be "… at least one direct recording electronic voting system or other voting system equipped for individuals with disabilities at each polling place". However, the *Americans with Disabilities Act of 1990 [ADA10]* requires that voters with disabilities be provided with auxiliary aids that allow them to participate equally in the voting process without discrimination. This is consistent with *Section 301* of HAVA cited above that requires a voting system to be accessible for individuals in a manner that provides the same opportunity for access and participation (including privacy and independence). If a majority of voters utilize hand-marked paper ballots, a sufficient number of accessible voting stations (including alternative language ballot features) must be available in each polling place to ensure their consistent availability in case of malfunctions. A sufficient number of machine-marked ballots must also be produced by those voting stations to ensure non-discrimination and ballot secrecy, particularly when the ballots produced by the accessible voting system differ in size, shape, and/or content from the hand-marked ballots and are thus readily identifiable. Procedures and training for poll workers on the operation of the accessible voting stations are also necessary to support this usage.

There is substantial experience[1] showing that having one accessible voting machine per polling place used only for voters with disabilities has worked poorly for voters with disabilities and may not be sufficient to provide equal access as required by law. For instance, data collected in recent elections highlight how difficult it is to ensure that a sufficient number of voters use the accessible voting machines to preserve the secrecy of machine-marked ballots and that poll workers are able to operate the machines successfully. To support best practices, states should consider legislation and additional resources to ensure balanced access to accessible voting machines wherever voting technology is deployed and used for elections.

The *VVSG 2.0* definition of a voting system does not expand the HAVA definition but focuses it on election processes. The *VVSG 2.0* principles, guidelines, and requirements apply to the election process functions and, by extension, to the voting devices that implement these functions.

The scope of most *VVSG 2.0* requirements apply to the entire voting system as opposed to specific devices, thus permitting the manufacturer more freedom to implement the requirements as they choose. However, when the scope of a requirement is limited to a specific function, that information is included in the text of the requirement, for clarity. For example:

- "A voting system's electronic display must be capable of..."

[1] For more details, see:
a) "Disability, Voter Turnout, and Voting Difficulties in the 2012 Elections" (Rutgers) **https://smlr.rutgers.edu/sites/default/files/images/Disability%20and%20voting%20survey%20report%20for%202012%20elections.pdf**;
b) "Experience of Voters with Disabilities in the 2012 Election Cycle" (National Council on Disability) **https://ncd.gov/rawmedia_repository/8%2028%20HAVA%20Formatted%20KJ%20V5%20508.pdf**; and
c) "The Blind Voter Experience: A Comparison of the 2008 and 2012 Elections" (National Federation of the Blind) **https://nfb.org/images/nfb/documents/word/2012_blind_voter_survey_report.docx**.

- “Scanners and ballot marking devices must include…”
- “The cryptographic E2E protocol used in the voting system must…”

Implications for Networking and Remote Ballot Marking

Traditionally, ballots have been cast at polling places or through mail-in absentee ballots. There has been a growing trend to provide flexibility for voters to vote early and in-person at vote centers or at home using remote ballot marking applications. These innovative methods of voting provide additional paths to voting independently and privately for voters including those with disabilities. Likewise, advances in technology have led to efficiencies in election administration, including increasing the use of e-pollbooks for easy check-in and electronic election results reporting for timely aggregation of unofficial election results.

These additional election systems require network access to synchronize voter records, access remote ballot marking applications, and transmit unofficial election results. The measures taken to securing these systems falls outside the scope of *VVSG 2.0*. However, the benefits and risks associated with the use of these technologies was carefully considered when developing the Guidelines, whereas the associated and requirements were created developed to ensure that the voting system is isolated from these additional election systems.

This section clarifies the boundary between the external election systems and the voting system as well as the use of wireless technologies within polling places or vote centers.

External Network Connections

VVSG 2.0 does not permit devices or components using external network connections to be part of the voting system. There are significant security concerns introduced when networked devices are then connected to the voting system. This connectivity provides an access path to the voting system through the Internet and thus an attack can be orchestrated from anywhere in the world (e.g., nation state attacks). The external network connection leaves the voting system vulnerable to attacks, regardless of whether the connection is only for a limited period or if it is continuously connected. These types of attacks include the following:

- The loss of confidentiality and integrity of the voting system and election data through malware injection or eavesdropping.
- The loss of availability to access data or perform election process (e.g., ransomware attack).

The *VVSG 2.0* requirements address the concerns of external network connections (see *14.2-E – External network restrictions* and *15.4-B – Secure network configuration documentation)*. Externally networked devices or components, such as those used for e-pollbooks or transmission of election results, must be physically isolated from the voting system. This

physical isolation can be described as an *air gap* between any systems that have an external network connection.

Remote Ballot Marking

Remote ballot marking is defined as an election system for voters to mark their ballots outside of a voting center or polling place. These systems are to be used as a tool which enables "no excuse" absentee voting. This allows a voter to receive a blank ballot to mark electronically, print, and then cast by returning the printed ballot to an election office. A voter may electronically fill out their ballot with a state-provided web application. Remote ballot marking applications provide another path to voting independently and privately for voters including those with disabilities.

The *VVSG 2.0* requirements apply to devices used to mark ballots inside a polling place or vote center. They do not apply to remote ballot marking devices and applications. The *VVSG 2.0* requirements affect only those voting system devices that constitute a voting system and that are submitted for testing and certification. For remote ballot marking, the voter uses a web application, their own personal device, and an external network (i.e., the Internet).

It should be noted that remote ballot marking applications need to comply with accessibility laws such as the *Americans with Disabilities Act of 1990 [ADA10]*. *VVSG 2.0* requirements that address the accessibility and usability for the electronic interface of a remote ballot marking software application can serve as an informative resource for developers of these systems. For example, *8.2-A — Federal standards for accessibility*, identifies the WCAG Level AA checkpoints in the *Section 508 [USAB18] – Standards* as a requirement for voting system electronic interfaces.

Internal Wireless Networks

Internal wireless networks wirelessly communicate or transfer information between two or more devices. Examples include use of wireless (Bluetooth) mice and keyboards or (Wi-Fi) printers. There are also growing trends towards using wireless technology for assistive devices such as headsets or hearing aids.

Wireless technology within the voting system introduces security concerns in that wireless networks can provide an entry point to the voting system for attackers. The security configurations for devices used in wireless technologies are not all equally secure, with some configured to provide more strength than others.

The *VVSG 2.0* requires that a voting system be incapable of broadcasting a wireless network (see *14.2-C – Wireless communication restrictions* and *15.4-C – Documentation for disabled*

wireless). Instead, a voting system could use *wired* technology, e.g., Ethernet cables, to connect devices such as printers.

Wireless personal assistive technologies are still possible, however. A voter may use their Bluetooth headset by using an adapter connected to the voting system's 3.5 mm standard headphone jack, which creates a Bluetooth wireless connection between the adaptor and the headset. This effectively limits the attack surface to that of the headphone jack's analog communications without limiting the use of the voter's personal assistive technology.

Major changes from VVSG 1.1 to VVSG 2.0

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 barcodes 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
- Guidance relevant to testing and certification has been moved to the EAC testing and certification manuals.

Principle 2 - High Quality Implementation

- Adds requirement to document and report on user-centered design process by developer to ensure system is designed for a wide range of representative voters, including those with and without disabilities, and election workers

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*, Section 508 Information and Communication Technology (ICT) Final Standards and Guidelines [USAB18]* and *Web Content Accessibility Guidelines 2.0 (WCAG 2.0) [W3C10]*
- 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) verifiable 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, suspended, post-voting)
- Does not require role-based access control (RBAC)
- Requires multi-factor authentication for critical operations:
    - Software updates to the certified voting system
    - Aggregating and tabulating
    - Enabling network functions
    - 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 *[NIST01]* validated cryptographic modules (except for end-to-end cryptographic functions)
- Requires cryptographic protection of various election artifacts
- Requires digitally signed cast vote records and ballot images
- 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
- Detection systems must be updateable
- Requires digital signatures or allowlisting for voting systems
- Requires malware detection focusing on backend PCs

VVSG document structure

This document contains the following sections:

- **Principles and Guidelines:** High level system design goals
- **Requirements:** Detailed technical requirements that support the principles and guidelines
- **Appendix A - Glossary of Terms:** 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:** References to external sources used in the writing of the requirements

Conformance Information

This section provides information and requirements about how manufacturers can use the material in 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.

Organization and Structure of VVSG 2.0 Requirements

The *VVSG 2.0* 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
- Text of each requirement
- Optional informative discussion field
- Optional informative field for applicability of the requirement

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

> **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 [W3C10]* and *Section 508 [USAB18*] software design issue standards.
>
> Applies to: Electronic interfaces

Requirements are indicated by the presence of a unique number in the left margin, followed by a descriptive title.

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

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

- *"Related requirements:"* VVSG requirements elsewhere in the document related to the current requirement.
- *"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.

Navigating through Requirements

You can navigate through the requirements:

From the list of principles and guidelines in the *Table of Contents*. Links in this list navigate to the requirements that support each principle or guideline.

From the list of all requirements in *Appendix B: Requirements Listing*. This list lets you quickly identify requirements in each section. Each title is also linked to the requirement text for navigation throughout the document.

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**.

Technical standards and terms used in the requirements

There are a number of technical standards that are incorporated in the Guidelines through the use of references. These are referred to by title in the body of the document. The full citations for these publications are provided in *Appendix C: References*. This appendix also includes other references that may be useful for understanding the information. References in requirements and informative text are linked to *Appendix C*.

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 what is commonly used by the information technology industry. In some cases, terminology is specific to elections or voting systems. Requirements that use words with special meanings are linked to their definitions in *Appendix A: Glossary of Terms*.

Conformance 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.

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

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.

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 to the VVSG 2.0

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

The VVSG 2.0 - Principles and Guidelines

The *VVSG 2.0* consists of 15 principles and 53 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 and its software are 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.

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 for usability with a wide range of representative voters, including those with and without disabilities.

8.4 - The voting system is evaluated for usability 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.

9.2 - 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 is designed to limit 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.

Principle 1
High Quality Design

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 Election Results Common Data Format Specification *(NIST SP 1500-100) [NIST16]* is required for imports and exports.

2 – Pre-election testing 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 - Casting which deals with the capabilities of the voting system to enable a voter to activate and cast a ballot. 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. Additionally, the requirements deal with capabilities needed for common vote variations, ballot measures, and write-ins.

5 - 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. This 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.

6 – Ballot handling for vote-capture devices 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.

7 – Exiting or suspending voting 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 or vote centers.

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

9 - Reporting results which deals with the need for the voting system to have the capability of creating 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.
- **Misfeed 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 a 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 a system that correctly implements specified properties from those that do not. They include:

- **Reporting of manufacturer-performed tests** – so testers have a baseline set of information significant for the specification, performance, and reporting of each test.
- **Coverage of manufacturer-performed tests**– so that all requirements applicable to a submitted system are also covered by submitted tests.

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

1.1.1 – Election definition

1.1.1-A – Election definition

The voting system must provide the capability to import, define, maintain, and export the information necessary to define ballots and hold an election, including for:

1. election districts,
2. contests and ballot measures,
3. candidates, and
4. ballot style information.

Discussion

This requirement states that election and ballot definition capabilities must be included within the voting system. Ballot style information includes those labels, headers, and other information typically found on ballots and that varies across jurisdictions and precincts. Requirements in *Principle 4: Interoperable* deal with using common data formats for importing and exporting election definition information.

1.1.1-B – Serve multiple or split precincts and election districts

The voting system must describe election districts and precincts in such a way that a given polling place may serve:

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

Discussion

This requirement addresses the capability to accommodate multiple ballot styles depending on the political geography being served by a polling place.

1.1.1-C – Multiple identifiers

The voting system must enable election officials to associate at least three identifiers that can be cross-referenced with each other for administrative subdivisions, election districts, contests, and candidates. This also includes:

1. locally defined identifiers;
2. state-wide-defined identifiers; and
3. Open Civic Data Identifiers [OCD-ID].

Discussion

This requirement is based on the need to support cross-referencing of statewide identifier schemes, such as *Open Civic Data Identifiers [OCD-ID]* with those used on a more local level.

1.1.1-D – Definition of parties and contests

The voting system 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; and
3. contests that include ballot positions with write-in opportunities.

1.1.1-E – Voting variations

The voting system must provide the capability to define and identify contests, contest options, candidates, and ballot questions using all voting variations indicated in the manufacturer-provided implementation statement.

Discussion

See requirements in sections *1.1.4 – Casting* and *1.1.8 – Tabulation* for voting variations most commonly used in the U.S.

1.1.1-F – Confirm recording of election definition

The voting system must check and confirm that its data is correctly recorded to a persistent storage system.

Discussion

Persistent storage includes storage systems such as non-volatile memory, hard disks, and optical disks.

1.1.1-G – Election definition distribution

The voting system must provide for creation of master copies of election definition information as needed to configure each voting device in the voting system.

1.1.1-H – Jurisdiction-dependent content

The voting system must enable election officials to update jurisdiction-dependent text, line art, logos, and images to ballot styles.

1.1.1-I – Include contests

The voting system must provide for the inclusion of all contests in a given ballot style, in which the voter is entitled to vote.

1.1.1-J – Exclude contests

The voting system must provide for the exclusion of any contest from a given ballot style, in which the voter is prohibited from voting because of place of residence or other administrative criteria.

Discussion

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

1.1.1-K – Primary elections, associate contests with parties

The voting system must support the association of different contests with different political parties when administering primary elections.

1.1.1-L – Ballot rotation, Election definition

The voting system must support the production of rotated ballots or activating ballot rotation functions in vote-capture devices by including relevant metadata in distributed election definitions and ballot styles.

1.1.1-M – Ballot configuration in combined or split precincts

The voting system must include the capability of creating distinct ballot configurations for voters from two or more election districts that are served by a given polling place or vote center.

1.1.1-N – Ballot style identification

The voting system must include the capability to generate codes or marks to uniquely identify the ballot style associated with any ballot.

1.1.2 – Pre-election testing

1.1.2-A – 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.

1.1.2-B – Installation of software and ballot styles

The system must include the capability to verify that software and ballot styles have been properly selected and to provide notification of any errors that occur while selecting or installing software and ballot styles.

Discussion

At a minimum, *notification* means an error message and a log entry. 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-C – Use of test ballots

The voting system must provide the capability to submit test ballots for use in verifying the integrity of the system.

1.1.2-D – Testing all ballot positions

Vote-capture devices must allow for testing that uses all potential ballot positions in the election as active positions.

1.1.2-E – Testing cast vote record creation

The voting system must include the ability to verify that cast vote records (CVRs) are created and tabulated correctly by permitting election officials 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-F – Testing codes and image creation

The voting system must include the capability to verify that encoded versions or images of voter selections on a ballot and any other encoded information on a ballot are created correctly by permitting election officials to compare the encodings and images with the test ballots.

Discussion

The purpose of this requirement is to give election officials the capability, prior to opening the polls, to audit encoded versions of voter selections. This process may include the review of created ballots and encoded information on each ballot to ensure that the images correctly match the ballot, thus validating accuracy in ballot creation. and that the ballot was created accurately. will include such as provided by a ballot marking device (BMD) using QR codes and gain assurance that the QR codes and any encoded data represented by the QR codes contains the voter's selections exactly as made. Likewise, to audit any image of the ballot made by a scanner to gain assurance that the image correctly matches the ballot. And, to audit any encoded information on the ballot to gain assurance it is being created correctly.

Related requirement: 1.1.2-C – Use of test ballots

1.1.2-G – Testing equipment calibration

Scanners must support testing 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-H – No side-effects from pre-election testing

Pre-election testing must introduce no lasting effects in regard to the operation of the voting system 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 counters that record ballots cast; and
5. normal wear and tear.

Discussion

It should be impossible (by design) for the pre-election testing to have any influence on the operation of the device(s) 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 pre-election testing. If a test election is run on the voting system as a means of providing pre-election testing, an election

official should be able to remove all artifacts of the test election except as noted in items 1 through 5 of this requirement.

1.1.2-I – Equipment status and readiness reports

The voting system must provide the capability to produce equipment readiness reports that show the readiness of the equipment, including:

1. whether calibration is needed;
2. consumable supplies such as toner or paper are sufficient for use;
3. batteries are fully charged; and
4. the status of other election-sensitive aspects of the equipment.

1.1.2-J – Ballot style readiness reports

The voting system must provide the capability to produce pre-election reports that include:

1. the allowable number of votes in each contest;
2. the tabulation method for each contest;
3. the inclusion or exclusion of contests as the result of precinct splits; and
4. samples of all final ballot styles.

1.1.2-K – Precinct-based voting devices readiness reports

Precinct-based voting devices must have the capability of generating readiness reports that include:

1. the election's identification data;
2. the identification of the precinct and polling place; and
3. the identification of all ballot styles used in that precinct.

1.1.2-L – All vote-capture devices readiness reports

Vote-capture devices must have to capability to generate a report that includes the following:

1. the election's identification data;
2. the identification of the precinct and polling place, if applicable;

3. the identification of the device;
4. the identification of all ballot styles loaded;
5. the contents of each active contest option register at all storage locations;
6. confirmation that no hardware or software failures were detected during setup and testing, or a record of those that occurred; and
7. any other information needed to confirm the readiness of the equipment.

1.1.3 – Opening the polls

1.1.3-A – Opening the polls

The voting system must provide functions to enter 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. More information about the activated stage is defined in Table 11-1.

1.1.3-B – Non-zero totals

The voting system must not enter the voting mode until all 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 counters:

1. must be recorded in the audit log, and
2. an election worker must be clearly notified of the event.

Discussion

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

1.1.4 - Casting

This section describes the requirements of the ballot issued to the voter and the types of contests that appear on the ballot. This includes characteristics that the voter must be aware of in order to accurately reflect the intent of their choices and the requirements of the voting system when the ballot is cast.

1.1.4-A – Voting and casting the ballot

The voting system must provide a ballot to each voter containing contests and contest choices using all voting variations that are indicated in the voting system implementation statement.

1.1.4-B – Control ballot configuration

The voting system must, where applicable:

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; and
3. enable the selection of the ballot configuration that is appropriate to the party affiliation declared by the voter in a primary election.

Discussion

This requirement does not apply to pre-printed paper ballots. For on-demand ballot printing systems, item 3 requires that the proper ballot style be selected for the voter and the appropriate ballot be printed for the voter's use. For an electronic display or ballot marking device, items 1-3 would be required, where poll workers may control the ballot configuration by using an activation device, issuing a token, or following other jurisdictional procedures to select the appropriate ballot style.

1.1.4-C – Precinct splits, Casting

Each ballot that is issued to a voter must include contests that are associated with a district that the voter's residential address falls within.

Discussion

If a precinct is not entirely contained in the district associated with the precinct, multiple ballot styles must be available to ensure that each voter in the precinct receives a ballot that only contains contests for which they are eligible to vote.

1.1.4-D – Ballot rotation, Casting

The order of contest options listed on each ballot must be in the order prescribed. The voting system must be able to correctly associate a voter's choice with the associated contest choice independent of where it appears on a specific voter's ballot.

Discussion

Many states require contest choice position order to be rotated on different ballots to prevent bias for or against a choice based on position listed.

1.1.4-E – Partisan closed primary ballot

The voting system must provide a type of ballot, used in a partisan primary election. to the voter that only contains contests associated with a specific party to which the voter is registered in addition to any nonpartisan contests that the voter is eligible to make choices.

Discussion

This type of ballot is used in states that run *closed primary elections* (voter is issued a ballot based on party of registration), *partially closed primary elections* (voter can receive a party-specific ballot that is different from their registration or an unaffiliated voter can choose a party ballot) and *partially open primary elections* (voters do not register by party and choose a party-specific ballot for the election).

1.1.4-F – Partisan open primary ballot

The voting system must provide a type of ballot, used in a partisan primary election, to the voter that contains partisan contests from all parties and any nonpartisan contests in which the voter is eligible to make choices. Only choices associated with one party will be permitted.

Discussion

This type of ballot is used in states that run *open primary elections*, where voters do not register by party but choose the party for which they wish to vote.

1.1.4-G – Indicate party affiliations and endorsements

The voting system must provide a type of ballot associated with:

1. a *partisan primary election* that identifies the party associated with each listed primary election contest (all listed contest options are affiliated with the listed party); and

2. a *partisan general election* that identifies the affiliated/endorsing party of each contest choice.

1.1.4-H – Write-in contest options

The voting system must be capable of enabling and recording the voter's write-in of desired candidate names.

Discussion

A write-in is a contest option on the ballot that permits the voter to identify a candidate of choice that is not already listed as a contest option and is captured when the ballot is cast. State rules determine when a write-in candidate option may be placed as a contest option on the ballot and what qualifies as a valid write-in selection that may be counted.

1.1.4-I – Write-in reconciliation

The voting system must be capable of gathering and recording write-in votes within a voting process that allows for reconciliation of aliases and double votes.

Discussion

Reconciliation of aliases means allowing election officials 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.

1.1.4-J – N-of-M contest, Casting

For the N-of-M contest, the voting system must be capable of gathering and recording votes in a contest where the voter may choose up to a specified number of choices from a list of contest options. These selections are independent of selections in any other contest.

Discussion

A baseline N-of-M contest is one where a voter is allowed N contest choices from a list of M choices and where votes are tallied independently of any other contest options on the ballot. N includes 1 (vote for 1 contest or typically a measure) or any larger number. If N is larger than M, all choices listed will be selected. It can be used for *approval voting* by setting N equal to M. It can also be used for *limited voting* by setting N to be less than the number of seats being elected.

1.1.4-K – Straight-party voting, Casting

For straight-party voting, the voting system must be able to provide a contest in which a voter may select political party contest choices that result in the selection of all partisan

contests on their ballot. In this instance, a selection of a political party choice automatically selects all contest choices associated with that party. The voting system must be capable of gathering and recording votes for both this contest and all partisan contests associated with it.

Discussion

Straight-party voting is a voting variation used in a general election. It provides the voter with the ability to select all candidates affiliated with a desired party in all partisan contests on the ballot by selecting one contest option. When a party is selected, the system must not prevent the selection of individual candidate options that may negate the original straight-party choice, nor must it require that voters utilize the straight-party voting option. Rules for determining the candidate choices resulting from the combination of direct option selections and straight-party option selections are determined by the rules in states that use straight-party voting.

1.1.4-L – Cumulative voting contest, Casting

For a cumulative voting contest, the voting system must be capable of gathering and recording votes in a contest where the voter may allocate no more than the allowed number of votes to one or more contest selections in whole vote increments.

Discussion

When a cumulative voting contest is on a ballot, the system must allow the voter to assign all allowed votes to any desired contest selection or to any set of contest selections in whole vote increments. The total of all selection assignments must not exceed the total votes allowed. (See *1.1.4-Q - Proportional voting contest (equal-and-even cumulative voting contest), Casting* for an alternate method of assigning multiple votes to a candidate.)

1.1.4-M – Ranked choice voting contest, Casting

For a ranked choice voting (RCV) contest, the voting system must be capable of gathering and recording votes in a contest where the voter must be able to rank contest selections in order of preference, as first choice, second choice, etc.

Discussion

The ballot presentation of a RCV contest is independent of the number of seats being elected. Depending on jurisdictional rules, the number of choice options provided may vary from a minimum of 3 to the number of contest choices on the ballot. Contest outcome determination requires cast vote records (CVR) to be processed post-election.

1.1.4-N – Party preference contest

For a party preference contest, the voting system must be capable of gathering and recording votes for a contest containing a list of political party choices. In this instance, the voting system uses a valid selection of a party in the contest, which limits gathering and recording of votes in all partisan contests on the ballot to those associated with the selected party.

Discussion

A party preference contest only appears on an *open primary ballot* when required by state rules. Its purpose is to allow the voter to select the party they intend to vote contests for and prevent the voter from spoiling the partisan section of the ballot by, for example, marking contests in a different party's section of the ballot.

1.1.4-O – Top-2 primary contest (blanket primary contest)

For a top-2 primary contest, the voting system must be capable of assigning candidates of all relevant parties to a single seat contest which is also assigned to all partisan ballots.

Discussion

In some states, this method is required to be used to fill designated partisan offices. The contest, also called a *blanket primary contest*, appears on all party-specific primary ballots. All candidates are listed as contest options including their party affiliation. The 2 candidates who receive the most votes will be on the general election ballot independent of their party affiliation.

1.1.4-P – Presidential delegate contest, Casting

For a presidential delegate contest, the voting system must be capable of gathering and recording votes for only those delegates that are affiliated with the voter's choice in the presidential preference contest.

Discussion

Presidential delegate voting is a voting variation that only is used in a *presidential primary election* on a party-specific primary ballot where delegates to the convention are selected by the voter when the method is selected by a state's political party. With this method, only contest option selections in delegate contests that are pledged to the voter's presidential candidate selection will be recorded. If the voter does not make a selection in the presidential preference contest, selections for presidential delegates will not be recorded.

1.1.4-Q – Proportional voting contest (equal-and-even cumulative voting contest), Casting

For a proportional voting contest, the voting system must be capable of gathering and recording votes for a contest which allow multiple votes to be assigned to a candidate. This is accomplished by prorating the number of allowed votes proportionally to the number of validly selected candidates.

Discussion

Also known as *equal-and-even cumulative voting*, this contest is an alternative to a cumulative voting contest in allowing multiple votes to be assigned to selected candidates. Votes are assigned based on the votes allowed and the number of valid selections made by dividing the number of votes allowed by the number of options chosen. Marking fewer selections than the number of votes allowed may result in fractional votes being assigned to a contest option.

1.1.4-R – Group voting contest, Casting

For a group voting contest, the voting system must be capable of designating a group select contest choice that automatically selects, gathers and records all contest choices associated with the group. More than one contest group select contest choice must be provided if the contest contains more than one group of candidates.

Discussion

A group voting contest is used to enable the voter to select a large number of allowed candidate options associated with a single group, party or ideology with a single option selection. There may be multiple groups of contest choices each associated with a single selection. The system treats a group selection as if all candidates in the group are selected when determining the number of selections made. This voting variation is currently only used in the State of Massachusetts to select Ward and Town party committee persons and only appears on the ballot in the presidential preference primary.

1.1.4-S – Top-2 IRV contest (supplementary or contingent vote contest)

For a top-2 instant runoff voting (IRV) contest, the voting system must be capable of gathering and recording votes in a contest where the voter must be able to rank contest options in order of preference as their first choice, second choice, etc.

Discussion

The top-2 IRV contest, also known as a supplementary or contingent vote contest, is an IRV type contest and provides the voter the ability to identify the contest options in order of preference in the same fashion as a standard IRV contest. Although voted the same as an IRV contest and requiring cast vote records to be processed post-election to determine outcome, only the top-2 candidates with the most votes are eligible to win.

1.1.5 – Recording voter choices

1.1.5-A – Casting and recording

The voting system must support casting a ballot, recording each vote precisely as indicated by the voter subject to the rules of the election jurisdiction, and creating a cast vote record that can be tabulated and audited.

1.1.5-B – Ballot orientation

The voting system, when using pre-printed ballots, must either:

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

1.1.5-C – 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; and
2. positions on the ballot associated with each contest selection made by the voter when multiple selections are permitted, if applicable.

Discussion

For item 2, some contests such as for RCV may place candidate choices on the same line of the ballot, therefore the positions of the candidates may need to be recorded.

1.1.5-D – 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; and
4. the total number of write-ins in the CVR.

1.1.5-E – 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 a voter has made a contest selection;
2. identification of all overvoted and undervoted contests;
3. the number of write-ins recorded for the contest; and
4. identification of the party for partisan ballots or partisan contests.

Discussion

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

1.1.5-F – Record ballot selection override information

The voting system, if recording 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; and
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 which differ from the political party contest choices. Election or contest rules may cause a scanner to invalidate the contest markings or require other actions.

1.1.5-G – 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; and
7. sequence of the corresponding voted ballot in the batch, when applicable.

Discussion

Item 2 can be any identification scheme that is preferential in the jurisdiction, e.g., polling place name, address, geographical coordinates, etc.

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.

1.1.5-H – Store and link corresponding image

The voting system must be capable of storing an image of a paper ballot and linking this image to the specific associated CVR.

Discussion

The image could be linked to the CVR by, for example, creating a filename for the image that is the same as the identifier from item 4 in Requirement *1.1.5-G – Record audit information*.

1.1.6 – Ballot handling for vote-capture devices

1.1.6-A – Detect and prevent ballot style mismatches

The voting system 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 credited to the wrong contest options.

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

1.1.6-B – Detect and reject ballots that are oriented incorrectly

The voting system must either:

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

1.1.6-C – Ballot separation when batch feeding

Batch-fed scanners, in response to unreadable ballots, write-ins, and other designated conditions, 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 election official to remove the ballot;
3. mark the ballot with an identifying mark to facilitate its later identification; and/or
4. if the ballot image uniquely identifies its corresponding ballot, use electronic adjudication to segregate the ballot.

Discussion

Item 4 allows the ballot image to be segregated if, for example, an identifier is printed on the ballot as it is scanned, so that the image of the ballot also contains this identifier. Without a unique identifier or other marking, the ballot image itself does not facilitate finding the corresponding paper ballot.

1.1.6-D – Overvotes, undervotes, blank ballots

Voter-facing scanners must provide a function that can be activated by election officials to stop the scanning process and display a message which will enable the removal and correction of 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; and
4. blank ballots.

Related requirements: 7.3-H – Overvotes
7.3-I – Undervotes

1.1.6-E – Write-ins, Ballot handling for vote-capture devices

Voter-facing scanners, when scanning a ballot containing a write-in vote, must either:

1. segregate the ballot in a manner that facilitate its later identification; or
2. if the ballot image uniquely identifies its corresponding ballot, use electronic adjudication to segregate the ballot.

Discussion

The requirement to separate ballots containing write-in votes is not applicable to systems in which a BMD encodes write-in votes in a machine-readable form. In this instance, 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.

1.1.6-F – Ability to clear mis-fed ballots

If multiple feed or misfeeding (jamming) occurs, batch-fed scanners must:

1. permit 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); and
2. prevent duplicate scanning of the ballots.

Discussion

Number 2 deals with whether CVRs have been created for the ballots that were jammed.

1.1.6-G – Scan to manufacturer specifications

The voting system must have the capability to provide a report of the mark detection thresholds that have been used to program the scanner so that the information is available upon request.

Discussion

Manufacturers must not make their specifications proprietary; auditors must be able to understand what and what does not constitute a valid voter mark on a particular scanner.

1.1.6-H – Accurately detect imperfect marks

The voting system 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; and
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 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. In plain language: scanning technologies may vary, but as a minimum requirement, all of them should be capable of reliably reading *this* mark.

1.1.6-I – Ignore extraneous marks inside voting targets

The voting system must include a capability to recognize any imperfections in the ballot stock, folds, and similar insignificant marks appearing inside the voting targets and not record them as votes.

Discussion

Insignificant marks appearing inside of the voting targets could be detected as votes, thus the capability to recognize the ballot folds or imperfections must be included as a part of the voting system. It may not be possible to completely eliminate this problem in all cases depending on scanner thresholds for detecting marks.

Related requirements: 1.1.6-G – Scan to manufacturer specifications

1.1.6-J – Marginal marks, without 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.

1.1.6-K – Repeatability

The determination of a vote on a manually marked paper ballot must be repeatable, such that it never changes from a vote to a non-vote or from non-vote to a vote.

Discussion

Since it is technically impossible to achieve repeatable readings of ballots containing marks that fall precisely on the scanning threshold, changing between a non-vote and a marginally machine-readable mark is allowed. Similarly, changing from a valid vote and a marginally machine-readable mark is allowed.

1.1.7 – Exiting or suspending voting

1.1.7-A – Exiting or suspending election mode

The voting system must provide designated functions for exiting or suspending an election mode in which voting is permitted.

Discussion

When voting is conducted across multiple days, for example, during early voting, these requirements are still applicable even though the election itself may not be over; this is with the exception of requirement *1.1.7-E – Prevent re-entering election mode*, which deals with preventing re-opening of the polls once they have been closed on election day.

1.1.7-B – No voting when voting is stopped

The voting system must prevent the further activation, marking, or casting of ballots by any device once the voting has stopped.

Discussion

This requirement is applicable to voter-facing scanners, batch-fed scanners and any other device that enables the activation or tabulation of the voting process. However, 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 jurisdictional procedure.

1.1.7-C – Voting stop integrity check

The voting system must provide an internal test that verifies that the prescribed closing or suspension procedures have been followed.

1.1.7-D – Report on voting stop process

The voting system must provide a means to produce a diagnostic test record that verifies the sequence of events, which indicate that the voting mode has been deactivated or suspended.

1.1.7-E – Prevent re-entering election mode

The voting system must not be capable of re-entering an election mode, in which voting is permitted, once the closing procedures have been completed for an election without an explicit override authorized by an administrator.

Discussion

When early voting is conducted across multiple days, this requirement does not prevent reopening of the polls on the following day.

Related requirements: 11.3.1-B – Multi-factor authentication for critical operations

1.1.8 – Tabulation

1.1.8-A – Tabulation

The voting system must support the tabulation function for all voting variations indicated in the implantation statement. This function includes:

1. extracting the valid votes from each ballot cast according to the defined rules;
2. creating and storing a CVR that contains the disposition of each contest selection as well as the disposition of each contest choice that is eligible to be cast; and
3. accumulation and aggregation of contest results and ballot statistics.

Discussion

Results accumulation and aggregation takes place at multiple levels within the voting system. Each tabulation unit must perform this function and must have the ability to transmit the CVRs and results to the election management system (EMS) for jurisdiction wide accumulation and aggregation.

1.1.8-B – Partisan primary elections

In partisan primary elections, the voting system must be capable of reporting separate totals for the number of ballots read and the number of ballots counted for each political party. This is independent of whether the primary type is closed or open.

Discussion

From a tabulation perspective, there are two types of partisan primary election ballots. A *closed primary ballot* is one in which a ballot is limited to contests associated with one political party and any nonpartisan contests. An *open primary ballot* is one which contains contests from all parties on the same ballot, but the voter may only select contest choices applicable to a single party.

1.1.8-B.1 – Tabulation of a closed primary ballot

The voting system must support the tabulation of ballots that are specific to a party or are nonpartisan and must be able to report combined totals for nonpartisan contests no matter what party ballot the contest appears on.

1.1.8-B.2 – Tabulation of an open primary ballot

When tabulating ballots from an open primary, the voting system must limit tabulation of votes to contests of one political party.

Discussion

In an open primary, a voter may select partisan contest choices that are associated with more than one political party. Therefore, tabulation of a ballot during an open primary will void the partisan content of the ballot and only contest selections in nonpartisan contests are tabulated. The ballot is treated like a nonpartisan ballot.

1.1.8-B.3 – Open primary ballot with party preference contest

If the ballot contains a party preference contest and a party preference contest choice is selected, the voting system must only tabulate partisan contest option selections from contests that are of the same party as is selected in the party preference contest.

Discussion

A party preference contest provides the voter with the ability to select their intended party and avoid cross-party selections voiding the partisan selection of the ballot. If a party preference contest option is not selected, partisan contests on the ballot are tabulated as if the party preference contest was not present.

Related requirements: 1.1.4-N – Party preference contest

1.1.8-C – Write-ins, Tabulation

The voting system must be capable of

1. tabulating votes for write-in candidates with separate totals for each contest choice, and
2. tabulating valid individual write-in candidate totals in each contest.

Discussion

Tabulation of candidate names that are manually written in on a hand voted paper ballot can only be tabulated as an aggregate total in each contest. Each name must be adjudicated from graphical images of the contest write-in area or from the ballot itself to determine the name of the candidate. When names are typed on an electronic voting unit such as a BMD, although the entered names must be recorded, only aggregate contest write-in totals are tabulated. Each individual write-in name must be adjudicated for validity before they can be aggregated. In most states, a write-in candidate must be registered to be valid. State rules also determine acceptable variations in the written name for the candidate to be credited with the vote. State rules also determine treatment of a written-in name of a candidate already listed on the ballot.

1.1.8-D – Ballot rotation, Tabulation

When the order of contest choices within a contest varies by ballot style, the voting system must tabulate votes for each contest selection independent of a contest selections location in the contest on the ballot.

Discussion

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

1.1.8-E – Straight-party voting, Tabulation

When tabulating a partisan general election ballot, which includes a validly selected straight-party contest option in a straight-party contest, the voting system must select each candidate contest choice that is endorsed by the selected party in every contest on the ballot unless the contest is specifically exempted.

Discussion

There are currently two different tabulation rule sets for handling a ballot with both a straight-party selection and a selection in a contest of a candidate not endorsed by the selected party, known as party crossover. In one, any selection of a contest choice in a partisan contest eliminates any straight-party selection in that contest. In the other, straight-party option selections in a contest are eliminated if the number of candidates selected exceeds the allowed number, whether directly selected by the voter or automatically selected by the straight-party. Other rules are possible as well.

Note that some states explicitly indicate that certain contests will not be affected by a straight-party selection.

1.1.8-F – Cross-party endorsement with straight-party voting

For straight-party tabulation, if a listed candidate option is endorsed by more than one political party, the voting system must be capable of tabulating votes for that candidate independent of which party option is validly selected.

1.1.8-G – Precinct splits, Tabulation

When multiple ballot styles are associated with a specific precinct, the voting system must be capable of keeping separate totals for the number of ballots read and counted for each ballot style or split. Tabulation must not be affected by variation of contest selection locations from one ballot style to another.

1.1.8-H – N-of-M contest, Tabulation

For N-of-M voting, the voting system must be capable of tabulating votes, overvotes, and undervotes in contests where the voter is permitted to select up to a specified number of contest choices.

Discussion

An N-of-M contest is one where a voter is allowed *N contest selections* from a list of *M choices* and where votes are tallied independent of any other contest choices. N includes 1 vote (1 vote for 1 contest or typically a measure) or any larger number. Contest choices include those where the contest choices are candidates for a specific office or measures/referenda where there are usually only two contest choices (Yes/No, For/Against) but may also be a list of choices (Tax rate A, Tax rate B, Tax rate C). An N-of-M contest is used for *approval voting* by setting N to be equal to M. This type of contest is used for *limited voting* by setting N to be less than the number of seats being elected. An N-of-M contest is also is used for top-2 primary contests (blanket primary contests), where N is always 1 but the 2 candidates with the most votes will be on the general election ballot.

1.1.8-I – Cumulative voting contest, Tabulation

For cumulative voting, the voting system must be capable of tabulating votes, overvotes, and undervotes in contests where the voter may allocate up to a specified number of votes over a list of contest choices in any manner they choose. This may result in possibly giving more than one vote to a given contest selection.

1.1.8-J – Ranked choice voting contest, Tabulation

For ranked choice voting (RCV), the voting system must

1. capture the voter's ranking of each contest selection and store it in the CVR associated with the ballot style;
2. aggregate 1st choice totals of each contest selection; and
3. process the collection of CVRs round-by-round according to the method specified in the implementation statement.

Discussion

Ranked choice voting (RCV) tabulation methods are different for single seat and multi-seat contests. Jurisdictional rules vary even when using the same basic method. A voting unit or precinct tabulating unit cannot perform RCV tabulation. RCV tabulation requires the concurrent availability of all CVRs associated with an RCV contest and is a post-voting accumulation/aggregation process. Some jurisdictional rules may only require use of the RCV tabulation process if aggregated first choice selections do not produce the total needed to exceed the threshold of votes required to win. Other jurisdictional rules do not use tabulated and aggregated 1st choice selections and require the RCV tabulation process to be used for all winners. Single winner RCV is also known as IRV (Instant Runoff Voting). STV (Single Transferable Vote) is a method used for multi-winner RCV. Another multi-winner process (Sequential At-Large IRV) uses successive IRV passes, one pass to determine each winner.

1.1.8-K – Group voting contest, Tabulation

When tabulating group voting contest choices, the voting system must automatically select each contest choice that is affiliated with the selected group as if the voter manually selected each of those candidate choices. Any selection of a contest choice outside of the group will constitute as an overvote if the number of candidates in the group selected is equal to the votes allowed.

Discussion

There may be multiple candidate groups in a contest. The ballot normally places contest options for all candidates in a group sequentially, with the group contest option first. If a contest is not fully voted by utilizing the group voting contest option, a voter can select additional contest options outside of the group, as long as the total does not exceed the votes allowed.

1.1.8-L – Presidential delegate contest, Tabulation

When tabulating a presidential delegate contest, the voting system must prevent votes for any delegate in the contest that is not representing the president candidate chosen by the voter's contest option selection in the presidential contest.

Discussion

Most states that directly elect presidential delegates do not have a tabulation associated with the presidential candidate selection. However, as of 2020, Alabama has included this association on both the democratic and republican ballots, while Rhode Island has the association on the democratic ballot. When used, if there is no presidential candidate selection or the presidential candidate and no affiliated delegate in the contest, no vote will be counted for any delegate contest option selection.

1.1.8-M – Recall contest pair

When tabulating a recall/replace contest pair, the voting system must only tabulate the replace contest (controlled contest) if there is a vote selection in the recall contest (controlling contest).

Discussion

The *recall contest* in the contest pair is typically a question used to determine whether an elected official should be recalled and the replace contest allows selection of the desired replacement. If the question is not voted, the replacement contest is not processed. However, the contest pair has been used for other purposes such as annexations and determination of tax rates.

1.1.8-N – Proportional voting contest (equal-and-even cumulative voting contest), Tabulation

Votes selections in a proportional voting contest (also known as an equal-and-even cumulative voting contest) must be tabulated for the selected contest option or options by dividing the allowed votes by the number of contest option selections; this may occur as long as the number of selections do not exceed the number of allowed votes.

Discussion

This may produce a fractional number of votes tabulated for a candidate. However, it is not possible to tabulate undervotes in this contest.

1.1.9 – Reporting results

1.1.9-A – Post-election reports

The voting system must have the capability to create post-election reports that contain cast ballot counts and vote counts for contests on the ballot types served by precincts or splits of precincts.

1.1.9-B – Report categories of cast ballots

The voting system must have the capability to report the number of ballots cast in total and broken down by ballot style. This is in addition to the associated units of political geography for the following categories of ballots cast:

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

Discussion

Associated units of political geography may also include state, county, city, town or township, ward, and districts.

1.1.9-C – Report categories of votes

The voting system must have the capability to report the following categories of votes:

1. in-person voting,
2. absentee voting,
3. write-ins,
4. accepted reviewed ballots, and
5. rejected reviewed ballots.

1.1.9-D – Reporting combined or split 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 data from the voting location by precinct.

1.1.9-E – Report counted ballots by contest

The voting system must have the capability to 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.

1.1.9-F – Report votes for each contest option

The voting system must have the capability to 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.

1.1.9-G – Report overvotes for each contest

The voting system must have the capability to report the number of overvotes for each relevant N-of-M or cumulative voting contest.

1.1.9-H – Report undervotes for each contest

The voting system must have the capability to 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.

1.1.9-I – Ranked choice voting, report results

The voting system must have the capability to report the contest choice vote totals for each ranked choice contest and 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.

1.1.9-J – Precinct reporting devices, reporting device consolidation

When more than one vote-capture device is used in a polling place, the voting system must have the capability to consolidate the data tabulated by each unit into a single report for the polling place.

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.

1.1.9-K – Precinct reporting devices, no tallies before polls close

The voting system must prevent the printing of vote data reports and extracting vote tally data while the polls are open.

Discussion

Providing ballot counts does not violate this requirement. The prohibition is against providing vote totals for ballot contests.

1.1.9-L – Report read ballots by party

The voting system must have the capability of reporting separate totals for each party in primary elections when reporting categories of read and counted cast ballots.

1.1.9-M – Reports are time stamped

All reports must include the date and time of the report's generation, including hours, minutes, and seconds.

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

Requirements in this section deal with voting system accuracy and reliability.

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

The data collected during the testing of this requirement contributes substantially to the evaluations of reliability, accuracy, and misfeed rate.

1.2-B – Reliably detectable marks

The voting system must detect marks on the ballot consistent with system mark specifications and differentiate between voter-made marks constituting votes versus voter-made marginal marks or other marks on the ballot.

Discussion

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

1.2-C – 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 [VVSG2005]*, 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.

1.2-D – Handle maximum volume

The voting system must be able to handle the maximum volume of activities in conditions approximating normal use in an entire election process according to manufacturer specifications.

Discussion

This requirement should be verified through operational testing if the limit is practically testable.

1.2-E – Respond gracefully to stress of system limits

Certain conditions tend to overload the system's capacity to process, store, or report data. These conditions include attempts to process more than the expected number of precincts, and to process more than the expected volume or ballot tabulation rate. Therefore, the voting system must be able to respond to the above conditions that overload the system's capacity, by ensuring that the voting system does not fail or halt suddenly. The voting system must give adequate warning if it is to fail or halt for any reason.

Discussion

This requirement should be verified through operational testing if the limit is practically testable.

1.2-F – No single point of failure

The voting system must protect against a single point of failure that would prevent further voting at the polling place.

Discussion

The intent of this requirement is to prevent, at the polling place, a situation in which failure of a component would prevent voting. This can be addressed in various ways, including being able to swap in/out devices without loss of data.

1.2-G – Misfeed rate benchmark

The voting system 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.

1.2-H – Protect against failure of input and storage devices

The voting system must withstand, without loss of data, the failure of any data input or storage device.

Discussion

The intent of this requirement is to prevent votes from being permanently lost due to the failure of a storage device that contains votes. For example, if a scanner fails, the voting system must have the ability to swap in a replacement data input device without the losing cast vote records that were previously recorded by the failed scanner.

1.2-I – FCC Part 15 Class A and B conformance

Voting devices must comply with the requirements of the *Rules and Regulations of the Federal Communications Commission, Part 15, Class B [FCC19a]*.

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

1.2-J – 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.

1.2-K – Power port connection to the facility power supply

Voting devices located in polling places 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.

1.2-L – Leakage from grounding port

Voting devices located in polling places 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.)

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 – Reporting of manufacturer-performed tests

Each test provided in a manufacturer-submitted report of internal testing performed (technical data package (TDP)) must, at least, include the following information:

1. requirement(s) under test;
2. items under test to exercise a given requirement;
3. pass-fail criteria necessary to determine whether or not a requirement has passed the test of conformity to the requirement;
4. evidence (observations, data) expected to provide justification for satisfying or failing a given pass-fail condition;
5. test procedures necessary to provide, observe, record, analyze, and interpret this evidence relative to pass-fail criteria;
6. where applicable, descriptions of the causes of variation, ambiguity, noise, or observed errors in observed and recorded evidence during tested procedures;
7. where applicable, descriptions of any necessary techniques, procedures, or processes applied to normalize or clean data prior to subjecting it to data analysis and interpretation relative to pass-fail criteria;
8. report of actual tests performed and their results; and
9. description and justification if a given test cannot be fully performed or exercised due to internal resource constraints, including description of alternative means of verification.

Discussion

This is a documentation requirement. Its intent is to ensure a baseline set of information provided in manufacturer-submitted report of manufacturer-performed internal testing submitted as part of the TDP. Manufacturers may likely have additional information, formatting, etc., as part of their particular testing practices, that they will include as is consistent with their internal testing best-practices.

1.3-B – Coverage of manufacturer-performed tests

Each requirement identified in a manufacturer-submitted implementation statement or conformance statement must describe one-or-more tests in their test-plan describing how it was tested.

Discussion

This requirement is to ensure that all requirements identified in the respective implementation and conformance statements are covered by the submitted test-plan.

Principle 2
High Quality Implementation

The voting system is implemented using high quality best practices.

2.1 - The voting system and its software are 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

The voting system is implemented using high quality best practices. are designed to provide transparency.

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:

2.1 - **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. The sections in ***Guideline 2.1*** cover:

1 – Workmanship which deals with best practices for providing high quality systems and parts, taking reasonable precautions to prevent defect or damage, and ensuring that system elements can be sufficiently durable and available with respect to lifetimes that are appropriate to their type and use.

2 – Maintainability covers the ability of a system and its components to be sufficiently identified and repaired during its operational lifetime.

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

2.3 - 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. The sections in ***Guideline 2.3*** cover:

1 – Software flow which identifies common pitfalls to be avoided when organizing software control flow so as to preserve its clarity and ease of evaluation.

2.4 - **Modularity** and complexity of the system software structure.

2.5 - 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. The sections in ***Guideline 2.5*** cover:

1 – Code integrity which deals with the protection of code from unauthorized change or tampering.

2 – Input/output errors supports practices to ensure the validity of inputs and outputs while also guarding against associated errors.

3 – Output protection which deals with the ability to protect against vulnerabilities known to affect outputs.

4 – Error handling addresses the need for internal error checking, particularly for common types of coding errors such as various types of overflows, pointer-related errors, and so on.

2.5 and 2.6 - **Graceful recovery** the capability of the voting system to handle and recover from errors, including failures of devices and components.

2.7 - **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 *Rules and Regulations of the Federal Communications Commission, 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 and its software are 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; and
5. block-structured exception handling (for example, try/throw/catch).

Discussion

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

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

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.

Previous versions of VVSG required voting systems to handle such errors by some means, preferably using programming language exceptions (*[VVSG2005] I.5.2.3.e*), but there was no unambiguous requirement for the programming language to support exception handling. These guidelines require programming language exceptions because without them, the programmer must check for every possible error condition in every possible location, which both obfuscates the application logic and creates a high likelihood that some or many possible errors will not be checked. Additionally, these guidelines require block-structured exception handling because, like all unstructured programming, unstructured exception handling obfuscates logic and makes its verification by the test lab more difficult. "One of the major difficulties of conventional defensive programming is that the fault tolerance actions are inseparably bound in with the normal processing which the design is to provide.

This can significantly increase design complexity and, consequently, can compromise the reliability and maintainability of the software." *[Moulding89]*

Existing voting system logic implemented in programming languages that do not support block-structured exception handling can be brought into compliance either through migration to a newer programming language (most likely, a descendant of the same language that would require minimal changes) or through the use of a COTS package that retrofits block-structured exception handling onto the previous language with minimal changes. While the latter path may at first appear to be less work, it should be noted that many library functions may need to be adapted to throw exceptions when exceptional conditions arise, whereas in a programming environment that had exceptions to begin with the analogous library functions would already do this (see Requirement *2.1-B – COTS language extensions are acceptable*).

2.1-B – COTS language extensions are acceptable

Requirement *2.1-A – Acceptable programming languages* 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.

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.

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

The source code review for workmanship now focuses on coding practices with a direct impact on integrity and transparency and on adherence to published, credible coding conventions, in lieu of coding conventions embedded within the standard itself.

The vast majority of coding conventions used in practice are tailored to specific programming languages. In these guidelines, the few coding conventions that have significant impact on integrity and transparency and that generalize relatively well to different programming languages have been retained, expanded, and made mandatory, while the many coding conventions that are language sensitive and stylistic in nature, and are made redundant by more recent, publicly available coding conventions, have been removed in favor of the published conventions.

As discussed, prescriptive coding conventions not directly related to integrity and transparency have been avoided in favor of published, credible conventions.

Coding conventions are considered to be **published** if they appear in a publicly available book, magazine, journal, or new media with analogous circulation and availability, or if they are publicly available on the Internet. This requirement attempts to clarify the "published, reviewed, and industry-accepted" language appearing in previous iterations of the VVSG, but the intent of the requirement is unchanged.

Coding conventions are considered to be **credible** if at least two different organizations with no ties to the creator of the rules or to the manufacturer seeking conformity assessment, and which are not themselves voting equipment manufacturers, independently decided to adopt them and made active use of them at some point within the three years before conformity assessment was first sought. This requirement attempts to clarify the "published, reviewed, and industry-accepted" language appearing in previous iterations of the VVSG, but the intent of the requirement is unchanged.

Coding conventions evolve, and it is desirable for voting systems to be aligned with modern practices.

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.

2.1.1 – Workmanship

2.1.1-A – General build quality

All manufacturers of voting systems must practice proper workmanship by:

1. adopting and adhering to practices and procedures that ensure their products are free from damage or defect that could make them unsatisfactory for their intended purpose; and
2. ensuring 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-B – Durability estimation

A manufacturer must submit a warranty model to the EAC, testing labs, and customers, that includes for each product, its relevant components, and associated consumables:

1. estimated replacement rates (e.g., 3 years, 10 years);
2. estimated costs per replacement;
3. estimated warranty types and costs;
4. associated replacement policies, services, and available maintenance agreements; and
5. plans for collecting, maintaining, and reporting data to the EAC to support and validate estimates.

Discussion

A number of factors associated with the durability of a product or its components can be highly variable and even particular to the type of components (e.g., COTS, consumables). This variance is also applicable to the resources of a given manufacturer. Thus, instead of prescribing a pre-estimated number for all manufacturers, the manufacturers are asked to make these estimates relative to their own products, components, and resources, and to provide the basis for these estimates (these warranties, replacement periods, etc.) to the EAC, labs, and customers. In this way, manufacturers can perform estimates most relevant to their chosen manufacturing strategies (i.e., COTS-centric vs. custom-built, and so on).

2.1.1-C – 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 2020-02-29, the *Government Paper Specification Standards, February 1999 No. 11 [GPO19].*

2.1.1-D – Ensure compatibility of specified paper and ink

Ink specified for use with the voting system must be compatible with the paper specifications provided by the manufacturer.

Discussion

The purpose of this requirement is to ensure that both the types of ink and paper used with a given system are compatible with each other in an effort to avoid many of the side-effects of mismatched ink and paper (e.g., excessive smudging).

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; and
3. labels and alarms related to failures.

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).

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, the name of the device, its part or model number, its revision identifier, its serial number, and if applicable, its power requirements.
2. If service or preventative maintenance is required, 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.

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 a user-centered design process.

The report must include, at a minimum:

1. a listing of user-centered design methods used;
2. the types of voters and election workers included in those methods;
3. how those methods were integrated into the overall implementation process; and
4. how the results of those methods contributed to developing the final features and design 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-9241-210:2019 Ergonomics of human-system interaction—Part 210: Human-centered design for interactive systems [ISO19b] 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, S*oftware engineering -- Software product Quality Requirements and Evaluation (SQUARE) -- Common Industry Format (CIF) for Usability* 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 [ISO10]*
- *ISO/IEC 25063:2014: Context of use description [ISO14]*
- *ISO/IEC 25062:2006: Usability test reports [ISO06b]*
- *ISO/IEC 25064:2013: User needs report [ISO13b]*
- *ISO/IEC 25066:2016 Evaluation report [ISO16]*

Related requirements: 8.3-A – Usability tests with voters
8.4-A – Usability tests 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.

Discussion

The concept of "block-structured exception handling," is the ability to associate exception handlers with blocks of logic, and implicitly, the presence of the exception concept in the programming language. (This simply means try/throw/catch or equivalent statements and should not be confused with the specific implementation known as Structured Exception Handling (SEH) [MS20].[2]) Unlike deeply nested blocks, exceptions cannot be eliminated by restructuring logic. "When exceptions are not used, the errors cannot be handled but their existence is not avoided." *[ISO00]*

Previous versions of VVSG required voting systems to handle such errors by some means, preferably using programming language exceptions ([*VVSG2005] I.5.2.3.e*), but there was no unambiguous requirement for the programming language to support exception handling. These guidelines require programming language exceptions because without them, the programmer must check for every possible error condition in every possible location, which both obfuscates the application logic and creates a high likelihood that some or many possible errors will not be checked. Additionally, these guidelines require block-structured exception handling because, like all unstructured programming,

unstructured exception handling obfuscates logic and makes its verification by the test lab more difficult. "One of the major difficulties of conventional defensive programming is that the fault tolerance actions are inseparably bound in with the normal processing which the design is to provide. This can significantly increase design complexity and, consequently, can compromise the reliability and maintainability of the software." *[Moulding89]*.

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.

Discussion

Existing voting system logic implemented in programming languages that do not support block structured exception handling can be brought into compliance either through migration to a newer programming language (most likely, a descendant of the same language that would require minimal changes) or through the use of a COTS package that retrofits block-structured exception handling onto the previous language with minimal changes. While the latter path may at first appear to be less work, it should be noted that many library functions may need to be adapted to throw exceptions when exceptional conditions arise, whereas in a programming environment that had exceptions to begin with the analogous library functions would already do this.

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.

2.3-D – Hard-coded passwords and keys

Voting system software must not contain hard-coded, including the use of:

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 *MITRE CWE-259: Use of Hard-coded Password [MITRE20a]* and *MITRE CWE-321: Use of Hard-coded Cryptographic Key [MITRE20b].*

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.

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.

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 – Legacy library units*, 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.

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

2.4-A – Modularity

Application logic must be designed in a modular fashion, meeting all the criteria stated in the definition of a module, namely that:

1. It must be a structural unit of software or analogous logical design.
2. If it contains callable units, those callable units must be tightly coupled.
3. Coupling between modules (“inter-module coupling”) must:
    a. be loose, and
    b. occur over defined interfaces.
4. It must contain all elements needed to compile or interpret successfully.
5. It must have limited access to data in other modules.
6. It must be substitutable with another module whose interfaces match the original module.

Discussion

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

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.

2.4-C – Module size and identification

Modules must be small and easily identifiable, such as being:

1. no more than 50% of all callable units (functions, methods, operations, subroutines, procedures, etc.) SHOULD exceed 25 lines of code in length, excluding comments, blank lines, and initializers for read-only lookup tables;
2. no more than 5% of all callable units SHOULD exceed 60 lines in length; and
3. no callable units SHOULD exceed 180 lines in length.

Discussion

"Lines," in this context, are defined as executable statements or flow control statements with suitable formatting.

2.4-D – Large data structures in separate files

Read-only large data structures longer than 25 lines must be placed in separate files from other source code if the programming language permits it.

Discussion

In practice, this case has often been illustrated by the need to put read-only large lookup tables into separate files. However, the same notion could apply to other kinds of data structures.

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.

2.5-B – Unsafe concurrency

Application logic must be free of race conditions, deadlocks, livelocks, and resource starvation.

Discussion

In addressing this requirement, information should be provided in the TDP describing the means by which *safe concurrency* was ensured relative to the design, implementation, and testing of the application logic.

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.

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.

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 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.

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 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.

2.5.2 – Input/output errors

2.5.2-A - Input validation and error defense

The voting system must:

1. monitor I/O operations;
2. validate all input against expected parameters, such as data presence, length, type, format, uniqueness, or inclusion in a set of whitelisted values;
3. report any input errors and how they were corrected; and

4. check information inputs to ensure that incomplete or invalid inputs do not lead to irreversible error.

Discussion

Input includes data from any input source: input devices (such as touch screens, keyboards, keypads, optical/digital scanners, and assistive devices), networking port, data port, or file. This general requirement applies to all programmed devices, while the specific ones following are only enforceable for application logic.

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 at *MITRE CWE 116: Improper Encoding or Escaping of Output [MITRE20c].*

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 touch screens, 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; and
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.

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.

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.

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.

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.

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 *MITRE CWE 134: Use of Externally-Controlled Format String [MITRE20d].*

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, and
2. dynamic memory allocation and management errors.

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.

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.

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.

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.

2.5.4-M – Election integrity monitoring

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.

2.5.4-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 at *MITRE CWE 89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') [MITRE20e].*

2.5.4-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:

1. in any device;
2. in any component (for example, memory, CPU, ballot reader, or printer) provided that catastrophic electrical or mechanical damage has not occurred; and
3. 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.

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.

2.6-C – 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 last known good state 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.

Requirements in this section deal with voting system reliability with regard to environmental conditions and electrical surges and interference.

2.7-A – 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; and
3. resistance of the voting system to electrical surges, interference, and loss of power.

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 *[CA06]* is used during various environmental conditions to determine the reliability of the voting system operations, as well as data from the test campaign regarding relevant VVSG requirements.

2.7-B – Continuous operation – typical environmental conditions

The voting system must operate for a continuous period of time during which ballots are cast and ballot positions are read and tabulated without error.

2.7-C – Continuous operation – varied environmental conditions

The voting system must operate for a continuous period of time during which ballots are cast and ballot positions are read and tabulated without error and in which temperature and humidity are varied.

2.7-D – Ability to support maintenance and repair physical environment conditions – non-operating

The voting system must be able to withstand non-operating physical environmental conditions simulating stresses that occur during maintenance and repair.

2.7-E – Ability to support transport and storage physical environment conditions – non-operating

The voting system must be able to withstand non-operating physical environmental conditions simulating stresses that occur during transport between storage locations and polling places.

2.7-F – Ability to support storage temperatures in physical environment – non-operating

The voting system must be able to withstand non-operating physical environmental conditions simulating temperature-related and humidity-related stresses that occur during storage.

2.7-G – Electrical disturbances

The voting system 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-H – Power outages, sags, and swells

The voting system must be able to withstand, without disruption of normal operation or loss of data, a complete loss of power lasting two hours.

Discussion

Essentially, battery backup must keep the voting system operational so that voting can continue for a minimum of two hours.

2.7-I – Withstand conducted electrical disturbances

All electronic voting systems must withstand conducted electrical disturbances that affect the power ports of the system.

2.7-J – 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-K – 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.

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 documentation 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 documentation lists what the manufacturer needs to cover about the personnel resources and training required for a jurisdiction to operate and maintain the system.

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 barcodes, 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 documentation

3.1.1-A – System overview documentation

The manufacturer must provide system overview documentation that identifies 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

System overview documentation must include high-level functional diagrams of the voting system that include all of its components. The diagrams must portray how the various components relate and interact.

Discussion

The diagrams could be engineering renderings or photographs.

3.1.1-C – System description

System overview documentation must include written descriptions and diagrams that present the following, 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; and
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.

Discussion

The diagrams could be engineering renderings or photographs.

3.1.1-D – Identify software and firmware by origin

System overview documentation must include full identification of all software and firmware items, indicating items that were:

1. written in-house including subcontracted;
2. procured as COTS, unmodified; and
3. procured as COTS and modified, including descriptions of the modifications to the software or firmware and to the default configuration options.

Description

Full identification would include authorship, version numbers, where procured, and other items to positively identify the COTs or in-house developed software

3.1.1-E – Traceability of procured software

System overview documentation 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 documentation

3.1.2-A – System performance documentation

The manufacturer must provide system performance documentation that includes:

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; and
5. design constraints, applicable standards, and compatibility requirements.

3.1.2-B – Maximum tabulation rate

System performance documentation must include the maximum tabulation rate for a bulk-fed scanner. 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

System performance documentation must include, for all types of optical scanners:

1. what constitutes a mark that is tabulatable;
2. what constitutes a mark that is ambiguous and may require adjudication; and
3. what constitutes a marginal mark that would not be tabulatable.

Discussion

Marginal marks could include those marks considered as stray or caused by defects or folds on the ballot.

3.1.2-D – Processing capabilities

System performance documentation must include 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. Therefore, this documentation must include the following attributes:

1. an explanation regarding 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; and
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 documentation

Manufacturers must provide a specific system security document that includes detailed information on the security architecture of the voting system and its security-related functions and how users are to properly employ them.

Discussion

This document is intended to further ensure transparency of the voting system. It includes a complete specification of the voting system security architecture, its different components, and how they work together when used properly. Information about security-related functions and components may also appear in other parts of the TDP as applicable but should also appear in this document. The document may contain detailed technical information but also is to contain usage instructions for employing security controls that are written clearly for the intended types of users, e.g., administrator, pollworker, etc.

3.1.3-B – Access control implementation

The system security document must include:

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; and
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

The system security document must include an explanation of how to implement all physical security controls for voting devices and other security-sensitive components of the voting system, including model procedures necessary for effective use of countermeasures.

3.1.3-D – Audit procedures

The system security document must include an explanation of how to conduct audit procedures to determine whether tabulation is accurate.

3.1.4 – Software installation documentation

3.1.4-A – Software installation documentation

The manufacturer must provide software installation documentation that lists 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

Software installation documentation must include 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; and
7. component identifiers (such as filenames) of the software, and type of software component (executable code, source code, or data).
8. flag to indicate whether or not the given software product should be considered "election-specific" (e.g., election-specific=[True|False]) to differentiate software used for implementing essential election application logic functions (such as counting) from more generic software (such as generic file-system functions).

3.1.4-C – Software location information

Software installation documentation must include 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 voting system software is installed on programmed devices of the voting system.

Discussion

This requirement applies to voting system 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

Software installation documentation must identify election specific software in the user documentation.

Discussion

This requirement applies to voting system software installed on programmed devices of the voting system. If the documentation can provide information (such as what is indicated in item 8 from *3.1.4-B – Software information*) then this should be sufficient to clearly distinguish those pieces of software that perform essential election functions (such as counting) from those that perform more generic, non-election-specific tasks (such as those that might perform only general file-system operations, regardless of election concerns).

3.1.4-E – Installation software and hardware

Software installation documentation must include 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 procedures

Software installation documentation must include the software installation procedures used to install software on programmed devices of the voting system in user documentation.

3.1.4-G – Baseline image creation

To replicate programmed device configurations, the software installation procedures must create a baseline image of the initial programmed device configuration with storage media and mechanism for verifying the image's validity using a digital signature.

3.1.4-H – Programmed device configuration replication

The software installation procedures must use the baseline image and associated digital signature and digital signature validation mechanism of the initial validated image to replicate the configuration onto other programmed devices.

Discussion

The main point of this requirement is to ensure transitive immutability of a given device configuration (based on a valid, original image that corresponds to an original cryptographic signature). In this way, it seeks to ensure that the starting image that is used for the replication of an image to a particular configuration or target device is the same as the one that was validated via digital signature mechanisms.

The process for dealing with varying details of alternative target platforms can be addressed with the use of modern deployment technologies to create configurable installation mechanisms. This is not uncommon for major software technology providers. Thus, technology providers will be expected to develop appropriate install and configuration mechanisms that can have configurable images that can be signed through this digital signature mechanism at the outset and when replicating to any

target configuration to ensure that both the image and the mechanisms for transforming that image in a given target deployment environment have been understood and validated from the beginning.

The above descriptions are meant to provide a way to validate a much wider range of deployment scenarios than has been experienced in the past. As a result, it is not expected or intended that this process would necessarily require strictly binary images, but rather, configurable ones, with the configuration settings and mechanisms for installation and signature verification provided, signed, and validated from the beginning.

3.1.4-I – 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 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 as well as associated digital signatures and mechanisms for installation and verification on programmed devices of the voting system; and
8. a unique identifier (such as a serial number) of the vote-capture device or election management system (EMS) which the software is installed.

Discussion

The purpose of this requirement is a continuation of *3.1.4-I – Software installation record creation*, to ensure transitive immutability from the original baseline image through a given installation process (i.e., installation of certified software).

The requirement emphasizes the importance of the final act of performing an installation of certified software on a target system configuration. It is a requirement to ensure that this event have some means by which an appropriate record, attesting to the facts of the installation event itself, can be produced and can provide the given information.

Creators of software installation mechanisms and procedures are asked to provide information in their installation user documentation specifying the elements of this record and that it should be recorded in the event of a certified software installation.

Related requirements: 3.1.4-H – Programmed device configuration replication

3.1.4-J – Procurement of voting system software

Software installation documentation must include that voting system software be obtained from a trusted distribution repository.

Discussion

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

3.1.4-K – Open market procurement of COTS software

Software installation documentation must include that COTS software be obtained from the open market.

3.1.4-L – Erasable storage media preparation

Software installation documentation 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-M – Trusted storage media

Software installation documentation must specify that trusted storage media be used to install software on programmed devices of the voting system.

Discussion

Trusted storage media can include read-only media.

Previous VVSGs emphasized the use of unalterable storage media which is believed to be too restrictive in the current technological context. Instead, it is preferable that read-only storage be used. And, as indicated in related requirements, it is assumed that any use of media, transport, or use of original images be associated with a mechanism for verifying the cryptographic signatures of those original images.

Related requirements: 3.1.4-H – Programmed device configuration replication
3.1.4-I – Software installation record creation

3.1.5 – System operations documentation

3.1.5-A – System operations documentation

Manufacturers must provide a specific system operations document for 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. It must:

1. provide a detailed description of procedures required to initiate, control, and verify proper system operation;
2. provide procedures that clearly enable the operator to assess the correct flow of system functions (as evidenced by system-generated status and information messages);
3. provide procedures that clearly enable the administrator to intervene in system operations to recover from an abnormal system state;
4. define and illustrate the procedures and system prompts for situations where operator intervention is required to load, initialize, and start the system;
5. define and illustrate 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. provide 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. support successful election definition and software installation and control by central election officials;
8. provide a schedule and steps for the software and ballot installation, including a table outlining the key dates relative to the start of voting, events, and deliverables; and
9. specify 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.

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 operations document must include 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 operations document must include a summary of system operating functions and modes to permit understanding of the system's capabilities and constraints.

3.1.5-D – Roles

The operations document must identify the roles of operating personnel and relate them to the operating modes of the system.

3.1.5-E – Conditional actions

The operations document must describe decision criteria and conditional operator functions such as error and failure recovery actions.

3.1.5-F – References

The operations document must list all reference and supporting documents pertaining to the use of the system during election operations.

3.1.5-G – Operational environment

The operations document 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; and
5. any other facility or resource required for the proper installation and operation of the system.

3.1.5-H – Readiness testing

The operations document must include 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 operations document must include 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; and
4. illustration and description of all status indicators and information messages.

3.1.5-J – Support

The operations document must include documentation of system operating procedures that:

1. describes procedures for providing technical support, system maintenance, and correction of defects, and for incorporating hardware upgrades and new software releases; and
2. defines the procedures required to support system installation and readiness testing.

3.1.5-K – Transportation and storage

The operations document must include any special instructions for the care and handling of voting devices and any removable media or records for:

1. shipment;
2. storage; and
3. archiving information.

3.1.6 – System maintenance documentation

3.1.6-A – System maintenance documentation

Manufacturers must include system maintenance documentation that provides information to support election workers, information systems personnel, or maintenance personnel in adjusting or removing and replacing components or modules in the field.

Discussion

Election workers such as polling place workers may not be permitted to replace components, however in some cases they may be permitted to adjust them. Thus, the documentation should be geared to the appropriate personnel.

3.1.6-B – General contents

Maintenance documentation must include 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

Maintenance documentation must include 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

Maintenance documentation 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 memory units;
6. how data output is initiated and controlled;
7. how power is converted or conditioned; and

8. how test and diagnostic information is acquired and used.

Discussion

The documentation should indicate how and when information is written from volatile to non-volatile memory, including redundant storage.

3.1.6-E – Maintenance procedures

Maintenance documentation must include preventive and corrective maintenance procedures for hardware, firmware, and software.

3.1.6-F – Preventive maintenance procedures

Maintenance documentation 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; and
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 procedure details

Maintenance documentation 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; and
6. any coordination required with the manufacturer, or other party, for COTS.

3.1.6-H – Special equipment

Maintenance documentation must identify and describe any special purpose test or maintenance equipment recommended for fault isolation and diagnostic purposes.

3.1.6-I – Parts and materials

Maintenance documentation must include detailed documentation of parts and materials needed to operate and maintain the system.

3.1.6-J – Approved parts list

Maintenance documentation must include a complete list of approved parts and materials needed to operate and maintain the system. 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, and
6. sources from which they may be obtained.

3.1.6-K – Marking devices

Maintenance documentation 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 ballot marking device (BMD).

3.1.6-L – Approved manufacturers

Maintenance documentation must include a listing of sources and model numbers for marking devices manufactured by multiple external sources that satisfy these requirements.

3.1.6-M – Ballot stock specification

Maintenance documentation 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-N – Ballot stock specification criteria

Maintenance 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-O – Printer paper specification

Maintenance documentation for voting systems that include printers must include specifications of the paper necessary to ensure correct operation and minimize jamming.

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.

3.1.6-P – System maintenance, maintenance environment

Maintenance documentation must identify all facilities, furnishings, fixtures, and utilities that will be required for equipment maintenance.

3.1.6-Q – System maintenance, maintenance support and spares

Maintenance documentation must identify:

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; and
3. organizational affiliation (for example, jurisdiction, manufacturer) of qualified maintenance personnel.

3.1.7 – Training documentation

3.1.7-A – Training documentation

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; and
7. testing to verify the correction of problems.

3.1.7-C – 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-D – 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

Manufacturers must provide setup inspection process documentation that includes the setup inspection process that the voting device was designed to support including a description of the risks of deviating from the process.

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

Setup inspection process documentation 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; and
4. executing logic and accuracy testing related to readiness of use in an election.

3.2-C – Setup inspection record generation

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

3.2-D – Installed software identification procedure

Setup inspection process documentation must include the procedures to identify all software installed on programmed devices of the voting system.

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

Setup inspection process documentation must include the procedures to verify the integrity of software installed on programmed devices of the voting system.

3.2-F – Election information value

Setup inspection process documentation must include a list of voting device storage locations for holding election information that can change during the election, except for the static values set to conduct a specific election.

3.2-G – Maximum and minimum values of election information storage locations

Setup inspection process documentation must include the maximum and minimum values of voting device storage locations for holding election information that can change during an election.

3.2-H – Variable value inspection procedure

Setup inspection process documentation must include the procedures to inspect the values of voting device storage locations for holding election information that can change during an election.

3.2-I – Backup power operational range

Setup inspection process documentation must include the nominal operational range for the backup power sources of the voting device.

3.2-J – Backup power inspection procedure

Setup inspection process documentation must include the procedures to inspect the remaining charge of the backup power sources of the voting device.

3.2-K – Cabling connectivity inspection procedure

Setup inspection process documentation must include the procedures to inspect the connectivity of the cabling attached to the voting device.

3.2-L – Communications operational status inspection procedure

Setup inspection process documentation must include the procedures to inspect the operational status of the communications capabilities of the voting device.

3.2-M – Communications on/off status inspection procedure

Setup inspection process documentation must include the procedures to inspect the on/off status of the communications capabilities of the voting device.

3.2-N – Quantity of voting equipment

Setup inspection process documentation must include a list of consumables associated with the voting device, including estimated number of usages per unit.

3.2-O – Consumable inspection procedure

Setup inspection process documentation must include the procedures to inspect the remaining amount of each of the voting device's consumables.

3.2-P – Calibration of voting device components

Setup inspection process documentation must include:

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

3.2-Q – Checklist of properties to be inspected

Setup inspection process documentation must include 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; and
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 publicly available documentation that:

1. describes system event logging capabilities and usage, and
2. 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 and not just in the TDP.

3.3-B – Specification of common data format usage

Manufacturers must provide publicly available documentation describing how the manufacturer has implemented a 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; and
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 CDF specification for its voting devices and the types of data exchanged or exported. Here is list of related references: *NIST SP 1500-103 Cast Vote Records Common Data Format Specification [CVR_CDF], NIST SP 1500-100 Election Results Common Data Format Specification [NIST16], NIST SP 1500-101 Election Event Logging Common Data Format Specification [LOG_CDF], NIST SP 1500-102 Voter Records Interchange(VRI) CDF Specification [VRI_CDF].*

3.3-C – Bar and other codes

Manufacturers must provide publicly available documentation that fully specifies the barcode, how barcoded data is formatted, and any other encoding standards or methods used on ballots or audit material.

Discussion

The voting system documentation needs to include the name and version of the standard used for barcodes 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. The report should be sufficient for a voter to understand the barcoded contents and for an auditor to develop applications that examine the barcoded contents.

3.3-D – Ballot selection codes

The voting system must be capable of producing a report on an election-by-election basis to show the meaning of codes and other data used within barcodes and CVRs to represent ballot selections and ballot style information.

Discussion

Codes that represent a voter's ballot selections are commonly used within barcodes and CVRs so as to save space. The codes will likely change for each election. The codes are meaningless to a voter or an auditor unless the voting system can produce a report that shows all codes possible and what contests and ballot selections they represent. If, for example, a code of 90 is used to represent a particular contest, then the report must show that 90 refers to the title or description of that particular contest. This includes other information within the barcode generally found on clear-text ballots to identify the ballot style.

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 formats 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 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 – Election programming data input and output

The voting system must include support for CDF specification(s) regarding:

1. import and export of election programming data, and
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. More information can be found in *SP 1500-100 Election Results Common Data Format Specification [NIST16].*

4.1-B – Tabulator report data

The voting system must include support for CDF specification(s) for import and export of election results reporting data.

Discussion

Importing results data is required 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. More information can be found in: NIST SP 1500-100 *Election Results Common Data Format Specification [NIST16]*.

4.1-C – Exchange of cast vote records (CVRs)

The voting system's audit, casting, tabulation, and vote-capture functions dealing with CVRs must have the capability of importing or exporting CVRs according to CDF specification(s).

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. This requirement indicates that these devices have the capability to import or export CVRs in the respective CDF(s). More information can be found in: NIST SP 1500-103 *Cast Vote Records Common Data Format Specification [CVR_CDF].*

4.1-D – Exchange of voting device election event logs

The voting devices comprising the voting system must include support for CDF specification(s) 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. More information can be found in:], *NIST SP 1500-101 Election Event Logging Common Data Format Specification [LOG_CDF].*

4.1-E – Voting device event code documentation

Manufacturers must provide a publicly available specification for event codes used in their equipment.

Discussion

Use of *NIST SP 1500-101 Election Event Logging Common Data Format Specification [LOG_CDF]* for election event logs only addresses the data format; it does not mandate a common lexicon for event codes. *NIST SP 1500-101 [LOG_CDF]* provides a separate schema for including documentation of event codes; manufactures may make this available publicly or upon request without condition.

4.1-F – Specification of common format usage

Manufacturers must include a specification describing how the manufacturer has implemented a 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 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 CDF specifications are used.

4.2-A – Standard formats

Publicly available non-proprietary formats must be used, where possible, for exchanging data.

Discussion

Examples include the use of common data encodings such as bar or QR codes.

4.2-B – Public documented manufacturer formats

Where publicly available non-proprietary formats are not available, manufacturers must include a specification that describes the protocol or data format.

Discussion

As an example, a manufacturer's algorithm or method for packing or compressing 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 – Interfaces and communication protocols

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 it will need to meet applicable environmental and electrical requirements and, potentially, other requirements depending on how the scanner is used. For example, if it is used to create CVRs, it will need to meet those requirements dealing with CVR creation and handling.

Principle 5
Equivalent and Consistent Voter Access

All voters can access and use the voting system regardless of their abilities.

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.

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) [HAVA02]* 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 Information and Communication Technology (ICT) Final Standards and Guidelines [USAB18]* which requires that electronic and information technology be accessible to people with disabilities, and the language access requirements in the *Voting Rights Act (VRA) [VRA65]*.

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. Also, in addition to actually casting their votes, voters must have access to those same display formats and interaction modes for all information and instructions related to casting those votes.

2 – Equivalent information also addresses the requirement that these display formats (visual, audio, enhanced visual) and interaction modes (touch, tactile, limited dexterity) 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 formats mid-stream, for example from visual to audio or from Spanish to English, the system must preserve all settings and votes cast.

Finally, note that this principle's requirements, including supporting the display formats and interaction modes listed in *5.1-A – Voting methods and interaction modes*, 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 – Voting methods and interaction modes

Within any method of voting, all display formats including enhanced visual and audio and all interaction modes including tactile and limited dexterity must have the same functionality as the visual format and touch mode including voting, verification, and casting.

Discussion

Methods of voting that a voting system might support include in-person voting, vote-by-mail, remote ballot marking, among others. The VVSG scope is in-person voting. For voting systems to meet this requirement they would need to include, for example:

- Features that support limited dexterity interaction to enable voters 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 scanner, 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 voting variations. 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 display formats and interaction modes.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.

5.1-B – Languages

The voting system must be capable of displaying and printing the ballot, contest options, review screens, voter verifiable paper records, and voting instructions in all languages the manufacturer has declared the system supports, in both visual and audio formats where applicable.

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.

This requirement originates with the *VRA [VRA65]*.

5.1-C – Vote records

All records, including paper ballots and voter verifiable paper records, must have the information required to support auditing by election workers and others who can only read 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 to support election administration and auditing. See *9.4 - The voting system supports efficient audits* for related requirements.

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.

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 support voters with disabilities throughout the process of voting from activation through casting. Requirements for individual system components are described in *Principle 7: Marked, Verified, and Cast as Intended*. This general requirement supports *HAVA [HAVA02].*

Related requirements: 6.1-B – Warnings

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 enhanced visual and audio formats and tactile and limited dexterity modes.

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. For ballot marking devices, for example, if the voter is using audio to make their selections, the voter verifiable paper record, not the stored voter selections, must be read back.

This requirement allows the voter to use the same access features throughout the entire voting session. 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.

This requirement supports *HAVA [HAVA02]*.

Related requirements: 7.1-I – Text size (paper)

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.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.

Related requirements: 7.3-N – Instructions for voters
7.3-O – Instructions for election workers

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 enhanced visual and audio formats and tactile and limited dexterity modes, all ballot options are to be presented in an equivalent manner.

Discussion

Certain differences in ballot 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.

5.2-B – Presenting content in all languages

All information that is presented to the voter in English must also be capable of being 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.

This requirement originates with the *VRA [VRA65]*.

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 display formats and interaction modes required in *5.1-A – Voting methods and interaction modes*. This includes voting, verification, and casting.

Discussion

For audio mode, this requirement can be met with 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 also ensure that the voter is aware of possible undervotes or overvotes. This includes information about activation.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

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 to the voter.

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 display format and interaction mode, especially for instructions.

This feature can assist voters with cognitive disabilities.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

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 set to audio-only; and
- visual cues are accompanied by sound cues unless the system is set to visual-only.

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, there would be no visual cue.

Audio output also supports non-written languages, voters with low literacy, or voters with low vision.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

5.2-F – Preserving votes

At any time during a voting session, an electronic voting interface must allow the voter to change all language and display format options, and the interaction settings that the voter can chose directly, while preserving all current vote selections. When changing settings, the

system must 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.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

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 formats, and interaction modes to anyone else.

Privacy covers:

- electronic and paper interfaces,
- audio and visual systems, and
- warning systems that must also preserve confidentiality.

Principle 6: Voter Privacy, covers voter privacy during voting. Requirements in *Principle 6* help ensure private and independent voting as mandated in the Help America Vote Act (HAVA).

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, display format and other options for 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.

This requirement supports *HAVA [HAVA02]*.

Related requirements: 7.2-F – Voter speech

6.1-B – Warnings

During the voting session, 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) [HAVA 02] 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.

Related requirements: 7.3-K– Warnings, alerts, and instructions

6.1-C – Enabling or disabling output

During the voting session, the voting system must make it possible for the voter to independently enable or disable either the audio or the visual output and be notified of the change, resulting in a visual-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 format is helpful to voters who cannot see the screen to confirm the change visually.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

Related requirements: 7.2-A – Display and interaction options
7.3-K – Warnings, alerts, and 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.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

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.

1. If a voting system includes any features voters might use after casting a ballot as part of end-to-end (E2E) verifiable system ballot tracking, they must be accessible.

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)[HAVA02] 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.

Note that in addition to features for voters after casting their ballot for E2E system ballot tracking, there are other features not in the scope of VVSG requirements that should be designed for accessibility such as forms or notices to cure problems with a vote-by-mail ballot, and sites to learn whether a provisional ballot was accepted for counting.

Related requirements:
- 2.2-A – User-centered design process
- 5.1-D – Accessibility features
- 5.1-E – Reading paper ballots
- 8.2-A – Federal standards for accessibility

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 *Principle 7* are derived from federal laws, including:

- the *Help America Vote Act of 2002 (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 though 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.

Applies to:	Electronic interfaces
Related requirements:	7.1-K – Audio settings

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 with the ballot presented to the voter using the new settings, but still keeping what was selected thus far.

Applies to:	Electronic interfaces
Related requirements:	5.2-F – Preserving votes

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.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

Applies to: Electronic interfaces

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, including:
    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, and

c. white text similar to #FAFAFA, providing a contrast ratio of at least 18:1.

3. 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), and
- grey text similar to #898989 on a dark background similar to #222222 (4.5:1).

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.

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; and
3. Red is used to indicate error conditions or a problem requiring immediate attention.

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 design element 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.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.

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 [VVSG2015]* 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 *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

Applies to:	Electronic interfaces
Related requirements:	5.2-A – No bias 5.2-F – Preserving votes 7.2-D – Scrolling 7.3-B – No split contests

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 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 [WCAG10] in requiring scaling with no horizontal scrolling up to 200% and allowing zooming with horizontal scrolling for larger text.

Applies to:	Electronic interfaces
Related requirements:	5.1-A – Voting methods and interaction modes 5.2-A – No bias 5.2-C – All information in all modes 5.2-F – Preserving votes 7.1-G – Text size (electronic display) 7.2-D – Scrolling

7.1-I – Text size (paper)

The voting system must be capable of printing paper ballots and other paper records with a font size of at least 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.

Applies to:	Printed Material
Related requirements:	5.1-E – Reading paper ballots
	7.1-G – Text size (electronic display)

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.

WCAG 2.0 [W3C10] and *Section 508 [USAB18]* require that at least one mode of characters displayed on the screen be a sans-serif font.

7.1-K – Audio settings

The voting system's audio format interface 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 20 dB 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 120 to 125 words per minute (wpm).
6. The range of speech rates supported is from 60-70 wpm to 240-250 wpm (or 50% to 200% of the default rate), with no distortion.
7. Adjusting the rate of speech does not affect the pitch of the voice.

Discussion

The top speech rate is slower than some audio users prefer for narrative reading to ensure that candidate names are pronounced clearly and distinctively.

Note that calculation of rate of speech can vary based on the length of the words in the sample, so requirements are stated as a small range.

Speech rates as slow as 50 wpm and as fast as 300 wpm can be included if this can be done without distortion or flanging.

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 *[TC04]*, 60 dB SPL is the volume of ordinary conversation.

FCC regulations for hearing aids, *47 CFR Parts 20 and 68: Hearing Aid Standard [FCC18]*, includes useful information about how to test audio volume and quality.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.

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.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

7.1-M – Audio comprehension

The voting system's audio format interface 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; and
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 of 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 [ITU19]*.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.

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 tactilely discernible without activating those controls or keys;
2. include a Unified English Braille, Contracted label if there is a text label; and
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.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

Related requirements: 7.2-E – Touch screen 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 available to the voter must be visually discernible, and also discernible through either touch or sound.

Discussion

This applies to any physical controls or keys that have a locking or toggle function.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

7.1-P – Identifying controls

Buttons and controls for the voter that perform different navigation or selection functions must be distinguishable by both shape and color for visual and tactile 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 *[TCnd].*

Some examples are:

- Color can be helpful to make different sets of functions visually distinct: groups of buttons can share a color, such as Volume UP/DOWN.
- Tactile perception requires different shapes, so that finding a control does not rely solely on the layout: all the shapes cannot be squares, but two or four triangles can be used if they point in different directions.
- As a group of well-known keys, a full alphabetic keyboard is acceptable for entering a write-in candidate name, but individual keys cannot be used for navigation or selection. Using these keys for functions would require a voter to see the visual labels or know the arrangement for those functions.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.

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 format and interaction mode options to enable voters to mark their ballot to vote, and verify and cast their ballot, supporting the full functionality in each mode:

1. Visual format;
2. Enhanced visual format;
3. Audio format;
4. Touch mode; and
5. Limited dexterity mode.

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 the tactile mode.

Limited dexterity mode controls include those that do not require dexterity and those that can be operated without use of hands.

Full functionality includes at least instructions and feedback regarding:

- 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.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

Related requirements: 5.1-A – Voting methods and 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 visual.

As with all requirements, this applies to all display formats and interaction modes.

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. This requirement includes the following:

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 display formats and 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:
    a. *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
    b. *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:
    a. 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;
    b. include easily perceivable cues in every display format to indicate that there is more information or there are more contest options available; and
    c. include an option for an audio format and visual format that sync during scrolling.
3. The navigation method must ensure that the voting system:

a. meets all requirements for providing feedback to the voter;

b. accurately issues all warnings and alerts including notifications of undervotes and overvotes;

c. meets all requirements for control size and interaction, and keeping all controls visible;

d. does not rely only on conventional platform scroll bars; and

e. 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 (electronic display), 7.1-H – Scaling and zooming (electronic display),* 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 screen 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*.

Applies to: Electronic interfaces

Related requirements: 7.1-G – Text size (electronic display)
7.1-H – Scaling and zooming (electronic display)
7.2-E – Touch screen gestures
7.2-F – Voter speech
7.2-H – Accidental activation
7.2.I – Touch area size
7.3-B – No split contests
7.3-E – Feedback
7.3-F – Correcting the ballot
7.3-H – Overvotes
7.3-I – Undervotes
7.3-K – Warnings, alerts, and instructions

7.2-E – Touch screen gestures

Voting system devices used by voters with a touch screen may use touch screen 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 touch interactions.
2. Gestures work consistently across the entire voting interaction.
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 are limited to simple, well-known gestures.
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 an interaction 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 format 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, and

- 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.

Applies to:	Electronic interfaces
Related requirements:	7.1-N – Tactile keys
	7.2-H – Accidental activation

7.2-F – Voter speech

If the voting system includes speech or human sounds as a way for voters to control 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.

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 format 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").

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.

The draft of WCAG 2.1, the next version of *WCAG 2.0 [W3C10]* 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.

Related requirements: 7.1-N – Tactile keys
7.2-E – Touch screen gestures

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 touch screens 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 (the next version of *WCAG 2.0 [W3C10]*) 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.

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.

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.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

Applies to: Physical 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. They can be used if manufacturers supply a stylus or other device that activates the capacitive screen.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

Applies to: Electronic interfaces

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.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.

7.2-N – System response time

The voting system's response time must meet the following response times:

1. The system initially responds to a voter action in no more than:
    a. 0.1 seconds for a visual change, and
    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, touch screen system ideally should not take 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).

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. The system must document the inactivity time.
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.

For a referendum, in audio format, the timer starts when the audio finishes.

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 sets minimum dimensions for clear floor space around a voting station and ensures that the manufacturer's voting station design and associated installation instructions support polling place layouts that can achieve this requirement.

In planning a polling place layout, election officials should consult the *U.S Access Board Technical Guide: Clear Floor or Ground Space and Turning Space [USAB14a]* and the *U.S. Department of Justice ADA Checklist for Polling Places [USDOJ16]* to be sure that a voter using a wheelchair can reach the voting station. They should also consider space needed if a voter's assistant also uses a mobility device.

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 [USAB14b].*

Discussion

This requirement is part of *Section 508 [USAB18]*. with the text of the requirements for reach height and depth with illustrations in the "#407 operable parts" section.

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 abilities 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.

A guide to meeting the requirements in the ADA standard for ensuring that voters can reach and us all operable parts can be found at *[USAB14b]*.

7.2-R – Control labels visible

Labels for physical controls used by voters must be placed:

1. on a surface of the voting system where voters can see them from a 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.

Discussion

This requirement provides a general scope that supports the other requirements in 7.3. It is meant to encourage innovation in meeting this principle while ensuring that any new design features not covered explicitly in 7.3 help and not hinder voters in understanding and voting their ballots effectively.

7.3-B – No split contests

The voting system must have the capability of displaying 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.

Related requirements: 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.

1. In an electronic ballot marking interface, the information for each contest includes, in a consistent order: 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.

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 spatial relationship in the ballot layout, must be consistent throughout the ballot for each type of contest.

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.

This requirement ensures that the mechanism for marking a selection in a contest to elect one or more candidates to an office is not to the left of some candidates' names and to the right of others.

If there is more than one spatial relationship, the difference should not be contradictory or confusing to a voter when combined on a single ballot.

Related requirements: 2.2-A – User-centered design process
5.2-A – No bias
7.3-N – Instructions for voters
8.3-A – Usability tests with voters

7.3-E – Feedback

The voting system must provide unambiguous feedback confirming the voter's selection.

Discussion

This requirement applies to electronic interfaces because on paper ballots the voter supplies the mark to indicate a selection, not the voting system. For example, the system can display a checkmark beside the selected option or conspicuously change its appearance.

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.

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 both electronic ballot interfaces and scanners and precinct-count optical scanners in *7.3-H – Overvotes* and in *7.3-I – Undervotes.*

This requirement supports *HAVA [HAVA02]*.

Related requirements: 5.2-F – Preserving votes
7.3-H – Overvotes
7.3-I – Undervotes

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:
    a. the voter's selections for that contest,
    b. a notification that they have not made a selection, or
    c. a notification that they have made fewer selections than allowed;
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 marks and casts a paper ballot.

Discussion

This requirement is an implementation of the *HAVA [HAVA02]* 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.

Related requirements:	5.2-F – Preserving votes 7.3-H – Overvotes 7.3-I – Undervotes

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 that identifies specific contests that have been overvoted in visual format, and with either audio format or sound cues.

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.

Voters marking paper ballots can be informed of the effect of overvoting through appropriately placed instructions.

This requirement supports *HAVA [HAVA02]*.

Applies to:	Electronic interfaces and ballot scanners
Related requirements:	5.1-D – Accessibility features 7.2-C – Voter control 7.3-K – Warnings, alerts, and instructions

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.

This requirement supports *HAVA [HAVA02]*.

Applies to:	Electronic interfaces and scanners
Related requirements:	7.2-C – Voter control
	7.3-K – Warnings, alerts, and instructions

7.3-J – Notification of casting

1. The voting system must notify the voter in both visual and audio format whether their ballot was successfully or unsuccessfully cast. If a ballot is not successfully cast (that is, the device did not complete the documented procedures for the system, including reading a paper ballot, recording an electronic image or record, or transporting the ballot to a ballot box), the voting device must notify the voter and provide clear instruction as to the steps the voter needs take to cast the ballot.
2. A scanning device must be capable notifying the voter that they have cast a paper ballot that is blank on one or both sides. The system may provide a means for an authorized election official to deactivate the notification of a blank ballot.

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.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

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:
    a. the nature of the issue or problem,
    b. whether the voter has performed or attempted an invalid operation or whether the voting system itself has malfunctioned in some way, and
    c. the responses available to the voter.
2. Each step in an instruction or item in a list of instructions must be separated:
    a. spatially in visual formats, and
    b. with a noticeable pause in audio formats.

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.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.

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. The exception is based on the *ADA Standards for Accessible Design. Chapter 7 [ADA10]*.

Related requirements: 7.1-N – Tactile keys
7.2-R – Control labels visible
8.1-E – Standard audio connectors
8.1-I – Standard PAT jacks

7.3-M – Identifying languages

A vote-capture device or other voting session device that offers language options to a voter must:

1. visibly present the controls to identify or change language on the screen at all times, not hidden within a help or settings feature, and
2. include the native version of each language name in the list of language options.

Discussion

Voters looking for an option for an alternative language can recognize it more easily as it is written in the language itself.

The English name or spelling can also be used to identify language, along with the native name.

Applies to: Electronic interfaces

7.3-N – Instructions for voters

The voting system must provide voters access to 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. Voting systems must present instructions 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 verify and cast, 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.

Related requirements: 5.1-F – Accessibility documentation

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:
    a. presented at a level appropriate for election workers who are not experts in voting system and computer technology, and
    b. in a format suitable for use in the polling place.
2. Printed procedural instructions, and on-screen instructions and messages must enable the election workers to verify that the voting system
    a. has been set up correctly (setup),
    b. is in correct working order to record votes (polling), and
    c. 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. Specific guidance on how to implement this requirement is contained in *[NIST08]*.

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.

Related requirements: 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 of 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."

For specific guidance on how to implement this requirement, see *[NIST09a].* 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.

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 for usability with a wide range of representative voters, including those with and without disabilities.

8.4 - The voting system is evaluated for usability with 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 he 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, the display must have the following characteristics:

1. For all electronic display screens:
    a. antiglare screen surface that shows no distinct virtual image of a light source or a means of physically shielding the display from such reflections, and
    b. minimum uniform diffuse ambient contrast ratio for 500 lx illuminance: 10:1.
2. If the display is the primary visual interface for making vote selections:
    a. minimum diagonal display size: 12 inches, and
    b. minimum display resolution: 1920 x 1080 pixels.
3. If the display screen is for messages to voters or poll workers:
    a. minimum diagonal display size: 7.9 inches, and
    b. minimum display resolution: 1024x768 pixels.

Discussion

Displays that measure larger than the 12-inch diagonal provide the opportunity for ballot layouts that can more easily use large text settings.

Applies to: Electronic interfaces

8.1-B – Flashing

If the voting system emits light 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 [W3C10]* and *Section 508 [USAB18]* software design issue standards.

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 so that a voter's personal assistive devices will not be necessary to operate the voting system correctly.

Discussion

This requirement does not preclude the voting system from providing interfaces to assistive technology. (See definition of "personal assistive devices" in *Appendix A - 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 can use their personal headsets, hearing aids, eyeglasses, canes, or other aids they typically have with them.

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.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

8.1-E – Standard audio connectors

The voting system must provide its audio signal for the audio format interface 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.

Applies to: Electronic interfaces

8.1-F – Discernable audio jacks

The audio jack on any voting station device must be in a location that voters can 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 C63.19-2019 [ANSI19]*.

Discussion

This requirement applies only to telephone style handsets/headphones to ensure their compatibility with assistive hearing devices.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

Related requirements: 6.1-D – Audio privacy
8.1-J – Hearing aids

8.1-H – Sanitized headphones

The voting system must be supplied with a means to sanitize headphones or handsets and instructions for election workers on the procedure to ensure that a sanitized headphone or handset is available to each voter.

Discussion

This requirement can be achieved in various ways, including the use of "throwaway" headphones or sanitary coverings.

8.1-I – Standard PAT jacks

A vote-capture device or voter-facing device 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. The jack must allow only switch activations 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 is related to the requirements for low dexterity modes (in *5.1-A – Voting methods and interaction modes* and in *7.2-A – Display and interaction options*). It ensures that voters with very low dexterity, in particular those who do not have the use of their hands can use the vote-capture devices by providing a means for them to connect personal assistive technology (PAT) if they cannot use the supplied touch or tactile input devices.

Examples of personal assistive technology switches include dual switches (sometimes called “adaptive switches” or “jelly switches”) and "sip and puff" devices that communicate as a single key press.

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.

The PAT jack is separate from the audio jack required in *8.1-F – Discernible audio jacks*, which connects to the audio output provided by the system.

Related requirements: 5.1-A – Voting methods and interaction modes
7.2-A – Display and interaction options

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 for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19-2019 [ANSI19].*

Discussion

"Hearing devices" include hearing aids and cochlear implants.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

Related requirements: 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 *IEC/UL 62368-1 [UL19], Edition 3: Standard for Audio/video, Information and Communication Technology Equipment - Part 1: Safety requirements* 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 62368-1 [UL19]*.

Discussion

IEC/UL 62368-1 is a comprehensive standard for IT equipment and addresses all the hazards discussed above under Safety. It replaces *IEC/UL 60950-1 [UL07].*

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 version of *Section 508 Information and Communication Technology (ICT) Final Standards and Guidelines [USAB18]*, in effect as of January 18, 2018, and the *WCAG 2.0 Level AA checkpoints [W3C10]* included in that standard.

Discussion

This applies to all parts of the voting system including the election management system (EMS).

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. This requirement also supports the ADA *[ADA10].*

Applies to: Electronic interfaces, including EMS

8.3 – The voting system is evaluated with a wide range of representative voters, including those with and without disabilities.

8.3-A – Usability tests with voters

The manufacturer must conduct usability tests with voters using the voting system, including all voter activities in a voter session from ballot activation to verification and casting.

The test participants must include voters who represent the following:

1. General population, using the visual interface (without audio), including:
    a. voters who are native speakers of the language being tested for each language defined as supported in the technical data package (TDP);
    b. blind voters, using the audio format plus tactile controls;
    c. voters with low vision, using the enhanced visual features with and without audio; and
    d. voters with limited dexterity, using the visual interface with low and no dexterity controls.
2. The manufacturer must submit a report of the results of their usability tests, including effectiveness, efficiency, and satisfaction measures, as part of the TDP using *ISO/IEC 25062:2006: Common Industry Format (CIF) for Usability Test Reports [ISO06b].*

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.

Related requirements: 2.2-A – User-centered design process
5.1-D – Accessibility features

8.4 – The voting system is evaluated for usability with election workers.

8.4-A – Usability tests with election workers

The manufacturer must conduct usability tests of the voting system setup, operation during voting, and shutdown as documented by the manufacturer, with representative election workers, to demonstrate that election workers can learn, understand, and perform these tasks successfully.

The tasks to be covered in the test must include:

1. Setup and opening for voting, which involves:
    a. operation during voting;
    b. use of assistive technology or language options that are part of the voting system;
    c. shutdown at the end of a voting day during a multi-day early voting period, if supported by the voting system;
    d. shutdown at the end of voting including running any reports;
    e. providing ballots in different languages;
    f. selecting the correct ballot type (for example, for vote centers); and
    g. setting up the voting system to use different display formats and interaction modes.
2. The test participants must include election workers representing a range of experience.
3. The manufacturer must submit a report of the results of their usability tests, as part of the TDP using *ISO/IEC 25062:2006: Common Industry Format (CIF) for Usability Test Reports [ISO06b].*

Discussion

Voting system manufacturers 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. This requirement covers the 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.

Related requirements: 2.2-A – User-centered design process
7.3-O – Instructions for 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 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. Delivery, return, and non-voting equipment process used for vote-by-mail fall out of the scope of the VVSG and is often based on jurisdictional procedure.

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. These requirements ensure that failures in voting system software can be detected and rectified

2 – Tamper-evidence requires the records used to record ballet selections cannot be undetectably altered. These 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 requires that voting machines allow voters the opportunity to verify that the system correctly interpreted their ballot selections, identify errors with their selections, and restart a voting session if a ballot is unacceptable. Records that protect against software failures only work if voters can verify their selections are correct.

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 requirements that paper-based (not cryptographic end-to-end verifiable) voting systems 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 - Cryptographic E2E verifiable deals with cryptographic protocols used in cryptographic E2E verifiable (not paper-based) voting systems, requiring that they be publicly available for review for 2 years before being used in a voting system. Individuals who vote on a cryptographic E2E verifiable system 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.

In 9.2 – Audit support requires that manufacturers identify the types of audits supported by a voting system, ensuring the system can handle audits held by election officials. The manufactures are also required to include any artifacts that the voting system produces to support the identified audits.

In 9.3 - Resilient records requires the data protection requirements under *Principle 13: Data Protection* are followed to ensure that voting system records are resilient in the presence of both intentional forms of tampering and accidental errors.

In 9.4 - Efficient audits covers requirements that ensure the system that will produce the records that allow election officials to conduct risk-limiting audits. Risk-limiting audits can detect the accuracy of a vote count within this specified margin of error.

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.

1. The voting system must meet the requirements within the Paper-based System Architectures or Cryptographic E2E Verifiable System Architectures section, or both.
2. The voting system documentation must include the method used to provide software independence.

Discussion

Software independence *[Rivest06]* 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 must 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 software independence:

- through the use of independent voter-verifiable paper records, and
- cryptographic E2E verifiable voting systems.

Paper-based and cryptographic E2E verifiable system architectures are software independent and both can be used within the same voting system. In this case where a voting system is identified as being a combination of both architectures, the system would need to be compliant with both sets of

requirements. However, a system that meets all of the paper-based requirements need not satisfy the E2E-requirements even if it incorporates E2E verifiable functionality.

Knowing the specific mechanism used to achieve software independence assists with determining if the system is truly is software independent.

The documentation should explain how any changes to the election outcome are detectable regardless of any fault or error in the voting system software. This may include how the voting systems handles a ballot after it is cast by the voter. For example, this documentation may answer the following questions:

- Is it able to print on the ballot?
- What information is printed on the ballot?
- Where is that information printed?

Related requirements can be found under: 9.1.5 – Paper records
9.1.6 – Cryptographic E2E verifiable

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 CVRs, ballot images and artifacts from a cryptographic E2E verifiable voting system.

The record also ensures that identified issues and other problems cannot be lost or unintentionally modified once they are discovered.

9.1.2-B – Tamper-evident record creation

Paper records or other tamper-evident electronic records of the voter's ballot selections must be captured when each ballot is cast.

Discussion

Voter-facing scanners and other vote-capture devices produce the paper records or other tamper evident electronic records. These records can be useful artifacts for post-election audits.

Applies to: Voter-facing scanners and electronic ballot markers

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

- Voter-facing scanners and other vote-capture devices can be used to meet this requirement. An electronic ballot marker can print a voter's ballot selections to review before casting. An E2E verifiable system can print a receipt that allows a voter to verify their selections are tabulated and captured correctly. *Principle 7: Marked, Verified, and Cast as Intended* includes more requirements for voter verification.

Applies to: Voter-facing scanners and electronic ballot markers
Related requirements: 7.3-G – Full ballot selections review

9.1.3-B – Ballot error correction

The voting system must allow a voter to start a new voting session if they would like to correct an error found in their ballot selections.

Discussion

If, after printing their ballot, a voter decides they would like to update or change a selection before casting, the voter must be able to get a new ballot and start a new voting session to mark their ballot as they intend. A voter can contact a poll worker to spoil their current ballot, receive a new ballot, and start a new voting session.

Applies to: Paper-based system architectures
Related requirements: 7.3-F – Correcting the ballot

9.1.3-C – 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.

9.1.4-B – 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 and demonstrates software independence. This documentation could be used as a starting point for election officials to develop the procedures used to audit an election.

Related requirements: 9.1.1-A – Software independent

9.1.5 – Paper records

9.1.5-A – Paper record production

A paper-based voting system must produce a voter-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.

Related requirements: 3.3-C – Bar and other codes

3.3-D – Ballot selection codes
5.1-E – Reading paper ballots
6.1-A – Preserving privacy for voters
6.2-A – Voter independence
9.1.5-C – Paper record intelligibility
9.1.5-D – Matching selections

9.1.5-B – Paper record retention

A paper-based voting system must retain a paper record of the voter's ballot selections.

9.1.5-C – Paper record intelligibility

The recorded ballot selections must be presented in a human-readable format that is understandable by the voter.

Discussion

The requirement ensures that a human-readable version of the data is also printed whenever a barcode is used to encode ballot selections.

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 barcode representations of a voter's ballot selections must use an open and interoperable format.

Related requirements: 3.3-C – Bar and other codes
3.3-D – Ballot selection codes

9.1.5-F – Unique identifier

A paper-based voting system must be capable of adding a unique identifier after a voter casts their ballot.

Discussion

Although not all jurisdictions may use this feature, voting systems are required to have the capability to add a unique identifier to ballots.

Applies to:	Paper-based system architectures
Related requirements:	1.1.5-G – Record audit information 9.4-A – Risk-limiting audit 9.4-B – Random numbers supporting audit processes 9.1.1-A – Software independent

9.1.5-G – Preserving software independence

After a voter verifies their selections on a voted ballot and submits the ballot for casting, a paper-based voting system must not be capable of making an undetectable change to the paper record.

Discussion

After a voter verifies and submits their ballot, a voting system may print on paper ballot to apply a unique identifier that is later used for auditing purposes. To preserve software independence the voting system should not be able to print over or within the ballot selection area because that would cause an undetectable change to the election outcome. Instead the voting system should only be able to print outside of the bounds of the ballot selection area and may also create further distinction by printing in a different font style or color.

This printing process should be preserved regardless of software or hardware updates.

Related requirements:	9.1.1-A – Software independent

9.1.6 – Cryptographic E2E verifiable

9.1.6-A– Verified cryptographic protocol

The E2E cryptographic protocol used by the cryptographic E2E verifiable voting system must be evaluated and approved through a public process established by the EAC.

Discussion

Due to the lack of E2E verifiable voting systems available within the current market, there are no verified E2E cryptographic protocols. A standard public process for approval of the E2E cryptographic protocols will need to be established outside of the VVSG. Once this process is established, the VVSG requirements can point to the approved/verified cryptographic protocols as acceptable for use within an E2E verifiable voting system.

9.1.6-B – Independent evaluation of E2E cryptographic protocol implementation

A cryptographic E2E verifiable voting system must undergo an independent evaluation to verify it correctly and securely implements an approved E2E cryptographic protocol.

Discussion

An independent evaluation can be performed by any entity outside of the voting system manufacturer. Example best practices include using guidance from the *FIPS 140 series [NIST01, NIST19a], NIST SP 800-133 Revision 2, Recommendation for Cryptographic Key Generation [NIST20f],* or *NIST SP 800-175B*, *Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms [NIST20g].* The independent evaluation and cryptographic engineering best practices used can be documented and submitted.

Lessons learned from the analysis of the source code of the Swiss Post system shows the value in making this code available for public review. See "How not to prove your election outcome" *[Lewis19b],* and "Ceci n'est pas une preuve" *[Lewis19a].*

9.1.6-C – Cryptographic ballot selection verification by voter

A cryptographic E2E verifiable voting system must:

1. be capable of providing evidence that an individual voter can use to confirm that the voting system correctly interpreted their ballot selections, while in the polling place; and
2. provide evidence such that if there is an error or flaw in the interpretation of the voters' selections, the evidence can be used for detection of the error or flaw.

Discussion

This requirement addresses cast-as-intended verification, which is one of the principal components necessary to achieve end-to-end- verifiability *[Benaloh14].*

Interpretation is the process by which the voting system converts the voter's contest option selections into the format used to store these selections. Therefore, this evidence must sufficiently prove the representation of the voter's contest option selections in digital form matches the voter selections as provided to the system.

Giving voters the opportunity to verify the voting system stored their ballot choices correctly is a fundamental building block in an end-to-end verifiable voting system.

See "End-to-end verifiability" *[Benaloh14]* and "Usability is not Enough: Lessons Learned from 'Human Factors in Security' Research for Verifiability" *[Kulyk18]* for more information on the various implementations of this technique.

Related requirements: 6.2-A – Voter independence
7.3-G – Full ballot selections review
9.1.6-E – Ballot receipt
10.2.4-A – Voting information in receipts

9.1.6-D – Methods for cryptographic ballot selection verification

1. A cryptographic E2E verifiable voting system documentation must include: the method for the voter to use the evidence provided for ballot selection verification to verify the correct interpretation of their ballot; and
2. a list of known verification tools, their supplier, and how the verification tools are used.

Discussion

Voter intent verification often relies on external verification tools to assist voters in the verification step(s). These can be external verifiers, which is either a second device, a website of a trusted institution, or software running inside the polling location. The manufacturer must provide documentation explaining the verification options available to voters. If the jurisdiction is expected to provide the verification tool or service, this must also be documented.

Related requirements: 9.1.6-C – Cryptographic ballot selection verification by voter

9.1.6-E – Ballot receipt

A cryptographic E2E verifiable voting system must provide a voter with a receipt that allows them to verify that their ballot has been correctly recorded and tallied by the system. These receipts

1. must not display any ballot selections made by the voter;
2. must not enable the voter to prove their selections on the cast ballot to others;
3. must be represented in a publicly documented format;
4. may contain a unique identifier; and
5. are accessible, verifiable, and preserve voter-privacy.

Discussion

This evidence should fail to confirm a voter's ballot has been correctly recorded and tallied by the system if the ballot has been removed, tampered with, or its selections altered, added to, or removed.

Related requirements: 6.1-A – Preserving privacy for voters
6.2-A – Voter independence
7.3-G – Full ballot selections review
8.3-A – Usability tests with voters
10.2.4-A – Voting information in receipts

9.1.6-F – Disputes involving ballot receipts

The cryptographic E2E verifiable voting system documentation must provide procedures for collecting, investigating, and adjudicating disputes from voters based on the contents of their ballot receipts.

Discussion

This documentation will include a process to address the scenario where a voter attempts to verify with their ballot receipt and believes there is a problem with their ballot receipt

Related requirements: 9.1.6-E – Ballot receipt

9.1.6-G – Evidence export

A cryptographic E2E verifiable voting system must:

1. be capable of exporting all evidence supporting ballot tabulation verification, and
2. provide the export in an open and consumable format.

Discussion

Most recorded-as-cast verification approaches require the public posting of the evidence at some point after all ballots have been aggregated and tallied. As required in the previous requirement, the evidence must not reveal how voters voted.

9.1.6-H– Mandatory ballot availability

A cryptographic E2E verifiable voting system must be capable of exporting all encoded ballots for public posting.

Discussion

The public posting does not have to be provided by the voting system, but the voting system must provide the evidence such that it can be published, and the verification process made accessible to voters. The public posting of these exported encoded ballots is performed by election officials and is an essential part of the E2E verifiable process. It allows the public to verify the election results.

9.1.6-I – Verification of encoded votes documentation

A cryptographic E2E verifiable voting system documentation must include:

1. the expected method by which voters will perform the ballot tabulation verification, and
2. how this method provides voters with the opportunity to verify that their ballots are included within the tabulation results.

Discussion

For example, a common method is to publish the evidence to a public bulletin board. The manufacturer should document this method or its alternative. The bulletin board, itself, might not be included in the scope of the voting system but the voting system must provide an export of the evidence to be published on the bulletin board.

9.1.6-J – Verifier reference implementation

A cryptographic E2E verifiable voting system documentation must include:

1. a free publicly available reference implementation of a tool which can be used:
    a. to verify evidence provided to a voter to prove that their ballot choices were correctly interpreted, and
    b. to verify the evidence reported for voters to perform ballot tabulation verification;
2. the build instructions for the reference implementation, along with the tool.

Discussion

For the system to support the cast-as-intended property of end-to-end verifiable systems there must be at least one tool available to voters to verify that their ballot selections have been correctly interpreted. Additionally, for a cryptographic E2E system be software independent, the voters need to have choices about what software use and trust when performing verification. By providing an open source reference implementation may facilitate development of third-party verification tools.

Related requirements: 9.1.6-C – Cryptographic ballot selection verification by voter

9.1.6-K – Privacy preserving, universally verifiable ballot tabulation

A cryptographic E2E verifiable voting system tabulation process must preserve the privacy of every voter and provide a method for public verification.

Discussion

To be publicly verifiable, the approach provides a means for any auditor or observer to verify the correct decryption and tabulation of the votes (not necessarily in that order) using cryptographic proofs that are generated by the process.

Related requirements: 6.1-A – Preserving privacy for voters

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 – Audit support documentation

The voting system documentation must specify the types of audits the voting system supports and the artifacts that the voting system provides to support those audits.

Discussion

Ballots, CVRs, and ballot images are examples of artifacts that can support a post-election audit.

Related requirements: 1.1.9-A – Post-election reports
3.1.3-D – Audit procedures

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 Guidelines *13.1* and *13.2* that are related to protecting audit records.

Discussion

CVRs and ballot images need sufficient data protection because they are needed for audits.

Related requirements: 13.1.2-A – Integrity protection for election records
13.2-A – Signing stored election records
13.2-B – Verification of election records

9.4 - The voting system supports efficient audits.

9.4-A – Risk-limiting audit

A paper-based voting system must produce paper records that allow election officials to conduct a risk-limiting audit.

Discussion

Voting systems contain information which enables election officials to conduct risk-limiting audits. For example, batch subtotal reporting by the voting system, may make the process of ballot sampling more efficient.

An evidence-based election requires convenient access to ballot sheets, ballot sheet images, and cast vote records for efficient and trustworthy public tabulation audits. Vendors should demonstrate how an election system provides all the information necessary for an independent Risk-Limiting Audit (RLA).

Some example features/paper records that may be produced to support risk-limiting audits include the following:

- the ability to associate electronic cast vote records (CVRs) with corresponding paper records while also preserving ballot secrecy;
- the ability to export of CVRs in an open and interoperable format;
- the ability to create a ballot manifest that allows users to identify the physical location of ballots (e.g., scanner name or number, batch number, and ballot sequence number); and
- supporting multi-sheet ballots, including association of each sheet with its corresponding CVR.

Related requirements:
4.1-C – Exchange of cast vote records (CVRs)
9.1.5 – Paper records
9.2-A – Audit support documentation
9.4-C – Unique ballot identifiers
9.4-D – Multipage ballots

9.4-B – Random numbers supporting audit processes

Voting systems that generate or rely on random or pseudo-random numbers for auditing purposes 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.

This documentation should specify:

- how random numbers are generated, and
- what any random numbers are used for.

One common use for random numbers is to create unique identifiers associated with ballots to assist in supporting audits.

The method for generating the pseudo-random numbers should meet the requirement *10.2.2-E Randomly generated identifiers.*

For additional information, see *NIST SP 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators [NIST15a].*

Related requirements: 9.4-C – Unique ballot identifiers
10.2.2-E – Randomly generated identifiers

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. Although the voting system has this capability, this does not require jurisdictions to use this feature if it conflicts with state laws. In order to conduct a ballot-comparison risk-limiting audit, paper ballot records must either be stored in the order in which they were scanned or contain a unique ballot identifier. A unique ballot identifier is a unique ID that provides information about the device it was scanned on and the batch in which it is stored. One example of a unique ballot identifier is: scanner ID, batch ID, and ballot card number. The unique ballot identifier must not tie a ballot to an individual voter

9.4-D – Multipage ballots

The voting system must be able to account for 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.

10.2 - 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.

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 cryptographic end-to-end (E2E) verifiable voting systems. It covers how election workers must select the indirect association option and how these ballots are to be stored separately from cast ballots. It also requires encryption of ballots not yet cast that contain an indirect association.

2 – Identification in vote records covers the use of identifiers for tying cast vote records (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 must also not allow identification of a voter. The goal is to ensure that a voter cannot be identified from the format of the ballot or method of voting. Best practices in polling places are also critical to ensuring that there are enough BMD-printed ballots to preserve ballot secrecy.

3 – Access to cast vote records (CVRs) 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.

4 – Voter information in other devices and artifacts requires that receipts produced by a voting system cannot contain voter information and must not violate ballot secrecy. Logs cannot contain individual or aggregate selections, nor can activation devices create or retain information that can be used to identify a voter's ballot. It should not be possible for any part of the voting system to be used to violate ballot secrecy, including in the absence of a 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.

Discussion

Examples include first name, last name, address, driver's license, and voter registration number and other personally identifiable information (PII). This requirement applies to the voting system itself, as the voting system cannot prevent a voter from self-identifying within write-in fields or other areas of the ballot.

Related requirements: 11.1-B – Voter information in log files

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

Indirect voter associations must only be used to associate a voter with their encrypted ballot selections.

Discussion

Certain channels of voting require indirect associations so that ineligible ballots can be removed before the ballot is read and counted. Some reasons include signature mismatch or death of a voter. The most common example of indirect association would be a randomly generated number. Best practice would ensure that indirect voter associations are only available to authorized election personnel.

This requirement only applies to paperless voting systems that also meet the requirements under *Guideline 9.1*, which states 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: Cryptographic E2E verifiable voting system architectures

10.2.1-C – Use of indirect voter associations

The voting system must only use indirect voter associations when the option is selected at the beginning of a voting session 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. These types of ballots are often considered provisional or recallable ballots.

Applies to: Cryptographic E2E verifiable voting system

10.2.1-D – Isolated storage location

Ballots that are not cast and contain an indirect association must be separated 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: Cryptographic E2E verifiable voting architectures

10.2.1-E – Removal of indirect voter associations

The voting system must be capable of removing the indirect voter association between a ballot and a voter once that voter is determined to be eligible.

Discussion

Provisional or recallable ballots may require indirect associations so that ballots can be removed before casting. After a voter's eligibility is determined the indirect voter association can be removed and the ballot can be added to collection of cast ballots. In the case of electronic E2E systems, whatever data record provides this association must be removed from the system.

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: Cryptographic E2E verifiable voting architectures

10.2.1-F – Confidentiality for ballots with indirect voter associations

The voting system must only be capable of decrypting a ballot after any indirect voter association to it has been removed.

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. The indirect voter association is not encrypted with the ballot.

The voting system must not be capable of decrypting a ballot that still has an indirect association to a voter. A possible approach to implement this is by requiring that a decryption key (or set of keys) be entered to decrypt ballots but disallowing input until after all indirect associations have been removed. If the key is present on the system at the same time as indirect associations, it may be possible for malicious software to decrypt ballots and associate selections with voters.

Applies to: Cryptographic E2E verifiable voting architectures

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: 9.1.5-F – Unique identifier

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 ballots votes are cast.

Discussion

No data or metadata is allowed whether in CVRs and ballot images or elsewhere if that metadata can be used to associate a voter with a record of voter intent. Otherwise, metadata can be useful for verification. For instance, date of creation of record in the voter-facing device might reveal the order of voting. Most other metadata won't be a problem.

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 accidently be used to reference a voter is not used within a file name.

10.2.2-D – Aggregating and ordering

Aggregated and final totals:

1. must not contain voter identifying information, and
2. must not be able to recreate the order in which the ballots were cast.

Discussion

Voter identifying information includes social security number, voter identification number, or driver's license number.

10.2.2-E – Randomly generated identifiers

Randomly generated identifiers used for audits must use random bit generators specified in the latest revision of *NIST SP 800-90* series on random bit generators.

Discussion

This requirement is important to ensure the use of a cryptographically secure pseudo-random number generator (CSPRNG) and also to ensure any random numbers, such as unique identifiers on a ballot, cannot be used to recreate the order in which a ballot was cast. Recreating the order of cast ballots can cause ballot secrecy issues if a voter's ballot can be identified.

To ensure voting system vendors are following the random number generation recommendations in the 800-90 series, they will need to submit to the Cryptographic Module Validation Program (CMVP) and the Cryptographic Algorithm Validation Program (CAVP) for conformance testing.

For additional information, see *NIST SP 800-90A Rev 1*, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators [NIST15a]* and *NIST SP 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation [NIST18a].*

Related requirements: 9.4-B – Random numbers supporting audit processes
10.2.2-D – Aggregating and ordering

10.2.3 – Access to cast vote records (CVR)

10.2.3-A – Restrict access to records of voter intent

The voting system must require administrator-level authorization to access the directory or storage location of CVRs, ballot images, and ballot selections.

Discussion

Cast vote records, ballot images, and ballot selections should be subject to special restrictions on access. Permissions to access these storage locations are limited only to those users who need to access the location. This may be especially essential during voting to protect ballot secrecy and avoid any exposure of results until polls are closed.

Related requirements: 11.3.1-B – Multi-factor authentication for critical operations
11.3.1-C – Multi-factor authentication for administrators
11.4-A – Least privilege for access policies
11.4-B – Separation of duties

10.2.3-B – 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.

This requirement does not apply when the CVR, ballot images, and ballot selections are stored on removable media and removed from the vote-capture device.

Related requirements: 11.1-A – Logging activities and resource access

10.2.4 – Voter information in other devices and artifacts

10.2.4-A – Voting information in receipts

Receipts produced by cryptographic E2E verifiable voting systems must not contain voter information.

Discussion

The voting system must not issue a receipt to the voter that would provide proof to another of how the voter voted.

10.2.4-B – 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-C – Activation device records

Ballot 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* cover 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.

The sections in ***Guideline 11.2*** cover:

1 – Authorized access ensures that only authorized users can access the voting system. All voting systems will have an administrator role 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. Differentiating theses stages helps limit access to the voting system to only those individuals strictly necessary at any given time.

2 – Role-based access control covers 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, limiting each person's access within the system.

The sections in ***Guideline 11.3*** cover:

1 – Access control mechanisms either permit authorized access or prevent unauthorized access to the voting system. This includes the capability of using 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. Multi-factor authentication provides additional security beyond the use of a single password.

2 – User Authentication Credentials 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. The voting system will securely store passwords and other authentication credentials (such as multi-factor authentication codes).

11.4 – Default access control policies enforce the principles of least privilege, minimizing access within the system to only what is strictly necessary, and separation of duties, narrowing roles so that access isn't granted too broadly for any group of users.

11.5 – Logical access restrictions. 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. This can help prevent unauthorized use if a system is left unattended.

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; and
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.

11.1-B – Voter information in log files

The voting system must not log any voter identifying information.

Discussion

The logging and storing of voter identifying information after a ballot is cast potentially violates voter privacy and ballot secrecy. Examples of voter identifying information include first name, last name, address, driver's license, and voter registration number.

Related requirements: 10.1-A – System use of voter information
10.2.4-B – Logging of ballot selections

11.1-C – Preserving log integrity

The voting system must prevent:

1. the logging capability from being disabled;

2. the log entries from being modified in an undetectable manner; and
3. The deletion of logs; with the exception of log rotation.

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.

The removal of logs is only appropriate for log rotation, which is when the stored logs are rotated out to create more space for continuous logging. The voting system should be capable of rotating the event log data to manage log file growth. Log file rotation may involve regular (e.g., hourly, nightly, or weekly) moving of an existing log file to some other file name and/or location and starting fresh with an empty log file. Preserved log files may be compressed to save storage space.

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.

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

Stage	Description
Pre-voting	Loading, and configuring device software, maintenance, loading election-specific files, preparing for election day usage
Activated	Activating the ballot, printing, casting, spoiling the ballot
Suspended	Occurring when an election official suspends voting

Post-voting	Closing polls, tabulating votes, printing records

Discussion

The groups or roles in 11.2-H (Table 11- 2) will be given specific permissions which can be affected by the voting stage (Table 11-1).

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.

An 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 [ANSI04]* document.

Discussion

This requirement extends *[VVSG2005] I. 7.2.1.1-a* by requiring role-based methods to follow *ANSI INCITS 359-2004 [ANSI04].*

11.2.2-B – Minimum groups or roles

At minimum, voting systems that implement RBAC must define groups or roles with the role descriptions within Table 11-2.

Table 11-2 – Minimum voting system groups or roles for RBAC

Group or role	Role description
Administrator	Can update and configure the voting devices and troubleshoots system problems.
Voter	A restricted process in the vote-capture device. It allows the vote-capture device to enter the activated state for voting activities.
Election Worker	Has the ability to open the polls, close the polls, recover from errors, and generate reports; Checks in voters and activates the ballot style; Loads ballot definition files.

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 – Minimum voting system groups or roles for RBAC* and the voting stages from *Table 11-1 – Voting stage descriptions*, to assign the minimum permissions in *Table 11-3*.

Discussion

Table 11-3 – Minimum permissions for each group or role 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

Group/Role	System	Pre-Voting	Activated	Suspended	Post-Voting
Administrator	EMS	Full Access	Full Access	Full Access	Full Access
	Electronic BMD	Full Access	Full Access	Full Access	Full Access
	Voter-Facing Scanner	Full Access	Full Access	Full Access	Full Access
Voter	EMS	---	---	---	---
	Electronic BMD	---	Vote and cast ballots	---	---
	Voter-Facing Scanner	---	Ballot Submission	---	---
Election Worker	EMS	Define and load election programming	---	---	Reconcile provisional or challenged ballots, write-ins, generate reports
	Electronic BMD	Open polls, L&A	Close or suspend polls, Recover from errors, Activate ballot and cancel unvoted ballots	Exit suspended state	Generate reports

	Voter-Facing Scanner	Open polls, L&A	Recover from errors	Exit suspended state	Generate reports

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 mechanisms

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; and
- 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.

11.3.1-B – Multi-factor authentication for critical operations

At a minimum, the voting system must be capable of using multi-factor authentication to verify a user has authorized access to perform critical operations, including:

1. runtime software updates to the certified voting system;
2. aggregation and tabulation;
3. enabling network functions;
4. changing device states, including opening and closing the polls;
5. deleting or modifying the CVRs and ballot images; and
6. modifying authentication mechanisms.

Discussion

NIST SP 800-63-3, Digital Identity Guidelines [NIST17c] 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)

Multi-factor authenticators can be tested for usability to ensure an appropriate balance of security, usability, and functionality. A significant impact to usability may require revision of the multi-factor authenticator implementation.

Related requirements: 8.4-A – Usability testing with election workers

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.

11.3.2 – User authentication credentials

11.3.2-A – Username and password management

If the voting system uses a username 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.

11.3.2-B – Password complexity

The voting system must, at minimum, meet the password complexity requirements within the latest version of *NIST SP 800-63B Digital Identity Guidelines* standards.

Discussion

NIST SP 800-63B [NIST17d] does not specify any additional password complexity requirements besides password length. At the time of this writing, the only recommended password complexity requirement is a minimum password length of 8 characters. *NIST SP 800-63B* also recommends that if a password is provided to the user it may be 6 characters and all numeric. NIST's password complexity recommendations are meant to make it easier for users to memorize their passwords, while decreasing user frustration.

11.3.2-C – Secure storage of authentication data

The voting system must store authentication data in a way that ensures confidentiality and integrity are preserved.

Discussion

Ensuring the confidentiality of stored authentication data (such as passwords) may involve the use of cryptography. The best practice at the time of this writing is to store a salted, one-way hash of passwords. Additional guidance for protecting authentication data can be found in *NIST SP 800-63B, Digital Identity Guidelines [NIST17d].*

11.3.2-D – Password disallow list

The voting system must compare all passwords against a manufacturer-specified list of well-known weak passwords and disallow the use of these weak passwords.

Discussion

Examples of common weak passwords include 0000, 1111, 1234.

11.3.2-E – Usernames within passwords

The voting system must ensure that the username is not used in the password.

Discussion

This requirement extends by restricting the use of usernames and related information in 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

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.

At the time of this writing, *NIST SP 800-12 [NIST17e]* defines "least privilege" as "the principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function."

Network access will also follow the principle of least privilege to ensure that devices only receive as much access as is necessary to perform the desired function.

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 – Session time limits

The voting system must enable an administrator the ability to do the following:

1. set the maximum time limit for a user's session, and
2. set the maximum time limit for user inactivity.

Discussion

NIST SP 800-63B [NIST17d] recommends a max session time of 12 hours regardless of inactivity and a max inactivity time of 30 minutes. Elections consist of temporary employees and user access may only be required during an election. A user's access may expire and terminate automatically at the end of an election.

Related requirements: 11.5-B – Reauthentication

11.5-B – Reauthentication

The voting system must require reauthentication of an authorized user after the administrator-specified time limit for the user's session or for user inactivity.

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.

For voters, session times are specified under requirement *7.2-O – Inactivity alerts*.

For more information, see *NIST SP 800-63B [NIST17d]*.

Related requirements: 7.2-O – Inactivity alerts
11.5-A – Session time limits

11.5-C – 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. *NIST SP800-63B* recommends allowing 5-10 attempts before starting 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

11.5-D – 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.

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 protect the physical security 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 alert 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 must be tested and be 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 or expose 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. The 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 to voting systems 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.

12.1-B – Unauthorized physical access alert

Voter-facing scanners and electronic BMDs must produce an alert if access to a restricted voting device component is detected during the activated voting stage.

Discussion

This alert is meant to call attention to election workers in the polling place.

More information about the activated stage is defined in *Table 11-1.*

Related requirements: 11.2.1-C – Access control by voting stage

12.1-C – Disconnecting a physical device

Voter-facing scanners and electronic BMDs must produce an alert if a connected component is physically disconnected during the activated voting stage.

Discussion

An alert can be provided in the form of an alarm to provide an audible and/or visual alert. 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 alert.

More information on the activated stage is defined in *Table 11-1*.

12.1-D – Logging of physical connections and disconnections

The voting system must log when a voter-facing scanner, electronic BMD, or other component is connected or disconnected during the activated voting stage.

Discussion

Logging of the devices is vital for determining cause and providing incident information if a physical security event occurs.

Related requirements: 11.2.1-C – Access control by voting stage
15.1-D – Logging event types

12.1-E – Secure containers

Unauthorized physical access to a container that stores or transports 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 requirements in *Principle 9-Auditable*, containers which hold either paper or electronic voting system records needed for audits need to be secure against physical access. An example of a physical container includes ballot boxes integrated and sold as part of the voting system.

Applies to: Voter-facing scanners, BMDs

12.1-F – Secure locking systems

If the voting system uses locks it 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

A lock used on the voting system can be evaluated against UL437 door locks and locking cylinders requirements. See *[UL13]* for UL listing for *door locks and locking cylinders* within the standard to review requirements for lockpicking and the attack resistance tests.

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-G – Backup power for power-reliant countermeasures

If the voting system uses a powered physical security countermeasure, that physical countermeasure must maintain its state when power is removed and must have a backup power supply. In addition, switching from primary power supply to backup power supply:

1. produces an alert;
2. happens automatically when primary power is unavailable; and
3. generates an event log entry, if possible.

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. Once primary power is unavailable, the switch to back up power should be automatic to avoid any gaps in functionality if the switch must be done manually.

If the physical countermeasure leverages the voting system's operating system, it can create an event log entry when it is switched to backup power. 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.

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 system must only expose 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, and panels, and vents. Voting operations include voting device upgrades and maintenance.

12.2-B – Physical port auto-disable

If a physical connection that supports digital communication between voting system components is broken during an activated or suspended state, the affected voting system port must be automatically disabled.

Discussion

Automatically disabling will require an election worker's attention to re-enable and re-attach any cabling. This remediation is required for continuity and to address any tampering. An added feature could be that the specific election worker performing maintenance is uniquely identified within the logs, but this is not required. This requirement does not include power cabling with a backup power supply or analog accessibility device ports that are used during the activated voting stage.

12.2-C - Physical port restriction

Voting systems must restrict physical access to voting system ports that accommodate removable media, with the exception of ports used to activate a voting session.

Discussion

Physical port access needs to be restricted when not in use. This requirement is not meant to impede the use of accessible technology. This requirement assists in restricting adversaries from adding wireless adapters or other malicious adapters to the voting system.

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.

12.2-D – Disabling ports

Voting systems must allow authorized administrators to logically 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.

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-C – Physical port restriction* applies to physical restrictions, whereas *12.2-D – Disabling ports* discusses logical disabling of ports.

Related requirements: 15.1-D – Logging event types

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*** **include**:

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. Configuration files contain important settings, including security settings, and altering them could impact the overall system

2 – Elections records deals with the need for the vote-capture and tabulation system and the EMS to protect the integrity of the cast vote records (CVRs) and ballot images when they are stored in the voting device. These protections should prevent undetectable changes to CVRs and ballot images.

13.2 – Source and integrity of election records covers the requirement that CVRs 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. Digital signatures are a form of integrity protection that can also help trace the source of any updates or alterations to election records.

13.3 – Cryptographic algorithms deals with the requirements that cryptographic functionality be implemented in a cryptographic module validated against *Federal Information Processing Standard (FIPS) 140 [NIST01]*. In addition, cryptographic functions specific to E2E cryptographic voting protocols must adhere to requirements set by the EAC 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 by election officials.

13.4 – Protecting sensitive data transmission 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 voting system receiving data 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.

Applies to:	Vote-capture and tabulation system
Related requirements:	11.2.1-A – Ensuring authorized access

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.

Applies to:	EMS workstation
Related requirements:	11.3.1-C – Multi-factor authentication for administrators 15.1-E – Configuration file access log

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.

Applies to:	Network appliance
Related requirements:	11.3.1-A – Access control mechanism application

13.1.2 – Election records

13.1.2-A – Integrity protection for election records

The voting system must integrity prevent modification of CVRs and ballot images when they are stored anywhere within the voting system.

Discussion

Applying access control can help prevent any unauthorized modifications to CVRs and ballot images.

Applying integrity protection ensures that any unauthorized modifications to CVRs and ballot images can be detected.

For example, ballot images can be integrity protected using a private key maintained in a Hardware Security Module and a cryptographic signature of the image.

Related requirements:	13.2-A – Signing stored election records 13.2-B – Verification of election records

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

13.2-A – Signing stored election records

Cast vote records and ballot images must be digitally signed when stored and before being transmitted.

Discussion

Digital signatures address the threat that the records might be tampered with when stored or transmitted. Cryptographic hashes do not sufficiently mitigate this threat, as election records could be altered and then re-hashed. Digital signatures also allow verification of the source of any created or modified records. Additional information can be found in *FIPS 186-4 Digital Signature Standard [NIST13c].*

13.2-B – Verification of election records

A voting system must:

1. cryptographically verify the integrity and authenticity of all election data received;
2. immediately log any verification error of received election results;
3. immediately present on-screen any verification errors; and
4. not tabulate or aggregate any data that fails verification.

Discussion

This process of verifying election data and results is a defense in depth measure against accidental errors or a malicious incident regarding modified or false election records. For example, checking the cryptographic integrity of received election results prevents modified election results from being maliciously modified and reported on election night.

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 current FIPS 140 validation, operating in FIPS mode.

This applies to:

1. software cryptographic modules, and
2. hardware cryptographic modules.

Discussion

Use of cryptographic modules validated at level 1 or above ensures that the cryptographic algorithms used are secure and correctly implemented. The current version of *FIPS 140[NIST01, NIST19a]* and information about the *NIST Cryptographic Module Validation Program* are available under *[NIST20e]* in Appendix C: References. 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.

13.3-B – E2E cryptographic voting protocols

Cryptographic functions specific to E2E cryptographic voting protocols must adhere to requirements set by the EAC and are omitted from FIPS 140-2 validation.

Discussion

The cryptographic E2E verifiable voting protocol used by the voting system is subject to the evaluation in requirement *9.1.6-B – Verified Cryptographic Protocol*. Common place cryptographic operations used within E2E systems, such as encryption, decryption, and hashing, are subject to the *FIPS 140 [NIST01, NIST19a]* validation requirement.

Applies to:	Cryptographic E2E verifiable voting systems
Related requirements:	9.1.6-A – Verified cryptographic protocol

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 *[NIST20a]*. 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.

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.

13.3-E – Cryptographic 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 – Confidentiality and integrity protection of transmitted data

The voting system must:

1. mutually authenticate all network connections;
2. cryptographically protect the confidentiality of all data sent over a network; and
3. cryptographically protect the integrity of all election data sent over the network.

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. Only wired local area network (LAN) communication, such as ethernet, is possible for *VVSG 2.0* voting systems. This requirement includes network appliances such as switches, firewalls, and routers within its scope.

This does not prevent the use of "double encrypted" connections employing cryptography at multiple layers of the network stack. Data, such as ballot images, must be encrypted before transmission.

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. For more information about TLS implementations, see *NIST SP 800-52 rev. 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations [NIST19b].*

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 is designed to limit 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 – Documented resiliency 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 must be carried out by election officials or others to ensure the integrity of the system.

14.2 – Designed to limit attack surface requires that the system will prevent extraneous processes and services from being installed or executed and will disable networking and non-essential features. The voting system should not be capable of wireless networking or connecting to external networks. 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 of restricting 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 – Supply chain 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*.

The sections in ***Guideline 14.3*** include:

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 on-screen alert, and may 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 all application running in userspace against an allowlist that identifies all approved and properly installed applications. It will also protect the integrity and authenticity of the allowlist configuration files.

14.4 – Authorized software updates 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, and
- 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. Some decisions may include prioritizing the mitigation or prevention of high risks that are likely to have a high impact an election. Many methods of conducting risk assessments exist, including *NIST SP 800-30-1: Guide for Conducting Risk Assessments [NIST12] or ISO/IEC 27005:2011 Information technology - Security techniques - Information security risk management [ISO18d].*

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. This requirement assists in providing the evidence that a manufacturer has gone through the risk determination process. *NIST SP 800-53* revision 5 *Security and Privacy Controls for Information Systems and Organizations [NIST20h]* can be useful to identify controls that can assist with addressing any identified threats.

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, and
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 – Non-essential networking interfaces

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 Wi-Fi and Bluetooth should be disabled.

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-B – Network status indicator

If a voting system has network functionality, 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-C – Wireless communication restrictions

Voting systems must not be capable of establishing wireless connections as provided in this section.

Discussion

Wireless connections can expand the attack surface of the voting system by opening it up to over-the-air attacks. Over-the-air access can allow for adversaries to attack remotely without physical access to the voting system. By disallowing wireless capabilities in the voting system, this limits the attack surface and restricts any network connections to be hardwired. Examples of how wireless can be disabled may include the following:

- a system configuration process that disables wireless networking devices,
- disconnecting/unplugging wireless device antennas, or
- removing wireless hardware within the voting system.

This requirement does not prohibit wireless hardware within the voting system so long as the hardware cannot be used e.g. no wireless drivers present.

This requirement applies solely to voting systems that are within the scope of the VVSG. It is not a prohibition on wireless technology within election systems overall. This requirement does not impact or restrict the use of assistive technology (AT) within the polling place. Voters with wireless AT may have to use an adapter that leverages the 3.5 mm headphone jack.

Related requirements: 8.1-E – Standard audio connectors
15.4-C – Documentation for disabled wireless

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 to confirm that wireless networking functionality is 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 – External network restrictions

A voting system must not be configured to:

1. establish a connection to an external network, or
2. connect to any device external to the voting system.

Discussion

The basic instructions provided by a vendor should clearly indicate that the intended use and installation of voting systems implements an air gap between the voting system and external networks or external devices. This requirement is intended to limit the voting systems attack surface and disallow connections of the voting system to technologies such as:

- e-pollbooks,
- public switched telephone networks (PSTNs), and
- cellular modems.

In particular, connections to the internet expand the attack surface even further than other wireless technologies because the data traverses over the internet, which reaches all over the world. This type of access allows a malicious actor to attack from various distances, meaning they do not have to be in close proximity of a polling place or near a specific jurisdiction. Exposure to the internet could allow nation-state attackers to gain remote access to the voting system. With remote access an attacker may be able to view all files within a voting system and make modifications to files within the voting system. These files may include election results and ballot records.

This type of exposure could also make voting systems vulnerable to ransomware. Ransomware is a type of malware that could deny access to election data or functionality, usually by encrypting the data with a key known only to the hacker who deployed the malware. Ultimately an attacker could render a voting system non-operational until a ransom is paid.

Related requirements: 15.4-B – Secure configuration documentation

14.2-F – Secure configuration and hardening documentation

The voting system must follow a secure configuration guide for all underlying operating systems and other voting system components, with any deviations from the secure configuration guidance 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. Some examples include Security Technical Implementation Guides (STIGs) *[DISA20]* and the Center for Internet Security (CIS) benchmarks.

Documenting deviations ensures that important settings are not overlooked and decisions to deviate are properly considered.

Related requirements: 15.4-B – Secure network configuration documentation

14.2-G – Unused code

The voting system software 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 because the surrounding code makes it impossible for a section of code to ever be executed. See *MITRE CWE-561 [MITRE20]*. Software with dead code is considered poor quality and reduces maintainability.

This requirement does not restrict the use of defensive code, such as exception handling to prevent failures because this code is still traversed to check conditions.

14.2-H – Use of exploit mitigation technologies

The voting system must use exploit mitigation technologies including data execution prevention (DEP) and address space layout randomization (ASLR), or equivalent mitigations.

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. If the voting system does not use DEP and ASLR, the equivalent mitigation technologies used must be identified.

Applications need to be written and compiled in such a way as to make use of underlying exploit mitigation technologies.

See the *OWASP Application Security Verification Standard [OWASP19]* for more information about exploit mitigation.

14.2-I – Importing software libraries

The voting system software must import only library components that are necessary.

Discussion

Importing entire software libraries significantly increases the attack surface of the software. Importing only the components of a library, such as modules, functions, or classes needed is a useful attack surface minimization strategy. Following the language's intended import design, such as importing only the specific module needed from a more general "standard" library, will also help with this goal.

This requirement is not intended to encourage developers to avoid the import process by copying code directly to software, which would greatly complicate the update process.

Not all 3rd party libraries are easily modifiable, making this attack surface reduction strategy impractical.

14.2-J – Vulnerability management plan

The voting system documentation must include the plan for how to address vulnerabilities found in the voting system and at minimum include the following:

1. how the voting system design process identifies and addresses well-known vulnerabilities**;**
2. disclosure of all known vulnerabilities within the system,
3. a patch management plan; and
4. the method to receive and send reports of vulnerabilities.

Discussion

This requirement informs how a voting system vendor is able to manage verified vulnerabilities to their voting system.

Certain information can also be included for each vulnerability, such as any severity, impact, or exploitability scores. Tools like the Common Vulnerability Scoring System (CVSS) can be used to communicate the metrics (including the severity) of software vulnerabilities.

For more information about vulnerability and patch management, see *NISTIR 8011 Volume 4, Automation Support for Security Control Assessments: Software Vulnerability Management [NIST20c]* and *NIST SP 800-40, Guide to Enterprise Patch Management Technologies [NIST13b].*

14.2-K – Known vulnerabilities

The underlying voting system platform must be free of well-known vulnerabilities as identified in the vulnerability management plan.

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.

14.3 - 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. the assurance requirements to mitigate supply chain risks;
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;
4. the plan for reviewing and auditing suppliers and partners; and
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…

- following *Appendix E* of *NIST SP 800-161 – Supply Chain Risk Management Practices [NIST15b] for Federal Information Systems and Organizations* guidance (Appendix E provides a supply chain management plan(strategy template).
- utilizing the *NIST Cybersecurity Framework Version 1.1 [NIST18c]* by referencing the Supply Chain Risk Management category and subcategory, and
- referencing the relevant security controls for supply chain in *NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations [NIST20b].*

Contract language provided must include the products or services acquired from the suppliers/partners and any evidence or artifacts that attest to the required level of assurance.

14.3-B – Criticality analysis

The voting system's documentation must include a list of critical components and suppliers defined by a criticality analysis and supplier impact analysis

Discussion

Defining the critical components and supplier 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 [NIST18b]* and *NISTIR 8272, Impact Analysis Tool for Interdependent Cyber Supply Chain Risks [NIST20d].*

14.3-C – 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; and
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 – Criticality analysis*. At minimum the bill of materials for critical components are required, but this does not restrict the voting system vendor from listing the bill of materials for other components.

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.

For more information about the risks of third-party components and developing software bills of materials, see *"Managing Security Risks Inherent in the Use of Third-party Components" [SAFECode19]* and resources from the *National Telecommunications and Information Administration about Software Bills of Materials [NTIA19].*

14.3.1 – Boot integrity

14.3.1-A – Cryptographic boot verification

The voting system must cryptographically verify firmware and software integrity before the operating system is loaded into memory.

Discussion
This requirement does not mandate hardware support for cryptographic verification. 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 – Notification of boot validation failure

If the voting system does not pass boot validation, it must present an on-screen alert and provide any other necessary information to understand the failure.

Discussion
Failure of boot validation needs to be provided to users so these errors can be further analyzed when needed. If the voting system is capable of pre-boot logging, failure information could be stored in a log for future analysis.

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 – Application allowlisting

The voting system must only run applications that have been verified against an allowlist.

Discussion

This requirement helps ensure only authorized applications run on the voting system.

Applies to: Vote-capture device

14.3.2-D – Integrity protection for software allowlists

The voting system must protect the integrity and authenticity of the allowlist configuration files.

Discussion

If the allowlist is improperly modified, the software allowlisting mitigation can be defeated. The most common way of providing allowlist configuration file protection could be a digital signature.

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 updated done by a networked method or performed using physical media.

Related requirements: 11.3.1-B – Multi-factor authentication for critical operations
11.3.1-C – Multi-factor authentication for administrators

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: 11.3.1-B – Multi-factor authentication for critical operations
11.3.1-C – Multi-factor authentication for administrators

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: 11.3.1-B – Multi-factor authentication for critical operations
11.3.1-C – Multi-factor authentication for administrators

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 – Event logging 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 pertaining to:

- general system functions
- networking
- software, and
- voting functions

In addition, when a system administrator is accessing a configuration file, the system needs to log identifying information about the user accessing that file including the user's, group or role.

15.2 – Error messages occur covers the requirement that systems provide immediate notification to the user when an error occurs as well as logging all errors and creating error reports. The system documentation must include procedures for how election officials should handle errors.

15.3 – 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, and
- 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 and remediates malware.

15.4 – Defense 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, as well as any documentation needed to explain how wireless capabilities have been disabled within the system. Documentation also lists security relevant configurations and is accompanied by network security best practices, including air-gap procedures to protect sensitive systems from external networks like the internet.

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, and
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: 10.1-A – System use of voter information
11.1-B – Voter information in log files

15.1-D – Logging event types

At minimum, the voting system must log the events included in Table 15-1.

Discussion

Table 15-1 – System events to log 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.

Logging system events provides insight into general system metrics, errors, and vulnerabilities. Information gathered from logs can be used to improve system performance by preventing future errors/issues or automate issue handling.

Table 15-1 – System events to log

System Event	Description
General system functions	
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.
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 • For paper-based systems, the initiation or termination of scanner and communications equipment operation • Printer errors • Detection or remediation of malware or other malicious software • Cryptographic boot validation success/failure

Non-critical status messages	Non-critical status messages that are generated by the device's data quality monitor or by software and hardware condition monitors.
Events that require election official intervention	Events that require election official intervention, so that each election official access can be monitored, and access sequence can be constructed.
Device shutdown and restarts	Both normal and abnormal device shutdowns and restarts.
Changes to system configuration settings	Configuration settings include but are not limited to registry keys, kernel settings, logging settings, and other voting device configuration settings.
Integrity checks for executables, configuration files, data, and logs.	Integrity checks that can indicate possible tampering with files and data.
The addition and deletion of files.	Files that are added or deleted from the voting device.
System readiness results	Includes but is not limited to: • 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.
Backup and restore	Successful and failed attempts to perform backups and restores.
Authentication and Access Control	
Authentication related events	Includes but is not limited to: • Login/logoff events (both successful and failed attempts) • Account lockout events • Password changes
Access control related events	Includes but is not limited to: • Use of privileges (such as a user running a process as an administrator)

	• Attempts to exceed privileges • All access attempts to application and underlying system resources • Changes to the access control configuration of the voting device
User account and role (or groups) management activity	Includes but is not limited to: • Addition and deletion of user accounts and roles • User account and role suspension and reactivation • Changes to account or role security attributes such as password length, access levels, login restrictions, and permissions • Administrator account and role password resets
Networking	
Enabling or disabling networking functionality	Includes but is not limited to: • Wired networking • Wireless networking
Software	
Installing, upgrading, patching, or modifying software or firmware	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.
Changes to configuration settings	Includes but is not limited to: • 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. • Changes to device settings including, but not limited to, enabling and disabling services. • Starting and stopping processes.
Abnormal process exits	All abnormal process exits.
Successful and failed database connection attempts (if a database is used).	All database connection attempts.
Changes to cryptographic keys	At a minimum, critical cryptographic settings include key addition, key removal, and re-keying.
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.
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

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 group or role accessing that file.

Discussion

A record of who modified a configuration file is important for auditing and accountability. The identifying information could include the username or the name of the user for improved traceability.

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

15.2-A – Presentation of voting application errors

The voting system must provide immediate notification to the user when a voting application error occurs.

Discussion

Voting application errors can disrupt a voter's voting session. Immediate notification of an issue or an error allows for prompt recovery and remediation.

Related requirements: 7.3-A – System-related errors
7.3-K – Warnings, alerts, and instructions

15.2-B – Voting application error handling documentation

The voting system documentation must include procedures for handling voting application errors.

Discussion

Documentation will assist election officials with steps to properly address errors.

Related requirements: 7.3-A – System-related errors
7.3-K – Warnings, alerts, and instructions
15.2-A – Presentation of voting application errors

15.2-C – Logging system errors

The voting system must log system errors.

Discussion

This requirement ensures that any system errors are logged for analysis and remediation. System errors do not include user errors, such as undervotes or overvotes.

Related requirements: 15.1-D – Logging event types

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 – Malware protection mechanisms

COTS workstations 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 [NIST13a] might be useful as supplemental guidance for protecting against malware. Malware protection mechanisms are not required for voter-facing scanners and electronic BMDs. Alternatively, voter-facing scanners and electronic BMDs are required to use protection mechanisms, such as digital signatures and allowlists. This requirement is focused on EMS COTS workstations and does not include peripherals devices (e.g., printers).

15.3-B – Updatable malware protection mechanisms

The malware protection mechanisms for COTS devices providing EMS functionality 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-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.-B- Updatable malware protection mechanisms.*

Applies to: EMS Workstations

15.3-D – Notification of malware detection

COTS workstations and servers providing EMS functionality must immediately 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. Once malware is detected, immediate notification of malware detection allows election officials to promptly take the proper action to avoid data integrity issues. This requirement is focused on EMS COTS workstations and does not include peripheral devices (e.g., printers).

15.3-E – Logging malware detection

The voting system must log instances of detecting malware.

15.3-F – Notification of malware remediation

COTS workstations and servers 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. This requirement is focused on EMS COTS workstations and does not include peripherals devices (e.g., printers)

15.3-G – Logging malware remediation

The voting system must log malware remediation activities.

Discussion

Remediation that requires the reimaging or reinstallation of the OS, may need to be logged external to the voting system. Prior to reimaging, the malware detection logs could be downloaded and stored on another system to capture the time stamp of the malware event and preserve the malware event log for further analysis.

15.4 - A voting system with networking capabilities employs appropriate, well-vetted modern defenses against network-based attacks, commensurate with current best practices.

15.4-A – Internal 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 internal 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 – Secure network configuration documentation

The voting system documentation must list security configurations and be accompanied by network security best practices.

Discussion

This documentation may include how external network services are not included as part of the voting system and are handled through a separate air-gapped process. For example, a sneaker-net process may be used to manually transfer elections results to another system that uses public telecommunications to transmit the unofficial election results to a central count center.

A variety of documentation providing secure configurations for network devices is publicly available from the US government.

If outside manufacturers provide guidance and best practices, these need to be documented and used to the extent practical.

This documentation may also include the use of firewalls and intrusion detection systems (IDS). Firewalls and IDSs are typically used to control and monitor the boundary between a private network and the internet. Although the current requirements do not allow for internet connectivity, firewalls and IDSs may also be used for internal boundaries and monitoring inside a private network. Guidance for Intrusion Detection and prevention systems can be found in *NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems [NIST07].*

Related requirements: 14.2-F – Secure configuration and hardening documentation

15.4-C – Documentation for disabled wireless

The voting system documentation must include information about how wireless is disabled within the voting system.

Discussion

Documentation for how the voting system is configured to disable wireless networking is important to meet requirement *14.2-D – Wireless network status indicator*, which disallows the use of any wireless connections. Example information for how wireless can be disabled may include the following:

- a system configuration process that disables wireless networking devices,
- disconnecting/unplugging wireless device antennas, and
- removing wireless hardware within the voting system.

A variety of documentation providing secure configurations for network devices is publicly available from the US government.

If outside manufacturers provide guidance and best practices exist, these need to be documented and used to the extent practical.

Applies to:	Voting systems with networking capabilities
Related requirements:	14.2-C – Wireless communication restrictions

15.4-D – Rule and policy updates

The voting system must be capable of updating rules and policies for 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.

Appendix A
Glossary of Terms

Glossary

A:

absentee ballot

Ballot used for **absentee voting**.
Synonyms: mail ballot, postal ballot

absentee voting

Voting that is typically unsupervised at a location chosen by the **voter** either before or on **election day**.
Synonyms: all-mail voting, mail voting, postal voting, vote-by-mail

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.

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**.

adjudication

Process of resolving flagged **cast ballots** to reflect **voter intent**. Common reasons for flagging include:

- write-ins,
- **overvotes**,
- marginal **machine-readable mark**,
- having no **contest selections** marked on the entire **ballot**, or
- the ballot being unreadable by a scanner.

administrator

A voting system user with the highest level of access.

Synonyms: admin, highest level of authorized user

air gap

A physical separation between systems that requires data to be moved by some external, manual procedure.

alert time

During a voting session, 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.

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(s) is the most-approved candidate(s).
Synonyms: equal-and-even cumulative voting, proportional voting

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.

audio format

A **display format** in which information is communicated through sound and speech.

Synonyms: audio ballot

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 trail

Information **recorded** during **election** activities to reconstruct steps followed or to later verify actions taken with respect to the **voting system**. **Audit trails** may include event logs, paper **records**, error messages, and **reports**.

authentication

Verifying the identity of a user, process, or **device**, often as a prerequisite to allowing access to resources in an information system.

B:

ballot

Presentation of the **contest options** for a particular **voter**.

ballot data

A list of **contests** and associated options that may appear on a **ballot** for a particular **election**.

display format

The concrete presentation of the contents of a **ballot** or other information for the voter or election official 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

Archival digital image (e.g. JPEG, PDF, etc.) captured from one or more sides of a paper ballot cast by an individual voter.

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 marking device

A **device** that:

- permits **contest options** to be selected and reviewed on an electronic interface,
- produces a human-readable **paper ballot**, and
- does not make any other lasting **record** of the **voter**'s selections.

Synonyms: BMD, EBM, electronic ballot marker

ballot measure

A question that appears on a **ballot** with options, usually in the form of an approval or rejection.
Synonyms: ballot issue, ballot proposition, ballot question, referendum

ballot measure option

A **contest option** that specifies a response to a **ballot measure**.

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 secrecy

A goal of **voting systems** to ensure that no **contest selections** can be associated with a **voter**.

ballot style

Ballot data that has been put into **contest** order for a particular **precinct** or precinct split 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 or squares or spaces that conform to accepted **standards**. Linear (1d) barcode standards include UPC, EAN and 128. QR is an example of a 2D barcode standard.

batch

A collection of **paper ballots** or ballot images or cast vote records gathered as a group for tabulation or for auditing.

batch-fed scanner

An electronic **voting device** that typically:

- 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 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.
Synonyms: CCOS, central tabulator, central-count optical scanner, high-speed optical scanner

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.
Synonyms: unmarked ballot

Bluetooth

A wireless protocol that allows two similarly-equipped devices to communicate with each other within a short distance, e.g., 30 ft.

C:

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.
Synonyms: voted ballot

cast vote record

Archival tabulatable **record** of a set of **contest selections** produced by a single **voter** as interpreted by the **voting system**.
Synonyms: CVR

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**.
Synonyms: consolidated precinct, super precinct

commercial-off-the-shelf

Hardware or software **components** that are widely available for purchase and can be integrated into special-purpose systems.
Synonyms: COTS

common data format

Standard and practice of creating and storing data in a common, described format that can be read by other systems.
Synonyms: CDF

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.
Synonyms: CIF

component

Element within a larger **voting system**.

confidentiality

Prevention of unauthorized disclosure of information.

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.
Synonyms: conformity assessment

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.
Synonyms: ballot marking target area, ballot selection position, target, target area

contest option vote

Vote that will be **tabulated** for a particular **contest option**.
Synonyms: 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").

counted ballot

A **read ballot** that has been processed and whose **votes** are included in the vote totals.
Synonyms: tabulated ballot, tallied ballot

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.
Synonyms: cross filing

cryptographic end-to-end(E2E) verifiable voting systems

A voting system that uses cryptographic techniques to store an encrypted copy of the voter's ballot selections while maintaining ballot secrecy and allows election outcomes to be independently and universally verified by members of the public. These voting systems provide voters with a special receipt of their cast ballot—one that allows them to verify their vote was included in the outcome but does not reveal to anyone how they voted.
Synonyms: Receipt-based system

cryptographic hash

A cryptographic algorithm that computes a numerical hash value based on a data file or electronic message. It should be infeasible in practice to find two distinct data files or messages that will result in the same numerical hash value. The numerical value 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 a **private key** is used to digitally sign an electronic document and the associated **public key** is used to verify the signature. Digital signatures provide data **authentication** and integrity protection.

direct voter associations

A voter’s personally identifiable information (PII) created or stored by the voting system that can be used to associate a voter with their ballot selections. Examples include first name, last name, address, driver’s license, voter registration number and other PII.
Synonyms: PII

E:

early voting

Voting that occurs prior to **election day** under the supervision of **election workers**.
Synonyms: in-person absentee voting

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 Assistance Commission

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.
Synonyms: EAC

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 component containing all applicable **election definition** data required by an election system device.

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 an authorized 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,
- **tabulate votes**,
- consolidate and **report** results, and
- maintain **audit trails**.

Synonyms: EMS

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 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.

Synonyms: ENR, ERR, election night reporting

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.
Synonyms: poll worker

electronic ballot interface

Subsystem within a **voting system** which communicates **ballot** information to a **voter** in visual, audio, or other **alternative format** which allows the voter to select **contest options** using vocalization or physical actions.

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.
Synonyms: EPB, e-poll book

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 **tabulated**. 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

A **display format** that is an alternative **visual format** supporting personal screen display choices such as text size, color contrast, and preferred language.

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 **contest option position** 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.
Synonyms: inadvertent mark, random mark, stray mark

F:

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,
- 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.

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.
Synonyms: FIPS

finding

(n) Result of a formal evaluation by a **test** lab or accredited expert.
Synonyms: verdict

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 device's specific hardware (such as the firmware that initially boots an operating system).

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**.

graceful recovery

Termination of a process that allows the operating system or parent process to regain normal control. Does not crash the machine or result in a general protection default (GPF) or blue screen. The user is not required to close the application and can continue to use the other functionality.

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**.
Synonyms: HAVA

I:

implementation statement

Statement by a **manufacturer** indicating the capabilities, features, and optional functions as well as extensions that have been implemented.
Synonyms: 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 voter associations

A unique identifier used to associate a voter with their ballot selections. Indirect associations do not include PII.

information security

Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, **confidentiality**, and availability.
Synonyms: IS

inspection

Examination of a product design, product, process, or installation and determination of its conformity with specific requirements.

interaction mode

Control or navigation option that enables **voters** to operate and interact with the **voting system**, used in conjunction with a display format**.**

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. Synonyms: IDS

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.

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.
Synonyms: L&A, LAT

limited dexterity mode

An **interaction mode** with **accessibility** features for **voters** with no use of one or both hands or low dexterity. This mode includes the tactile mode and the non-manual mode.

M:

machine-readable mark

Mark in a **contest selection** position of a **paper ballot** that meets requirements for detection by a scanner.

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.
Synonyms: malicious code

manually-marked paper ballot

Paper ballot marked by a **voter** using a writing utensil.
Synonyms: MMPB

manufacturer

Entity with ownership and control over a **voting system** submitted for testing.
Synonyms: vendor

marked ballot

Ballot that contains all of the selections made by a **voter**.

message authentication code

A data authenticator generated from the message, usually through cryptographic techniques, that is designed to reveal both accidental errors and intentional modifications of the data. In general, a cryptographic key is also required as an input.
Synonyms: MAC

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 **candidates** are elected to fill a specified number of **seats**.

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 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.
Synonyms: NIST

non-manual mode

An interaction mode that use assistive technology, for example, a sip-and-puff switch, to allow voters with no use of their hands to operate the voting system.

non-party-specific contest

Contest where eligibility to **vote** in that contest is independent of **political party** affiliation.

nonvolatile memory

Memory in which information can be stored indefinitely with no external power applied.

O:

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.
Synonyms: pick-your-party primary

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; or
- be fully open source or may have only a portion of the software open source.

optical scan

Voting system that **tabulates votes** marked in **contest option positions** or contained with a barcode 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.
Synonyms: over-vote

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 side

The face of a **paper ballot sheet**. A **paper ballot** may have two sides.

paper-based voting system

A voting system that records votes, counts votes, and/or produces a report of the vote count from votes cast on paper cards or sheets

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.

penetration testing

An evaluation method that enables researchers to search for vulnerabilities in a system. Synonyms: Pen Testing

personal assistive device

Assistive technology belonging to **voters** rather than any supplied with the **voting system**.

personally identifiable information

Any information about an individual 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.

Synonyms: PII, voter identifying information, VII

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 place

Location at which **voters** may **cast** in-person **ballots** under the supervision of **election workers** during one or more specific time periods.
Synonyms: poll, polling station

post-election tabulation audit

A post-election **audit** that involves hand-counting a sample of **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 detect 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.
Synonyms: tabulation district, ward

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**.
Synonyms: split, split precinct, sub-precinct

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.

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.
Synonyms: affidavit ballot

Q:

quick response code

A 2D, trademarked barcode. An optical, 2-D machine-readable representation of data that conforms to accepted standards.
Synonyms: QR Code

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.
Synonyms: score voting

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.

Synonyms: IRV, RCV, instant run-off voting, ranked order

read ballot

Cast ballot that has been successfully accepted and initially processed, e.g., scanned by an optical scanner.
Synonyms: scanned ballot

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.

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.

resilience

The ability to recover gracefully from error conditions and unexpected circumstances. For example, manually marked paper preserves evidence of exceptions that can advise both adjudication and audit to achieve better interpretation of original voter intent.

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

Post-election tabulation 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).
Synonyms: RLA

S:

seat

An **elected office** position that a single officeholder may occupy for a term of **office**.

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. In practice, voting systems are generally viewed as possessing the quality of software independence when they allow for a voter-verifiable paper record of voters' contest selections to be created and compared against vote totals or against an electronic cast vote record used in determining vote totals.
Synonyms: SI

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.

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** regulations regarding 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**.

support software

Software that aids in developing, maintaining, or using other software, for example, compilers, loaders and other utilities.

switch

An assistive technology primarily used by people with motor impairments to access and control computers and other devices.

secret key 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**.
Synonyms: count

tabulation report

A **report** containing the counts associated with **ballots** that have been tabulated.

tactile controls

A tactile control is a physical control 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.

tactile mode

An interaction mode that uses tactile controls to operate the voting system.

tamper-evidence

A feature of a physical or digital artifact that provides evidence of unauthorized modification or access (e.g., tamper-evident seal).

technical data package

Manufacturer documentation relating to the **voting system**, which can include manuals, description of **components**, and details of architectural and engineering design.
Synonyms: TDP

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 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.

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.
Synonyms: authentication token, cryptographic token

touch mode

Interaction mode that uses a touch screen to operate the voting system.

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**.
Synonyms: civil township

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.
Synonyms: under-vote

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**.
Synonyms: UOCAVA

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**.

V:

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 information is 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 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**, and **ranked choice 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.
Synonyms: VBM, all-mail voting, mail voting, postal voting

vote-capture device

Component of a voting system that captures and/or counts voter selections from paper or electronic ballots. Vote-capture devices may or may not be directly voter-facing; voter-facing vote-capture devices include ballot marking devices and voter-facing scanners, while non-voter facing vote-capture devices include batch-fed scanners.

voter

Person permitted to **cast** a **ballot**.

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 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 record

A paper document that the **voter** can review before officially **casting** their **ballot**.
Synonyms: VVPR

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.
Synonyms: PCOS, precinct-count optical scanner

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** for voters,
- capture **votes** cast by voters,
- **count** votes,
- label **ballots** needing special treatment,
- generate **reports**,
- export election data including election results,
- archive election data, and
- produce **records** in support of audits.

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).
Synonyms: VSTL

W:

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**.

Appendix B
Requirements Listing

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 – Serve multiple or split precincts and election districts
1.1.1-C – Multiple identifiers
1.1.1-D – Definition of parties and contests
1.1.1-E – Voting variations
1.1.1-F – Confirm recording of election definition
1.1.1-G – Election definition distribution
1.1.1-H – Jurisdiction-dependent content
1.1.1-I – Include contests
1.1.1-J – Exclude contests
1.1.1-K – Primary elections, associate contests with parties
1.1.1-L – Ballot rotation, Election definition
1.1.1-M – Ballot configuration in combined or split precincts
1.1.1-N – Ballot style identification

1.1.2 – Pre-election testing
1.1.2-A – Built-in self-test and diagnostics
1.1.2-B – Installation of software and ballot styles
1.1.2-C – Use of test ballots
1.1.2-D – Testing all ballot positions
1.1.2-E – Testing cast vote record creation
1.1.2-F – Testing codes and image creation
1.1.2-G – Testing equipment calibration
1.1.2-H – No side-effects from pre-election testing
1.1.2-I – Equipment status and readiness reports
1.1.2-J – Ballot style readiness reports
1.1.2-K – Precinct-based voting devices readiness reports
1.1.2-L – All vote-capture devices readiness reports

1.1.3 – Opening the polls
1.1.3-A – Opening the polls
1.1.3-B – Non-zero totals

1.1.4 - Casting
1.1.4-A – Voting and casting the ballot
1.1.4-B – Control ballot configuration
1.1.4-C – Precinct splits, Casting
1.1.4-D – Ballot rotation, Casting
1.1.4-E – Partisan closed primary ballot
1.1.4-F – Partisan open primary ballot
1.1.4-G – Indicate party affiliations and endorsements
1.1.4-H – Write-in contest options
1.1.4-I – Write-in reconciliation
1.1.4-J – N-of-M contest, Casting
1.1.4-K – Straight-party voting, Casting
1.1.4-L – Cumulative voting contest, Casting
1.1.4-M – Ranked choice voting contest, Casting
1.1.4-N – Party preference contest
1.1.4-O – Top-2 primary contest (blanket primary contest)
1.1.4-P – Presidential delegate contest, Casting
1.1.4-Q – Proportional voting contest (equal-and-even cumulative voting contest), Casting
1.1.4-R – Group voting contest, Casting
1.1.4-S – Top-2 IRV contest (supplementary or contingent vote contest)

1.1.5 – Recording voter choices
1.1.5-A – Casting and recording
1.1.5-B – Ballot orientation
1.1.5-C – Record contest selection information
1.1.5-D – Record write-in information
1.1.5-E – Record election and contest information
1.1.5-F – Record ballot selection override information
1.1.5-G – Record audit information
1.1.5-H – Store and link corresponding image

1.1.6 – Ballot handling for vote-capture devices
1.1.6-A – Detect and prevent ballot style mismatches
1.1.6-B – Detect and reject ballots that are oriented incorrectly
1.1.6-C – Ballot separation when batch feeding
1.1.6-D – Overvotes, undervotes, blank ballots
1.1.6-E – Write-ins, Ballot handling for vote-capture devices
1.1.6-F – Ability to clear mis-fed ballots
1.1.6-G – Scan to manufacturer specifications
1.1.6-H – Accurately detect imperfect marks
1.1.6-I – Ignore extraneous marks inside voting targets
1.1.6-J – Marginal marks, without bias
1.1.6-K – Repeatability

1.1.7 – Exiting or suspending voting
1.1.7-A – Exiting or suspending election mode
1.1.7-B – No voting when voting is stopped
1.1.7-C – Voting stop integrity check
1.1.7-D – Report on voting stop process
1.1.7-E – Prevent re-entering election mode

1.1.8 – Tabulation
1.1.8-A – Tabulation
1.1.8-B – Partisan primary elections
1.1.8-B.1 – Tabulation of a closed primary ballot
1.1.8-B.2 – Tabulation of an open primary ballot
1.1.8-B.3 – Open primary ballot with party preference contest
1.1.8-C – Write-ins, Tabulation
1.1.8-D – Ballot rotation, Tabulation
1.1.8-E – Straight-party voting, Tabulation
1.1.8-F – Cross-party endorsement with straight-party voting
1.1.8-G – Precinct splits, Tabulation

1.1.8-H – N-of-M contest, Tabulation
1.1.8-I – Cumulative voting contest, Tabulation
1.1.8-J – Ranked choice voting contest, Tabulation
1.1.8-K – Group voting contest, Tabulation
1.1.8-L – Presidential delegate contest, Tabulation
1.1.8-M – Recall contest pair
1.1.8-N – Proportional voting contest (equal-and-even cumulative voting contest), Tabulation
1.1.9 – Reporting results
1.1.9-A – Post-election reports
1.1.9-B – Report categories of cast ballots
1.1.9-C – Report categories of votes
1.1.9-D – Reporting combined or split precincts
1.1.9-E – Report counted ballots by contest
1.1.9-F – Report votes for each contest option
1.1.9-G – Report overvotes for each contest
1.1.9-H – Report undervotes for each contest
1.1.9-I – Ranked choice voting, report results
1.1.9-J – Precinct reporting devices, reporting device consolidation
1.1.9-K – Precinct reporting devices, no tallies before polls close
1.1.9-L – Report read ballots by party
1.1.9-M – Reports are time stamped

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

1.2 – Assessment of accuracy
1.2-A – Assessment of accuracy
1.2-B – Reliably detectable marks
1.2-C – Minimum ballot positions
1.2-D – Handle maximum volume
1.2-E – Respond gracefully to stress of system limits
1.2-F – No single point of failure
1.2-G – Misfeed rate benchmark
1.2-H – Protect against failure of input and storage devices
1.2-I – FCC Part 15 Class A and B conformance
1.2-J – Power supply from energy service provider
1.2-K – Power port connection to the facility power supply
1.2-L – Leakage from grounding port

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 – Reporting of manufacturer-performed tests
1.3-B – Coverage of manufacturer-performed tests

Principle 2: High Quality Implementation

The voting system is implemented using high quality best practices.

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

2.1 – Software quality
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 – Durability estimation
2.1.1-C – Durability of paper
2.1.1-D – Ensure compatibility of specified paper and ink
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 – Design and implementation process
2.2-A – User-centered design process

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

2.3 – Voting system logic
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 – Modularity
2.4-A – Modularity
2.4-B – Module testability
2.4-C – Module size and identification
2.4-D – Large data structures in separate files

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

2.5 – System processes and data
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 - Input validation and error defense

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 – Graceful recovery
2.6-A – Surviving device failure
2.6-B – No compromising voting or audit data
2.6-C – Coherent checkpoints

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

2.7 – Physical environments
2.7-A – Assessment of reliability
2.7-B – Continuous operation – typical environmental conditions
2.7-C – Continuous operation – varied environmental conditions
2.7-D – Ability to support maintenance and repair physical environment conditions – non-operating
2.7-E – Ability to support transport and storage physical environment conditions – non-operating
2.7-F – Ability to support storage temperatures in physical environment – non-operating
2.7-G – Electrical disturbances
2.7-H – Power outages, sags, and swells
2.7-I – Withstand conducted electrical disturbances
2.7-J – Emissions from other connected equipment
2.7-K – Electrostatic discharge immunity

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 documentation
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 documentation
3.1.2-A – System performance documentation
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 documentation
3.1.3-B – Access control implementation
3.1.3-C – Physical security
3.1.3-D – Audit procedures

3.1.4 – Software installation documentation
3.1.4-A – Software installation documentation
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 procedures
3.1.4-G – Baseline image creation
3.1.4-H – Programmed device configuration replication
3.1.4-I – Software installation record creation
3.1.4-J – Procurement of voting system software
3.1.4-K – Open market procurement of COTS software
3.1.4-L – Erasable storage media preparation
3.1.4-M – Trusted storage media

3.1.5 – System operations documentation
3.1.5-A – System operations documentation
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 – Support
3.1.5-K – Transportation and storage

3.1.6 – System maintenance documentation
3.1.6-A – System maintenance documentation
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 procedure details
3.1.6-H – Special equipment
3.1.6-I – Parts and materials
3.1.6-J – Approved parts list
3.1.6-K – Marking devices
3.1.6-L – Approved manufacturers
3.1.6-M – Ballot stock specification
3.1.6-N – Ballot stock specification criteria
3.1.6-O – Printer paper specification
3.1.6-P – System maintenance, maintenance environment
3.1.6-Q – System maintenance, maintenance support and spares

3.1.7 – Training documentation
3.1.7-A – Training documentation
3.1.7-B – Personnel
3.1.7-C – User functions versus manufacturer functions
3.1.7-D – Training requirements

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

3.2 – Setup inspection documentation

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 – Public documentation

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 – Ballot selection codes

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 – Interoperable formats

4.1-A – Election programming data input and output
4.1-B – Tabulator report data
4.1-C – Exchange of cast vote records (CVRs)
4.1-D – Exchange of voting device election event logs
4.1-E – Voting device event code documentation
4.1-F – Specification of common format usage

4.2 - Standard, publicly available formats for other types of data not addressed by CDF specifications are used.

4.2 – Standard formats

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 – Interfaces and communication protocols

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 – COTS

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.

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

5.1 – Consistent experience

5.1-A – Voting methods and 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 – Equivalent information

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 – Privacy of interaction

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 – Default settings

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 – Controls
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 – Touch screen 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 – Understandable information
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 – Protect from 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 for usability with a wide range of representative voters, including those with and without disabilities.

8.3-A – Usability tests with voters

8.4 – The voting system is evaluated for usability with 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
9.1.2 – 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 – Ballot error correction
9.1.3-C – Voter reported errors
9.1.4 – Auditable
9.1.4-A – Auditor verification
9.1.4-B – 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
9.1.5-F – Unique identifier
9.1.5-G –Preserving software independence
9.1.6 – Cryptographic E2E verifiable
9.1.6-A– Verified cryptographic protocol
9.1.6-B – Independent evaluation of E2E cryptographic protocol implementation
9.1.6-C – Cryptographic ballot selection verification by voter
9.1.6-D – Methods for cryptographic ballot selection verification
9.1.6-E – Ballot receipt
9.1.6-F – Disputes involving ballot receipts
9.1.6-G – Evidence export
9.1.6-H– Mandatory ballot availability
9.1.6-I – Verification of encoded votes documentation
9.1.6-J – Verifier reference implementation
9.1.6-K – Privacy preserving, universally verifiable ballot tabulation

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 – Audit support documentation

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 – Efficient audits
9.4-A – Risk-limiting audit
9.4-B – Random numbers supporting audit processes
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 – Isolated storage location
10.2.1-E – Removal of indirect voter associations
10.2.1-F – Confidentiality for ballots with indirect voter associations
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 – Aggregating and ordering
10.2.2-E – Randomly generated identifiers
10.2.3 – Access to cast vote records (CVR)
10.2.3-A – Restrict access to records of voter intent
10.2.3-B – 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 – Logging of ballot selections
10.2.4-C – 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 – Access privileges
11.1-A – Logging activities and resource access
11.1-B – Voter information in log files
11.1-C – Preserving log integrity
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 mechanisms
- 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 – User authentication credentials
- 11.3.2-A – Username and password management
- 11.3.2-B – Password complexity
- 11.3.2-C – Secure storage of authentication data
- 11.3.2-D – Password disallow list
- 11.3.2-E – 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 – Default access control policies
- 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 – Logical access restrictions
- 11.5-A – Session time limits
- 11.5-B – Reauthentication
- 11.5-C – Account lockout
- 11.5-D – Lockout time duration

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 – Mechanisms to detect unauthorized physical access
- 12.1-A – Unauthorized physical access
- 12.1-B – Unauthorized physical access alert
- 12.1-C – Disconnecting a physical device
- 12.1-D – Logging of physical connections and disconnections
- 12.1-E – Secure containers
- 12.1-F – Secure locking systems
- 12.1-G – 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 – Physical ports and access points essential to voting
- 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

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

13.2 – Source and integrity of election records
- 13.2-A – Signing stored election records

13.2-B – Verification of election records

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

13.3 – Cryptographic algorithms
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 – Cryptographic key management documentation

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

13.4-A – Confidentiality and integrity protection of transmitted 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 – Documented resiliency against security failures and 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 is designed to limit its attack surface by avoiding unnecessary code, data paths, connectivity, and physical ports, and by using other technical controls.

14.2 – Designed to limit attack surface
14.2-A – Non-essential networking interfaces
14.2-B – Network status indicator
14.2-C – Wireless communication restrictions
14.2-D – Wireless network status indicator
14.2-E – External network restrictions
14.2-F – Secure configuration and hardening documentation
14.2-G – Unused code
14.2-H – Use of exploit mitigation technologies
14.2-I – Importing software libraries
14.2-J – Vulnerability management plan
14.2-K – Known vulnerabilities

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

14.3 – Supply chain
14.3-A – Supply chain risk management strategy
14.3-B – Criticality analysis
14.3-C – Bill of materials
14.3.1 – Boot integrity
14.3.1-A – Cryptographic boot verification
14.3.1-B – Preventing of boot on error
14.3.1-C – Notification of boot validation failure
14.3.2 – Software integrity
14.3.2-A – Installing software
14.3.2-B – Software verification for installation
14.3.2-C – Application allowlisting
14.3.2-D – Integrity protection for software allowlists

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

14.4 – Authorized software updates

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 – Event logging
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 – Error messages
15.2-A – Presentation of voting application errors
15.2-B – Voting application error handling documentation
15.2-C – Logging system errors
15.2-D – Creating error reports

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

15.3 – Malware protection mechanisms
15.3-A – Malware protection mechanisms
15.3-B – Updatable malware protection mechanisms
15.3-C – Documenting malware protection mechanisms
15.3-D – Notification of malware detection
15.3-E – Logging malware detection
15.3-F – Notification of malware remediation
15.3-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 practices.

15.4 – Defense against network-based attacks
15.4-A – Internal network architecture documentation
15.4-B – Secure network configuration documentation
15.4-C – Documentation for disabled wireless
15.4-D – Rule and policy updates

Appendix C References

Reference	Citation
ADA10:	**The Americans with Disabilities Act of 1990.**
ANSI04:	**International Committee for Information Technology Standards, American National Standard for Information Technology – Role Based Access Control (ANSI INCITS 359-2004), February 2004.**
ANSI19:	**American National Standard for Methods of Measurement of Compatibility between Wireless Communication Devices and Hearing Aids, ANSI C63.19-2019.**
ANSI15b:	**CISPR 24:2010+A1:2015, Information technology equipment - Immunity characteristics - Limits and methods of measurement.**
ANSI93:	**ANSI C63.16:1993, American National Standard Guide for Electrostatic Discharge Test – Methodology and Criteria for Electronic Equipment.**
Benaloh14:	**Benaloh et al., End-to-end verifiability, February 2014.**
CA06:	**California Volume Reliability Testing Protocol. January 31, 2006**
CIS20:	**Center for Internet Security, CIS Benchmarks, 2020.**
CVR_CDF:	**Wack et al. Cast Vote Records Common Data Format Specification (NIST SP 1500-103), Version 1.0. February 2019.**
DISA20:	**Defense Information Systems Agency, Security Technical Implementation Guides (STIGs), 2020.**
NIST16:	**Wack et al. Election Results Common Data Format Specification (NIST SP 1500-100), Version 2.0, September 2019.**
FCC18:	**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.**
FCC19a:	**Title 47, Part 15, Rules and Regulations of the Federal Communications Commission, Radio Frequency Devices.**
GPO19:	**Government Paper Specification Standards No. 13, May 2019.**
HAVA02:	**The Help America Vote Act of 2002, Public Law 107-252.**

ISO00:	**ISO/IEC TR 15942:2000, Information technology—Programming languages—Guide for the use of the Ada programming language in high integrity systems.**
ISO06b:	**ISO/IEC 25062:2006 Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Common Industry Format (CIF) for Usability Test Reports.**
ISO10:	**ISO/IEC TR 25060:2010** **Systems and software engineering — Systems and software product Quality Requirements and Evaluation (SQuaRE) — Common Industry Format (CIF) for usability: General framework for usability-related information.**
ISO13a:	**ISO/IEC TR 24772:2013** **INFORMATION TECHNOLOGY -- PROGRAMMING LANGUAGES -- GUIDANCE TO AVOIDING VULNERABILITIES IN PROGRAMMING LANGUAGES THROUGH LANGUAGE SELECTION AND USE.**
ISO13b:	**ISO/IEC 25064:2013** **Systems and software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Common Industry Format (CIF) for usability: User needs report.**
ISO14:	**ISO/IEC 25063:2014** **Systems and software engineering — Systems and software product Quality Requirements and Evaluation (SQuaRE) — Common Industry Format (CIF) for usability:**
ISO16:	**ISO/IEC 25066:2016 Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Evaluation report**
ISO18:	**ISO/IEC/IEEE 90003:2018** **SOFTWARE ENGINEERING -- GUIDELINES FOR THE APPLICATION OF ISO 9001:2015 TO COMPUTER SOFTWARE.**
ISO18d:	**ISO/IEC 27005:2018 Information technology - Security techniques - Information security risk management, July 2017.**
ISO19a:	**ISO/IEC PRF TR 24772-1** **PROGRAMMING LANGUAGES -- GUIDANCE TO AVOIDING VULNERABILITIES IN PROGRAMMING LANGUAGES -- PART 1: LANGUAGE INDEPENDENT.**
ISO19b:	**ISO/IEC 9294-210:2019 Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems.**
ISO8601	**ISO/IEC 8601-1:2019 Date and Time Format.**
ITU19:	**International Telecommunications Union (ITU) (nd) Rec. ITU-T P.50 October 2019.**
Kulyk18:	**Oksana Kulyk, Melanie Volkamer, Usability is not Enough: Lessons Learned from 'Human Factors in Security' Research for Verifiability, October 2018.**

Lewis19a:	**Sarah Jamie Lewis, Olivier Pereira, Vanessa Teague, *Ceci n'est pas une preuve*, March 2019.**
Lewis19b:	**Sarah Jamie Lewis, Olivier Pereira, Vanessa Teague, How not to prove your election outcome, March 2019.**
LOG_CDF:	**Wack et al. Election Event Logging Common Data Format Specification Draft (NIST SP 1500-101), Version 1.0. September 2017.**
MITRE20:	**MITRE Common Weakness Enumeration 561: Dead Code, August 2020.**
MITRE20a:	**MITRE Common Weakness Enumeration 259: Use of Hard-coded Password, August 2020.**
MITRE20b:	**MITRE Common Weakness Enumeration 321: Use of Hard-coded Cryptographic Key, August 2020.**
MITRE20c:	**MITRE Common Weakness Enumeration 116: Improper Encoding or Escaping of Output, June 2020.**
MITRE20d:	**MITRE Common Weakness Enumeration 134: Use of Externally-Controlled Format String, August 2020.**
MITRE20e:	**MITRE Common Weakness Enumeration 89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), August 2020.**
Moulding89:	**M. R. Moulding, "Designing for high integrity: the software fault tolerance approach," Section 3.4. In C. T. Sennett, ed., High-Integrity Software, Plenum Press, New York and London, 1989.**
NIST01:	**National Institute of Standards and Technology Federal Information Processing Standards 140-2: Security Requirements for Cryptographic Modules, May 2001.**
NIST07:	**Karen Scarfone, Peter Mell, National Institute of Standards and Technology Special Publication 800-94: Guide to Intrusion Detection and Prevention Systems, February 2007.**
NIST08:	**Dana E. Chisnell, Susan C. Becker, Sharon J. Laskowski, Svetlana Z. Lowry, National Institute of Standards and Technology IR 7519, Style Guide for Voting System Documentation, August 2008.**
NIST09:	**Karen Scarfone and Paul Hoffman, National Institute of Standards and Technology Special Publication 800-41, Revision 1: Guidelines on Firewalls and Firewall Policy, September 2009.**
NIST09a:	**Janice (Ginny) Redish and Sharon J. Laskowski, National Institute of Standards and Technology IR 7596, Guidelines for Writing Clear Instructions and Messages for Voters and Poll Workers, May 2009.**
NIST12:	**Joint Task Force Transformation Initiative, National Institute of Standards and Technology Special Publication 800-30, Revision 1: Guide for Conducting Risk Assessments, September 2012.**
NIST13a:	**Murugiah Souppaya, Karen Scarfone, National Institute of Standards and Technology Special Publication 800-83, Revision 1: Guide to Malware Incident Prevention and Handling for Desktops and Laptops, July 2013.**

NIST13b:	**Murugiah Souppaya, Karen Scarfone, National Institute of Standards and Technology Special Publication 800-40, Revision 3: Guide to Enterprise Patch Management Technologies, July 2013.**
NIST13c:	**National Institute of Standards and Technology Federal Information Processing Standards 186-4: Digital Signature Standard, July 2013.**
NIST15a:	**Elaine Barker, John Kelsey, National Institute of Standards and Technology Special Publication 800-90A, Revision 1: Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015.**
NIST15b:	**Jon Boyens et al., National Institute of Standards and Technology Special Publication 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations, April 2015**
NIST17c:	**Paul A. Grassi, Michael E. Garcia, James L. Fenton, National Institute of Standards and Technology Special Publication 800-63-3: Digital Identity Guidelines, June 2017.**
NIST17d:	**Paul A. Grassi et al., National Institute of Standards and Technology Special Publication 800-63B: Digital Identity Guidelines: Authentication and Lifecycle Management, June 2017.**
NIST17e:	**Michael Nieles, Kelley Dempsey, Victoria Yan Pillitteri, National Institute of Standards and Technology Special Publication 800-12, Revision 1: An Introduction to Information Security, June 2017.**
NIST18a:	**Turan et al. National Institute of Standards and Technology Special Publication 800-90B: Recommendation for the Entropy Sources Used for Random Bit Generation, January 2018.**
NIST18b:	**Celia Paulsen, Jon Boyens, Nadya Bartol, Kris Winkler, National Institute of Standards and Technology Interagency or Internal Report 8179: Criticality Analysis Process Model: Prioritizing Systems and Components, April 2018.**
NIST18c:	**National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 2018.**
NIST19a:	**National Institute of Standards and Technology Federal Information Processing Standards 140-3: Security Requirements for Cryptographic Modules, March 2019.**
NIST19b:	**Kerry McKay, David Cooper, National Institute of Standards and Technology Special Publication 800-52, Revision 2: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, August 2019.**
NIST20a:	**Eliane Barker, National Institute of Standards and Technology Special Publication 800-57 Part 1, Revision 5: Recommendation for Key Management Part 1 – General, May 2020.**
NIST20b:	**Joint Task Force, National Institute of Standards and Technology Special Publication 800-53, Revision 5: Security and Privacy Controls for Information Systems and Organizations, September 2020.**

NIST20c:	**Kelley Dempsey, Eduardo Takamura, Paul Eavy, George Moore, National Institute of Standards and Technology Interagency or Internal Report 8011 Volume 4: Automation Support for Security Control Assessments: Software Vulnerability Management, April 2020.**
NIST20d:	**Celia Paulsen et al., National Institute of Standards and Technology Interagency or Internal Report 8272: Impact Analysis Tool for Interdependent Cyber Supply Chain Risks, August 2020**
NIST20e:	**National Institute of Standards and Technology Cryptographic Module Validation Program, October 2020.**
NIST20f:	**Elaine Barker, Allen Roginsky, Richard Davis, National Institute of Standards and Technology Special Publication 800-133, Revision 2: Recommendation for Cryptographic Key Generation, June 2020.**
NIST20g:	**Elaine Barker, National Institute of Standards and Technology Special Publication 800-175B, Revision 1: Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms, March 2020.**
NIST20h:	**Security and Privacy Controls for Information Systems and Organizations, National Institute of Standards and Technology Special Publication 800-53, Revision 5, September 2020.**
NTIA19:	**National Telecommunications and Information Administration, Software Bill of Materials, 2019.**
OCD-ID:	**Open Civic Data Identifiers Specification.**
OWASP19:	**Open Web Application Security Project, Application Security Verification Standard 4.0, March 2019.**
Rivest06:	**Ronald R. Rivest and John P. Wack, "On the notion of "software independence" in voting systems," July 28, 2006.**
SAFECode19:	**SAFECode, Managing Security Risks Inherent in the Use of Third-party Components, May 2019.**
TC04:	**Trace Center (2004), About Decibels (dB).**
TCnd:	**Trace Center (nd). EZ Access design is an example of button functions distinguishable by both shape and color.**
UL07:	**UL 60950-1:2007, Edition 2, Information Technology Equipment – Safety – Part 1: General Requirements. March 27, 2007.**
UL13:	**UL 437:2013, Edition 8, Standard for Key Locks. May 15, 2013.**
UL19:	**UL 62368:1 Edition 3, Standard for Audio/video, Information and Communication Technology Equipment - Part 1: Safety requirements**
USAB14a:	**US Access Board Technical Guide: Clear Floor or Ground Space and Turning Space. February 2014.**
USAB14b:	**US Access Board Guide to the ADA Standards, Chapter 3 Operable Parts.**

USAB18:	**US Access Board (2018) Section 508 Information and Communication Technology (ICT) Final Standards and Guidelines (36 CFR Parts 1193 and 1194, RIN 3014-AA37, Final Rule, March 23, 2018)**
USDOJ16:	**US Department of Justice ADA Checklist for Polling Places, 2016.**
VRA65:	**The Voting Rights Act of 1965, Public Law 89-110, August 6, 1965.**
VRI_CDF:	**Wack et al. Voter Records Interchange (VRI) CDF Specification (NIST SP 1500-102), Version 1.0. August 2017.**
VSS1990:	**Performance and Test Standards for Punchcard, Marksense, and Direct Recording Electronic Voting Systems, January 1990 edition with April 1990 revisions, in Voting System Standards, U.S. Government Printing Office, 1990.**
VVSG2005:	**2005 Voluntary Voting System Guidelines, Version 1.0, Volumes I and II, March 6, 2006.**
VVSG2015:	**2015 Voluntary Voting System Guidelines, Version 1.1, Volumes I and II. March 31, 2015.**
W3C10:	**W3C WAI (2010) WCAG 2.0 Web content and Accessibility Guidelines.**