2012

DRAFT VVSG 1.1

U.S. Election Assistance Commission

Volume I

AUGUST 31, 2012

Table of Contents

Volume I Voting System Performance Guidelines

Volume II National Certification Testing Guidelines

Voluntary Voting System Guidelines Overview

Guide to Section Locations

Draft VVSG 1.1

September 1, 2011

This document represents a draft revision of the Election Assistance Commission's (EAC) 2005 Voluntary Voting System Guidelines (VVSG) Version 1.0. It has been prepared by the National Institute of Standards and Technology (NIST) for the EAC, and does not represent a consensus view or recommendation from NIST, nor does it represent any policy positions of NIST.

This document consists of the VVSG Version 1.0, revised with new material mostly from the Technical Guidelines Development Committee (TGDC) VVSG Recommendations to the EAC of August 31, 2007. It also contains changes to the 2005 VVSG material as a result of EAC decisions on Requests for Interpretation (RFI) of requirements in the 2005 VVSG. This document has been highlighted in places where changes have been made, new material has been added, or previous material has been deleted. Typos and formatting issues in the previous material that have been corrected are not highlighted.

Background

The Election Assistance Commission (EAC) requested that NIST investigate whether certain requirements in the 2007 TGDC Recommendations could be integrated with or replace current requirements in the 2005 VVSG in order to improve the overall quality and uniformity of testing for voting systems and to make key improvements in the 2005 VVSG while the TGDC Recommendations is in public review. The EAC requested also that the requirements also be accompanied by tests being developed by NIST as part of its test suites for the TGDC Recommendations. Other criteria used to identify candidate requirements from the TGDC Recommendations included that

- would not require hardware changes to current voting systems,
- would not require complex changes in software to current voting systems, and
- would not substantially change the structure of the VVSG 2005.

The EAC, with initial input from NIST (see http://vote.nist.gov/EACResearch-AmendedVVSG-2005-20081030.pdf), selected the requirements from the TGDC Recommendations to include in the 2005 VVSG revision. The EAC and NIST then reviewed comments received from the public review of the TGDC Recommendations (which ended in April, 2008) and revised the TGDC Recommendations requirements accordingly. Using this material, NIST then revised the 2005 VVSG Version 1.0.

Overview of Revisions

The following list identifies the major sections of material in this draft that are revised with updated material from the TGDC Recommendations. Items 10, Cryptography, and 11, External Interface Requirement, identify newly developed material.

1. **Hardware and Software Performance Benchmarks and Test Method**

- **Volume I Section 2.1.2**, added a requirement to clarify that the accuracy benchmark is not intended to allow tolerance of software faults that result in systematic miscounting of votes.
- **Volume I Section 4.1.1** is replaced by Part 1 Section 6.3.2 (Accuracy) of the TGDC Recommendations.
- **Volume I Section 4.1.5.1.e.ii (under Ballot Handling) and 4.1.5.2.f** (under Ballot Reading Accuracy) of the 2005 VVSG are replaced by Part 1 Section 6.3.3 (Misfeed Rate) of the TGDC Recommendations. Previous versions of the VVSG specified separate and different benchmarks for multiple feeds and the rejection of ballots that meet all vendor specifications. These separate benchmarks have now been merged into a single "misfeed" benchmark because there is no consequential difference in the impact of these events nor in the recovery behaviors that are required of the voting system. Scanners are not permitted to feed multiple ballots and fail to detect this occurrence (Volume I Req. 4.1.5.1.e).
- **Volume I Section 4.3.3** is replaced by new requirements on reliability based on the use case in the TGDC Recommendations, and all requirements on availability and maintainability (I.4.3.4, I.4.3.5, I.6.2.4, I.6.2.5, one paragraph of II.2.4.1, II.4.7.2, and II.4.7.5) are deleted. A conflicting requirement in Volume I Section 4.1.4.3 is also deleted. Harmonizing changes are made in Volume II Sections 1.3.1.2, 1.8.2.6, 2.4.1, and 4.7.2.
- **Volume II Sections 1.8.2.3 and 4.5** of the 2005 VVSG are partially harmonized with Part 3 Section 2.5.3 of the TGDC Recommendations to restrict the use of test fixtures that bypass portions of the voting system.
- **Volume II Appendix C** is replaced by a test method based on Part 3 Section 5.3 of the TGDC Recommendations, which is applicable to the assessment of accuracy and misfeed rate. Volume II Section 4.7.1.1 (accuracy testing information previously included within the specification of the Temperature and Power Variation Tests) is made redundant and deleted.

2. **Quality Assurance and Configuration Management**

- **Requirement I.4.3.4.a** is deleted (redundant with added material).
- **Volume I Chapter 8** is replaced by Part 1 Section 6.4.2 of the TGDC Recommendations.
- **Volume I Chapter 9** is deleted.
- **Volume II Section 2.11** is deleted. It is replaced by a new section in Volume II Part 2 Chapter 2 of the TGDC Recommendations.
- **Volume II Section 2.12** is replaced by Physical Configuration Audit (PCA) and Functional Configuration Audit (FCA) requirements that were displaced from Volume I Section 9.7.
- **Volume II Chapter 7** is replaced by Part 3 Section 4.4 of the TGDC Recommendations.

3. **Software Workmanship**

- **Volume I Section 5.2** of the 2005 VVSG is replaced by Part 1 Sections 6.4.1 through 6.4.1.8 of the TGDC Recommendations, and redundant material is removed from Volume I Section 5.1.

- **Volume II Section 5.4** of the 2005 VVSG is replaced by Part 3 Section 4.5.1 of the TGDC Recommendations.
- **Volume II Section 1.8.2.6** (Certification Test Practices) of the 2005 VVSG is harmonized with Part 3 Section 2.5.5 of the TGDC Recommendations to clarify the handling of logic defects.
- **Volume II Sections 1.3.1.3, 1.7.1.2 and 5.2** are harmonized with the changes to Volume I Chapter 5.

4. **Test Plan and Test Report - Appendices A and B of Volume II** of the 2005 VVSG are harmonized with the current EAC manuals and NOC 09-001.

5. **TDP and Voting Equipment User Documentation – Volume II Section 2.1.1.1** of the 2005 VVSG is revised to include an outline of the TDP and the Voting Equipment User Documentation that is based on the TGDC Recommendations. Miscellaneous TDP requirements are added or modified to correct problems.

6. **(Non-EMC) Environmental Hardware**

   - **Volume I Section 4.1.2.13** (Environmental Control – Operating Environment) of the 2005 VVSG is revised with an operational temperature and humidity test requirement, with temperatures ranging from 41 °F to 104 °F (5 °C to 40 °C) and relative humidity from 5% to 85%, non-condensing.
   - **Volume II Section 4.7.1** (Temperature and Power Variation Tests) is replaced with requirements for testing according to appropriate procedures of MIL-STD-810D. Most of the previous text in this section was devoted to test materials, including detailed test scenarios, which will be included in the test materials for the final version of the VVSG 1.1.

7. **Human Factors Requirements** – The usability and accessibility requirements in **Volume I Section 3 of the 2005 VVSG** are replaced with requirements from Part 1 Chapter 3 of the TGDC Recommendations, with the exception of Chapter 3's performance benchmark requirements. Part 1 Chapter 3 of the TGDC Recommendations is primarily a maintenance level upgrade to the 2005 VVSG with minor modifications, clarifications, and a few additions including performance and poll worker usability requirements. (The 2005 VVSG Section 3 was mostly new material based on research, best practices, and standards relating to human factors and the design of user interfaces as they apply to voting systems.)

8. **System Security Documentation Requirements** - Security documentation requirements in **Volume II Section 2.6** (Security Documentation) of the 2005 VVSG are revised with requirements from Part 2 Section 3.5 (System Security Specification) of the TGDC Recommendations. The new requirements include high-level security descriptions of the voting system and specific areas including

   - Access control,
   - Software installation security,

- System event logging,
- Physical security,
- Setup inspection, and
- Cryptography.

9. **Electronic Records - Section 2.4.4** (Electronic Records) has been added to **Volume I Section 2** (Functional Requirements) of the 2005 VVSG; it contains requirements from Part 1 Chapter 4.3 (Electronic Records) of the TGDC Recommendations. These requirements cover the electronic reports generated by the voting system, including specific reports for tabulators and Election Management Systems (EMS).

10. **Voter Verified Paper Audit Trails (VVPAT)** - VVPAT requirements in **Volume I Sections 7.9.1 through 7.9.4** (Voter Verifiable Paper Audit Trail Requirements) are replaced with requirements from Part 1 Chapter 4.4.2 (VVPAT) of the TGDC Recommendations.

11. **Cryptography** - Cryptography requirements in the 2005 VVSG are revised with requirements from Part 1 Section 5.1 (Cryptography) of the TGDC Recommendations. When cryptography is used in a voting system, the requirements call for the use of a level 1 FIPS 140 validated cryptographic module (which allows software as well as hardware implementations, whereas the TGDC Recommendations allowed only hardware implementations). In addition, the new requirements require the use of NIST approved cryptographic algorithms at the 112-bit security strength or higher.

12. **External Interface Requirement - Volume I Section 7.4.6** (Software Setup Validation) of the 2005 VVSG are revised with newly developed requirements to allow an alternative method to validate software on voting systems. The requirements state that voting systems must support one of the two verification methods specified in the requirements. The current software verification method allows software to be verified after software has been installed. The alternative software verification method verifies software as it is being installed on the voting system and requires voting systems to have mechanisms to protect the software once installed.

13. **EAC Requests for Interpretation (RFI) decisions** - Requirements and discussion throughout the 2005 VVSG are revised based on the current set of EAC RFI decisions, from 2007-01 through 2010-08, located at http://www.eac.gov/testing_and_certification/request_for_interpretations1.aspx.

14. **Electronically-assisted ballot markers (EBMs) and hybrid devices** – Volume I Sections 1.5.1.3, 2.3.2, 2.3.3.3, and Chapter 3 are adjusted to clarify how the requirements of the VVSG apply to EBMs and other new kinds of voting devices.

15. **Minor clarifications and corrections** resulting from public comments and experience in the certification program are integrated throughout the document.

VOLUNTARY VOTING SYSTEM GUIDELINES

Volume I

Voting System Performance Guidelines

Voluntary Voting System Guidelines Overview

The United States Congress passed the Help America Vote Act of 2002 (HAVA) to modernize the administration of federal elections, marking the first time in our nation's history that the federal government has funded an election reform effort. HAVA provides federal funding to help the states meet the law's uniform and non-discretionary administrative requirements, which include the following new programs and procedures: 1) provisional voting, 2) voting information, 3) statewide voter registration lists and identification requirements for first-time registrants, 4) administrative complaint procedures, and 5) updated and upgraded voting equipment.

HAVA also established the U.S. Election Assistance Commission (EAC) to administer the federal funding and to provide guidance to the states in their efforts to comply with the HAVA administrative requirements. Section 202 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* (referred to herein as the *Guidelines* and/or *VVSG*), is the third iteration of national level voting system standards that has been developed. The Federal Election Commission published the *Performance and Test Standards for Punchcard, Marksense and Direct Recording Electronic Voting Systems* in 1990. This was followed by the *Voting Systems Standards* in 2002.

Version 1.0 of the VVSG was adopted by a vote of EAC on December 13, 2005. Version 1.1 of the VVSG was created by the EAC in an effort to update and improve version 1.0 of the VVSG. Specifically Version 1.1 provides updates to requirements in the areas of security, reliability, usability, and accessibility. These improvements enhance the testability and clarity of several of the requirements contained in version 1.0 of the VVSG.

Purpose and Scope of the *Guidelines*

The purpose of the *Voluntary Voting System 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 to ensure the integrity of voting systems. The *VVSG* specifies the functional requirements, performance characteristics, documentation requirements, and test evaluation criteria for the national certification of voting systems. The *VVSG* is composed of two volumes: Volume I, *Voting System Performance Guidelines* and Volume II, *National Certification Testing Guidelines.*

Effective Date

The *Voluntary Voting System Guidelines Version 1.1* will take effect after their final adoption by the EAC. At that time, all new systems submitted for national certification will be tested for conformance with these guidelines. In addition, if a modification to a system qualified or certified to a previous standard is submitted for national certification after this date, every component of the modified system will be tested against the *VVSG Version 1.1.* All previous versions of national standards will become obsolete at this time.

This *VVSG* effective date provision has no effect on the mandatory voting system requirements prescribed in HAVA Section 301(a), which states must comply with on or before January 1, 2006. The EAC issued Advisory 2005-004 to assist states in determining if a voting system is compliant with Section 301(a). This advisory is available on the EAC website at www.eac.gov.

Volume I: *Voting System Performance Guidelines Summary*

Volume I, the *Voting System Performance Guidelines*, describes the requirements for the electronic components of voting systems. It is intended for use by the broadest audience, including voting system developers, manufacturers and suppliers; voting system testing labs (VSTL); state organizations that certify systems prior to procurement; state and local election officials who procure and deploy voting systems; and public interest organizations that have an interest in voting systems and voting system standards. It contains the following sections:

Section I describes the purpose and scope of the *Voting System Performance Guidelines.*

Section 2 describes the functional capabilities required of voting systems. This section has been revised to reflect HAVA Section 301 requirements.

Section 3 describes new standards that make voting systems more usable and accessible for as many eligible citizens as possible, whatever their physical abilities, language skills, or experience with technology. This section reflects the HAVA 301 (a)(3) accessibility requirements.

Sections 4 through 6 describe specific performance standards for election system hardware, software, telecommunications, and security. Environmental criteria have been updated in Section 4.

Section 7 describes voting system security requirements and includes new requirements for voting system software distribution, generation of software reference information, validation of software during system setup, and the use of wireless. It also includes requirements for voter verifiable paper audit trail components for direct-recording electronic voting systems.

Section 8 describes requirements for manufacturer quality assurance and configuration management practices and the documentation about these practices required for the EAC certification process.

Appendix A contains a glossary of terms.

Appendix B provides a list of related standards documents incorporated into the *Guidelines* by reference, documents used in the preparation of the *Guidelines,* and referenced legislation.

Volume II: *National Certification Testing Guidelines Summary*

Volume II, the *National Certification Testing Guidelines*, is a complementary document to Volume I. Volume II provides an overview and specific detail of the national certification testing process, which is performed by independent voting system test labs (VSTL) accredited by the EAC. It is intended principally for use by manufacturers: VSTLs: and election officials who certify, procure, and accept voting systems. This volume contains the following sections:

Guide to Section Locations

Section 1 describes the purpose of the National Certification Testing Guidelines.

Section 2 provides a description of the Technical Data Package that manufacturers are required to submit with their system for certification testing.

Section 3 describes the basic functionality testing requirements.

Sections 4 through 6 define the requirements for hardware, software and system integration testing. Section 6 has been revised to reflect new requirements for usability and accessibility testing.

Section 7 describes the required examination of manufacturer quality assurance and configuration management practices.

Appendix A provides the requirements for the National Certification Test Plan that is prepared by the VSTL and provided to the EAC for review.

Appendix B describes the scope and content of the National Certification Test Report which is prepared by the VSTL and delivered to the EAC along with a recommendation for certification.

Appendix C describes a test method that is usable for assessing conformity to the requirements on accuracy and misfeed rate.

1 Introduction

Table of Contents

1 Introduction

1.1 Purpose and scope of the Voluntary Voting System Guidelines

The purpose of the *Voting System Performance 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. The performance guidelines specify the functional requirements, performance characteristics, documentation requirements, and test evaluation criteria for the national certification of voting systems. To the extent possible, these requirements and specifications are described so they can be assessed by a series of defined, objective tests.

Except as noted below, Volume I of the *Guidelines* applies to all system hardware, software, telecommunications, and documentation intended for use to:

- Prepare the voting system for use in an election
- Produce the appropriate ballot formats
- Test that the voting system and ballot materials have been properly prepared and are ready for use
- Record and count votes
- Consolidate and report election results
- Display results on-site or remotely
- Produce and maintain comprehensive audit trail data

Some voting systems use one or more commercial off-the-shelf (COTS) devices (such as card readers, printers, and personal computers) or software products (such as operating systems, programming language compilers, and database management systems). These devices and products are exempt from certain portions of system certification testing, as long as they are not modified for use in the voting system.

1.2 Use of the Voluntary Voting System Guidelines

The *Guidelines* are intended for use by multiple audiences to support their respective roles in the development, testing, and acquisition of voting systems:

- The accredited testing laboratories who use this information to develop test plans and procedures for the analysis and testing of systems in support of the national certification testing process
- State and local election officials who are evaluating voting systems for potential use in their jurisdictions

- Voting system designers and manufacturers who need to ensure that their products fulfill all these requirements so they can be certified

1.3 Evolution of Voting System Standards

1.3.1 Federal Election Commission

The first voting system standards were issued in January 1990, by the Federal Election Commission (FEC). This document included performance standards and testing procedures for Punchcard, Marksense, and Direct-Recording Electronic (DRE) voting systems. These standards did not cover paper ballot and mechanical lever systems because paper ballots are sufficiently self-explanatory not to require technical standards and mechanical lever systems are no longer manufactured or sold in the United States. The FEC also did not incorporate requirements for mainframe computer hardware because it was reasonable to assume that sufficient engineering and performance criteria already governed the operation of mainframe computers. However, vote tally software installed on mainframes was covered.

A national testing effort was initiated by NASED in 1994. As the system qualification process matured and qualified systems were used in the field, the NASED Voting Systems Board, in consultation with the testing labs, identified certain testing issues that needed to be resolved. Moreover, rapid advancements in information and personal computer technologies introduced new voting system development and implementation scenarios not contemplated by the 1990 Standards.

In 1997, NASED briefed the FEC on the importance of keeping the Standards up to date. Following a requirements analysis completed in 1999, the FEC initiated an effort to revise the 1990 Standards to reflect the evolving needs of the elections community. This resulted in the 2002 Voting Systems Standards.

Voters and election officials who use voting systems represent a broad spectrum of the population, and include individuals with disabilities who may have difficulty using traditional voting systems. In developing accessibility provisions for the 2002 Voting System Standards, the FEC requested assistance from the Access Board, the federal agency in the forefront of promulgating accessibility provisions. The Access Board submitted technical standards to meet the diverse needs of voters with a broad range of disabilities. The FEC adopted the entirety of the Access Board's recommendations and incorporated them into the 2002 Voting Systems Standards.

1.3.2 Election Assistance Commission

In 2002, Congress passed the Help America Vote Act, which established the U.S. Election Assistance Commission (EAC). EAC was mandated to develop and adopt new voluntary voting system guidelines and to provide for the testing, certification, and

decertification of voting systems. HAVA also established the Technical Guidelines Development Committee (TGDC) with the duty of assisting the EAC in the development of the new guidelines. The Director of NIST chairs the TGDC, and NIST was tasked to provide technical support to their work.

1.3.3 The EAC's Voting System Testing and Certification Program

The purpose of the Voting System Testing and Certification Program is to validate and document, through an independent testing process, that voting systems meet the requirements set forth in *VVSG* Volume 1 - *Voting System Performance Guidelines*, and perform according to the manufacturer's specifications for the system. Volume 1 specifies the minimum functional requirements, performance characteristics, documentation requirements, and test evaluation criteria that voting systems must meet in order to receive national certification. At this time, 35 states either require national certification or utilize the national standards when certifying voting systems. The EAC's Testing and Certification Program Manual documents the procedural requirements for this program.

Certification Testing under the EAC's program can only be performed by EAC accredited Voting System Test Labs (VSTLs). These VSTLs have been accredited for demonstrated technical competence to test voting systems using the *Guidelines*. Volume 2 of the *VVSG - National Testing and Certification Guidelines* - provides guidance on the testing process and describes the associated documentation requirements. These tests encompass the examination of software; the inspection and evaluation of system documentation; tests of hardware under conditions simulating the intended storage, operation, transportation, and maintenance environments; operational tests to validate system performance and function under normal and abnormal conditions; and examination of the manufacturer's system development, testing, quality assurance, and configuration management practices. Certification tests address individual system components or elements, as well as the integrated system as a whole. The EAC's Voting System Test Laboratory Program Manual sets out the procedures for the accreditation of testing laboratories.

Since 1994, testing of voting systems was performed by Independent Test Authorities (ITAs) certified by NASED. Upon the successful completion of testing, the ITA issued a Qualification Test Report to the manufacturer and NASED. The Technical Committee of the NASED Voting Systems Board would review the test report and, if satisfactory, issue a Qualification Number. The Qualification Number remains valid for as long as the voting system remains unchanged.

HAVA mandated that the certification testing process be transferred from NASED to EAC. National certification testing complements and evaluates the manufacturer's developmental testing and beta testing. The VSTL is expected to evaluate the completeness of the manufacturer's developmental test program, including the sufficiency of manufacturer tests conducted to demonstrate compliance with the *Guidelines* as well as the system's performance specifications. The VSTL undertakes sample testing of the

manufacturer's test modules and also designs independent system-level tests to supplement and check those designed by the manufacturer. Although some of the certification tests are based on those prescribed in the Military Standards, in most cases the test conditions are less stringent, reflecting commercial, rather than military, practice.

Upon review of test reports and a determination that satisfactory results were achieved that address the full scope of testing, EAC will issue a certification number that indicates the system has successfully completed testing by a VSTL for compliance with the *Guidelines*. The certification number applies to the system as a whole and does not apply to individual system components or untested configurations.

After a system has completed initial certification testing, further examination of the system is required if modifications are made to hardware, software, or telecommunications, including the installation of software on different hardware. Manufacturers request review of modifications by the VSTL based on the nature and scope of changes made. The VSTL will assess whether the modified system should be resubmitted for certification testing and the extent of testing to be conducted, and then it will provide an appropriate recommendation to the EAC and the manufacturer.

1.3.4 State Certification Testing

State certification tests are performed by individual states, with or without the assistance of outside consultants, to:

- Confirm that the voting system presented is the same as the one certified under the *Guidelines*
- Test for the proper implementation of state-specific requirements
- Establish a baseline for future evaluations or tests of the system, such as acceptance testing or state review after modifications have been made
- Define acceptance tests

State certification test scripts are not included in the *Guidelines,* as they must be defined by the state, with its laws, election practices, and needs in mind. However, it is recommended that they not duplicate the national certification tests, but instead focus on functional tests and qualitative assessment to ensure that the system operates in a manner that is acceptable under state law. If a voting system is modified after state certification is completed, it is recommended that states reevaluate the system to determine if further certification testing is warranted.

Certification tests performed by individual states typically rely on information contained in documentation provided by the manufacturer for system design, installation, operations, required facilities and supplies, personnel support and other aspects of the voting system. States and jurisdictions may define information and documentation requirements additional to those defined in the *Guidelines*. By design, the *Guidelines* do not address these additional requirements. However, national certification testing will address all the capabilities of a voting system stated by the manufacturer in the system

documentation submitted with the testing application to the EAC, including additional capabilities that are not required by the states.

1.3.5 Acceptance Testing

Acceptance tests are performed at the state or local jurisdiction level upon system delivery by the manufacturer to:

- Confirm that the system delivered is the specific system certified by EAC and, when applicable, certified by the state
- Evaluate the degree to which delivered units conform to both the system characteristics specified in the procurement documentation, and those demonstrated in the national and state certification tests
- Establish a baseline for any future required audits of the system

Some of the operational tests conducted during certification may be repeated during acceptance testing.

1.4 Definitions, References, and Types of Voting Systems

1.4.1 Definitions and References

The *Guidelines* contain terms describing function, design, documentation, and testing attributes of voting system hardware, software and telecommunications. Unless otherwise specified, the intended sense of technical terms is that which is commonly used by the information technology industry. In some cases terminology is specific to elections or voting systems. A glossary of terms is contained in Appendix A. Non-technical terms not listed in Appendix A **shall** be interpreted according to their standard dictionary definitions.

There are a number of technical standards that are incorporated in the *Guidelines* by reference. These are referred to by title in the body of the document. The full citations for these publications are provided in Appendix B. In addition, this appendix includes other references that may be useful for understanding and interpretation.

1.4.2 Types of Voting Systems

HAVA Section 301 defines a voting system as the total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment), that is used to define ballots; to cast and count votes; to report or display election results; and to maintain and produce any audit trail information. In addition, a voting system includes the practices and associated documentation used to identify system components and

versions of such components; to test the system during its development and maintenance; to maintain records of system errors and defects; to determine specific system changes made after initial certification; and to make available any materials to the voter (such as notices, instructions, forms, or paper ballots).

Traditionally, a voting system has been defined by the mechanism the system uses to cast votes and further categorized by the location where the system tabulates ballots. In addition to defining a common set of requirements that apply to all voting systems, the *VVSG* states requirements specific to a particular type of voting system, where appropriate. However, the *Guidelines* recognize that as the industry develops new solutions and the technology continues to evolve, the distinctions between voting system types may become blurred. The fact that the *VVSG* refers to specific system types is not intended to stifle innovations that may be based on a more fluid understanding of system types. However, appropriate procedures must be in place to ensure new developments provide the necessary integrity and can be properly evaluated in the certification process.

Consequently, manufacturers that submit a system that integrates components from more than one traditional system type or a system that includes components or technology not addressed in the *Guidelines* **shall** submit the results of all beta tests of the new system when applying for national certification. Manufacturers **shall** also submit a proposed test plan to the EAC for use in national certification testing. The *Guidelines* permit manufacturers to produce or utilize interoperable components of a voting system that are tested within the full voting system configuration.

The listing below summarizes the functional requirements that HAVA Section 301 mandates to assist voters. While these requirements may be implemented in a different manner for different types of voting systems, all types of voting systems must provide these capabilities:

- permit the voter to verify (in a private and independent manner) the vote selected by the voter on the ballot before the ballot is cast and counted
- provide the voter with the opportunity (in a private and independent manner) to change the ballot or correct any error before the ballot is cast and counted
- notify the voter if he or she has selected more than one candidate for a single office, inform the voter of the effect of casting multiple votes for a single office, and provide the voter an opportunity to correct the ballot before it is cast and counted
- be accessible for individuals with disabilities in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters
- provide alternative language accessibility pursuant to Section 203 of the Voting Rights Act

1.4.2.1 Paper-Based Voting System

A paper-based voting system records votes, counts votes, and produces a tabulation of the vote count from votes cast on paper cards or sheets. A marksense (also known as optical

scan) voting system allows a voter to record votes by making marks directly on the ballot, usually in voting response locations. Additionally, a paper-based system may allow for the voter's selections to be indicated by marks made on a paper ballot by an electronic input device, as long as such an input device does not independently record, store, or tabulate the voter selections.

1.4.2.2 Direct-Recording Electronic Voting System

A direct-recording electronic (DRE) voting system records votes by means of a ballot display provided with mechanical or electro-optical components that can be activated by the voter; that processes data by means of a computer program; and that records voting data and ballot images in memory components. It produces a tabulation of the voting data stored in a removable memory component and as printed copy. The system may also provide a means for transmitting individual ballots or vote totals to a central location for consolidating and reporting results from precincts at the central location.

1.4.2.3 Public Network Direct-Recording Electronic Voting System

A public network DRE voting system is an election system that uses electronic ballots and transmits vote data from the polling place to another location over a public network. Vote data may be transmitted as individual ballots as they are cast, periodically as batches of ballots throughout the Election Day, or as one batch at the close of voting. For purposes of the *Guidelines*, public network DRE voting systems are considered a form of DRE voting system and are subject to the standards applicable to DRE voting systems. However, because transmitting vote data over public networks relies on equipment beyond the control of the election authority, the system is subject to additional threats to system integrity and availability. Therefore, additional requirements are applied to provide appropriate security for data transmission.

The use of public networks for transmitting vote data must provide the same level of integrity as other forms of voting systems, and must be accomplished in a manner that precludes three risks to the election process: automated casting of fraudulent votes, automated manipulation of vote counts, and disruption of the voting process such that the system is unavailable to voters during the time period authorized for system use.

1.4.2.4 Precinct Count Voting System

A precinct count voting system is a voting system that tabulates ballots at the polling place. These systems typically tabulate ballots as they are cast and print the results after the close of polling. For DREs and some paper-based systems these systems provide electronic storage of the vote count and may transmit results to a central location over public telecommunication networks.

1.4.2.5 Central Count Voting System

A central count voting system is a voting system that tabulates ballots from multiple precincts at a central location. Voted ballots are typically placed into secure storage at the polling place. Stored ballots are transported or transmitted to a central counting location. The system produces a printed report of the vote count, and may produce a report stored on electronic media.

1.5 Conformance Clause

This section provides information and requirements relating to how manufacturers and VSTLs use this document to assess whether a voting system conforms to the VVSG.

1.5.1 Structure of Requirements

Each part of the VVSG is organized into sections that address topics of interest. Sections typically begin with prose explaining the general purpose, etc. This is informative background to help understand the requirements. Sections also contain requirements, which are the hard and fast rules to be followed for conformance. The VVSG carefully distinguish normative requirements from informative context by using normative keywords as defined below.

Each voting system requirement in Volume I is identified according to a hierarchical scheme in which higher-level requirements (such as "provide accessibility for visually impaired voters") are supported by lower-level requirements (e.g., "provide an audio-tactile interface"). Thus, requirements are nested. When the nesting hierarchy has reached four levels (i.e., 1.1.1.1), further nested requirements are designated with lowercase letters, then roman numerals. Therefore, all requirements are traceable by a distinct reference.

Some requirements are directly testable and some are not. The latter tend to be higher-level and are included because (1) they are testable indirectly insofar as their lower-level requirements are testable, and (2) they often provide the structure and rationale for the lower-level requirements. Satisfying the lower-level requirements will result in satisfying the higher-level requirement.

1.5.1.1 Normative Language

The following keywords are used to convey conformance requirements:

- **Shall –** indicates a mandatory requirement in order to conform. Synonymous with "is required to."

- **Shall not**, **is prohibited** –indicates a mandatory requirement that indicates something that is not permitted (allowed) in order to conform.
- **Should, is encouraged -** indicates an optional recommended action, one that is particularly suitable, without mentioning or excluding others. Synonymous with "is permitted and recommended."
- **May** - indicates an optional, permissible action. Synonymous with "is permitted."

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

Informative parts of this document include examples, extended explanations, and other matter that contain information necessary for proper understanding of the *Guidelines* and conformance to it. Unless otherwise specified, a list of examples should not be interpreted as excluding other possibilities that were not listed.

1.5.1.2 Applicability

The requirements, prohibitions, options, and guidance specified in these guidelines apply to voting systems, voting system manufacturers, VSTLs, and software repositories. In general, requirements for voting systems in these guidelines apply to all types of voting systems, unless prefaced with explanatory narrative that applicability is limited to a specific type of system or device.

The term "manufacturer" imposes documentation or testing requirements for the manufacturer. Other terms in these guidelines **shall** be construed as synonymous with "manufacturer," including "vendor," "voting system designers," and "implementer."

The terms used to designate requirements and procedural guidelines for accredited national certification testing laboratories are indicated by referring to "VSTL" (Voting System Test Lab). Other terms in these guidelines **shall** be construed as synonymous with "VSTL," including "accredited test labs," and "test labs." The term "repository" will be used to designate requirements levied on the National Software Reference Library repository maintained at NIST or any other designated repository.

These *Guidelines* are voluntary in that each of the states can decide whether to require the voting systems used in their state to have a national certification. States may decide to adopt these *Guidelines* in whole or in part at any time, irrespective of the effective date. In addition, states may specify additional requirements that voting systems in their jurisdiction must meet. The national certification program does not in any way pre-empt the ability of the states to have their own system certification process.

1.5.1.3 Categorizing Requirements

The *Guidelines* set forth a common set of requirements for national certification that apply to all types of electronic voting systems. They also provide requirements that are applicable for particular circumstances, such as alternative language capability or disability accessibility. The requirements implementing the HAVA Section 301(a)

mandates, except for disability accessibility, must be met by all voting systems. The alternative language capability mandated by Section 301(a)(4) must be met by all systems intended for use in jurisdictions subject to Section 203 of the Voting Rights Act. The Section 301(a)(3) disability accessibility requirements must be met by all systems intended to fulfill the one per polling place disability equipped voting system provision of Section 301(a)(3)(B).

In addition, the *Guidelines* categorize some requirements into related groups or classes of functionality to address equipment type, ballot tabulation location, and voting system component (e.g., election management system, voting machine). Hence, all of the requirements contained in the *Guidelines* do not apply to all elements of all voting systems. For example, requirements categorized as applying to DRE systems are not applicable to paper-based voting. The requirements implementing disability accessibility are not required of all voting systems, only by those systems the manufacturer designates as accessible voting systems.

Among the categories defined in the *VVSG* are two types of voting systems with respect to mechanisms to cast votes – paper-based voting systems and DRE voting systems. Additionally, voting systems are further categorized by the locations where ballots are tabulated – precinct count voting systems, which tabulate ballots at the polling place, and central count voting systems, which tabulate ballots from multiple precincts at a central location. The *Guidelines* define specific requirements for systems that fall within these four categories as well as various combinations of these categories.

When a device that is submitted for certification testing combines functions of more than one of the categories referred to in the *Guidelines*, that device must comply with all of the requirements that would apply to either or both categories of devices. For example, an electronic vote-capture device that is capable of recording votes either on an optical scan paper ballot or in electronic memory must comply with the requirements for paper-based systems when a paper record is created, and must comply with the requirements for DREs when electronic records are created.

1.5.1.4 Extensions

Extensions are additional functions, features, and/or capabilities included in a voting system that are not required by the *Guidelines*. To accommodate the needs of states that may impose additional requirements and to accommodate changes in technology, these guidelines allow extensions. For example, the requirements for a voter verifiable paper audit trail feature will only be applied to those systems designated by the manufacturer as providing this feature. The use of extensions **shall** not contradict nor cause the nonconformance of functionality required by the *Guidelines*.

1.5.2 Implementation Statement

The manufacturer **shall** provide an implementation statement with their application to the EAC for national certification testing.

An 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 (i.e., additional functionality beyond what is defined in the VVSG) that it implements.

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

a. An implementation statement **shall** include:
    i. Full product identification of the voting system, including version number or timestamp;
    ii. Separate identification of each device that is part of the voting system;
    iii. Version of VVSG to which conformity assessment is desired;
    iv. Voting variations supported (see Volume I Section 2.1.7.2);
    v. Device capacities and limits
    vi. List of languages supported;
    vii. List of accessibility capabilities; and
    viii. Signed attestation that the foregoing accurately characterizes the system submitted for testing.

A keyboard, mouse, accessibility peripheral or printer connected to a programmed voting device, as well as any optical drive, hard drive or similar component installed within it, are considered components of the voting device, not separate devices.

Specified capacities and limits should include the limit (if any) on the length of a candidate name that the system can process and display without truncation and similar limits for any other text fields whose usable or practically usable sizes are bounded. If the system provides a way to access the entirety of a long name even when it does not fit the width of the display and does not use any data structures that would force truncation, such a limit might not apply.

2 Functional Requirements

Table of Contents

2 Functional Requirements

This section contains requirements detailing the functional capabilities required of a voting system. This section sets out precisely what a voting system is required to do. In addition, it sets forth the minimum actions a voting system must be able to perform to be eligible for certification.

For organizational purposes, functional capabilities are categorized as follows by the phase of election activity in which they are required:

> **2.1 Overall System Capabilities**: These functional capabilities apply throughout the election process. They include security, accuracy, integrity, system auditability, election management system, vote tabulation, ballot counters, telecommunications, and data retention.
>
> **2.2 Pre-voting Capabilities**: These functional capabilities are used to prepare the voting system for voting. They include ballot preparation, the preparation of election-specific software (including firmware), the production of ballots, the installation of ballots and ballot counting software (including firmware), and system and equipment tests.
>
> **2.3 Voting System Capabilities**: These functional capabilities include all operations conducted at the polling place by voters and officials including the generation of status messages.
>
> **2.4 Post-voting Capabilities**: These functional capabilities apply after all votes have been cast. They include closing the polling place; obtaining reports by voting machine, polling place, and precinct; obtaining consolidated reports; and obtaining reports of audit trails.
>
> **2.5 Maintenance, Transportation and Storage Capabilities**: These capabilities are necessary to maintain, transport, and store voting system equipment.

In recognition of the diversity of voting systems, the *Guidelines* apply specific requirements to specific technologies. Some of the guidelines apply only if the system incorporates certain optional functions (for example, voting systems employing telecommunications to transmit voting data). For each functional capability, common requirements are specified. Where necessary, these are followed by requirements applicable to specific technologies (i.e., paper-based or DRE) or intended use (i.e., central or precinct count).

2.1 Overall System Capabilities

This section defines required functional capabilities that are system-wide in nature and not unique to pre-voting, voting, and post-voting operations. All voting systems **shall** provide the following functional capabilities, further outlined in this section:

2.1.1 Security
2.1.2 Accuracy
2.1.3 Error Recovery
2.1.4 Integrity
2.1.5 System Audit
2.1.6 Election Management System
2.1.7 Vote Tabulating Program
2.1.8 Ballot Counter
2.1.9 Telecommunications
2.1.10 Data Retention

Voting systems may also include telecommunications components. Technical standards for these capabilities are described in Sections 3 through 6 of the *Voluntary Voting System Guidelines.*

2.1.1 Security

System security is achieved through a combination of technical capabilities and sound administrative practices. To ensure security, all systems **shall**:

a. Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability
b. Provide system functions that are executable only in the intended manner and order, and only under the intended conditions
c. Use the system's control logic to prevent a system function from executing if any preconditions to the function have not been met
d. Provide safeguards in response to system failure to protect against tampering during system repair or interventions in system operations
e. Provide security provisions that are compatible with the procedures and administrative tasks involved in equipment preparation, testing, and operation
f. Incorporate a means of implementing a capability if access to a system function is to be restricted or controlled
g. Provide documentation of mandatory administrative procedures for effective system security

2.1.2 Accuracy

Memory hardware, such as semiconductor devices and magnetic storage media, must be accurate. The design of equipment in all voting systems **shall** provide for the highest possible levels of protection against mechanical, thermal, and electromagnetic stresses that impact system accuracy. Section 4 provides additional information on susceptibility requirements.

To ensure vote accuracy, all systems **shall**:

a. Record the election contests, candidates, and issues exactly as defined by election officials
b. Record the appropriate options for casting and recording votes
c. Record each vote precisely as indicated by the voter and produce an accurate report of all votes cast;
d. Include control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) to demonstrate that the system has been designed for accuracy
e. Provide software that monitors the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected

In addition, DRE systems **shall**:

f. As an additional means of ensuring accuracy in DRE systems, voting devices **shall** record and retain redundant copies of the original ballot image. A ballot image is an electronic record of all votes cast by the voter, including undervotes.

The accuracy benchmark specified in Section 4.1.1 is intended to allow tolerance for unpreventable hardware-related errors that occur rarely and randomly as a result of physical phenomena affecting optical scanning sensors. It is not intended to allow tolerance of software faults that result in systematic miscounting of votes. As was written in Section 7.1.1 of the 1990 VSS, “In this case, no margin for error exists.” Therefore,

g. In all systems, voting system software, firmware, and hardwired logic **shall** maintain absolute correctness (introduce no errors) in the recording, tabulating, and reporting of votes.

2.1.3 Error Recovery

To recover from a non-catastrophic failure of a device, or from any error or malfunction that is within the operator's ability to correct, the system **shall** provide the following capabilities:

a. Restoration of the device to the operating condition existing immediately prior to the error or failure, without loss or corruption of voting data previously stored in the device
b. Resumption of normal operation following the correction of a failure in a memory component, or in a data processing component, including the central processing unit
c. Recovery from any other external condition that causes equipment to become inoperable, provided that catastrophic electrical or mechanical damage due to external phenomena has not occurred

2.1.4 Integrity

Integrity measures ensure the physical stability and function of the vote recording and counting processes.

To ensure system integrity, all systems **shall**:

a. Protect against a single point of failure that would prevent further voting at the polling place
b. Protect against the interruption of electrical power
c. Protect against generated or induced electromagnetic radiation
d. Protect against ambient temperature and humidity fluctuations
e. Protect against the failure of any data input or storage device
f. Protect against any attempt at improper data entry or retrieval
g. Include built-in measurement, self-test, and diagnostic software and hardware for detecting and reporting the system's status and degree of operability

In addition to the common requirements, DRE systems **shall**:

h. Maintain a record of each ballot cast using a process and storage location that differs from the main vote detection, interpretation, processing, and reporting path
i. Provide a capability to retrieve ballot images in a form readable by humans

2.1.5 System Audit

This subsection describes the context and purpose of voting system audits and sets forth specific functional requirements. Election audit trails provide the supporting documentation for verifying the accuracy of reported election results. They present a concrete, indestructible archival record of all system activity related to the vote tally, and are essential for public confidence in the accuracy of the tally, for recounts, and for evidence in the event of criminal or civil litigation.

These requirements are based on the premise that system-generated creation and maintenance of audit records reduces the chance of error associated with manually generated audit records. Because most audit capability is automatic, the system operator has less information to track and record, and is less likely to make mistakes or omissions.

The subsections that follow present operational requirements critical to acceptable performance and reconstruction of an election. Requirements for the content of audit records are described in Section 5.

The requirements for all system types, both precinct and central count, are described in generic language. Because the actual implementation of specific characteristics may vary from system to system, it is the responsibility of the manufacturer to describe each system's characteristics in sufficient detail so that VSTLs and system users can evaluate the adequacy of the system's audit trail. This description **shall** be incorporated in the System Operating Manual, which is part of the Technical Data Package.

Documentation of items such as paper ballots delivered, paper ballots collected, administrative procedures for system security, and maintenance performed on voting equipment are also part of the election audit trail, but are not covered in these technical standards. Useful guidance is provided by the FEC publication *Innovations in Election Administration #10: Ballot Security and Accountability*, available on the EAC's website.

2.1.5.1 Operational Requirements

Audit records **shall** be prepared for all phases of election operations performed using devices controlled by the jurisdiction or its contractors. These records rely upon automated audit data acquisition and machine-generated reports, with manual input of some information. These records **shall** address the ballot preparation and election definition phase, system readiness tests, and voting and ballot-counting operations. The software **shall** activate the logging and reporting of audit data as described below.

a. Voting system equipment **shall** record activities through an event logging mechanism.
b. Voting system equipment **shall** enable file integrity protection for stored log files as part of the default configuration.
c. The voting system equipment logs **shall** not contain information that, if published, would violate ballot secrecy or voter privacy or that would compromise voting system security in any way.
d. The voting system equipment **shall** log at a minimum the following data characteristics for each type of event: 1) system ID; 2) unique event ID and/or type; 3) timestamp; 4) success or failure of event, if applicable; 5) User ID trigger the event, if applicable; 6) Resources requested, if applicable.
    i. Timekeeping mechanisms **shall** generate time and date values.
    ii. The precision of the timekeeping mechanism **shall** be able to distinguish and properly order all audit records.
    iii. Timestamps **shall** include the date and time, including hours, minutes and seconds.
    iv. Timestamps **shall** comply with ISO 8601 and provide all four digits of the year and include the applicable time zone.
    v. Voting system equipment **shall** only allow administrators to set or adjust the clock.

vi. Voting system equipment **shall** limit clock drift to a minimum of 1 minute within a 15 hour period after the clock is set.

e. Voting system equipment **shall** log all normal and abnormal events.
   i. Voting system equipment **shall** ensure that event logging cannot be disabled.
f. Voting system equipment **shall** implement default settings for secure log management activities, including log generation, transmission, storage, analysis and disposal.
g. Voting system equipment **shall** log logging failures, log clearing, and log rotation.
h. Voting systems **shall** store logs in a publicly documented log format, such as XML, or include a utility to export the logs into a publicly documented for off-system viewing.
i. The manufacturer **shall** ensure that voting system equipment is supplied with enough free storage to include several maximum size event logs.
j. Voting systems **shall** be capable of retaining event log data from previous elections.
k. Voting system equipment **shall** only allow administrators to modify the log data retention settings including the actions to take when a log reaches its maximum retention such as overwriting logs, rotating logs, or halting logging.
l. Voting system equipment **shall** be capable of rotating the event log data to manage log file growth.
m. Voting system equipment **shall** restrict event log access to write or append-only for privileged logging processes and read-only for administrators accounts or roles.
n. Voting system equipment **shall** digitally sign and export event logs at the end of an election.
o. Voting systems **shall** include an application or program to view, analyze, and search event logs.
p. Voting system equipment **shall** halt voting activities and create an alert if the logging system malfunctions or is disabled.
q. Voting system equipment **shall** create an alert at user-defined intervals as logs begin to fill.
r. Voting system equipment **shall** protect event log information from unauthorized access, modification and deletion.
s. If the voting system provides log archival capabilities, it **shall** ensure the integrity and availability of the archived logs.

All voting systems **shall** meet the requirements for error messages below.

a. The voting system **shall** generate, store, and report to the user all error messages as they occur.
b. All error messages requiring intervention by an operator or precinct official **shall** be displayed or printed clearly in easily understood language text, or by means of other suitable visual indicators.
c. When the voting system uses numerical error codes for trained technician maintenance or repair, the text corresponding to the code **shall** be self-contained or affixed inside the voting machine. This is intended to reduce inappropriate reactions to error conditions, and to allow for ready and effective problem correction.

d. All error messages for which correction impacts vote recording or vote processing **shall** be written in a manner that is understandable to an election official who possesses training on system use and operation, but does not possess technical training on system servicing and repair.
e. The message cue for all voting systems **shall** clearly state the action to be performed in the event that voter or operator response is required.
f. Voting system design **shall** ensure that erroneous responses will not lead to irreversible error.
g. Nested error conditions **shall** be corrected in a controlled sequence such that voting system status **shall** be restored to the initial state existing before the first error occurred.

The *Guidelines* provide latitude in software design so that manufacturers can consider various user processing and reporting needs. The jurisdiction may require some status and information messages to be displayed and reported in real-time. Messages that do not require operator intervention may be stored in memory to be recovered after ballot processing has been completed.

The voting system **shall** display and report critical status messages using clear indicators or English language text. The voting system need not display non-critical status messages at the time of occurrence. Voting systems may display non-critical status messages (i.e., those that do not require operator intervention) by means of numerical codes for subsequent interpretation and reporting as unambiguous text.

Voting systems **shall** provide a capability for the status messages to become part of the real-time audit record. The voting system **shall** provide a capability for a jurisdiction to designate critical status messages.

2.1.5.2 Use of *Multitasking Operating Systems*[1]

To ensure completeness and integrity of audit data for election software, further requirements must be applied to *voting devices that use multitasking operating systems (including COTS operating systems)* capable of executing multiple application programs simultaneously. These *operating* systems *support* both servers and workstations and *include* the many varieties of UNIX and Linux, and those offered by Microsoft and Apple. Election software *(including any COTS or other software applications used in the voting system)* running on these systems is vulnerable to unintended effects from other user sessions, applications, and utilities executing on the same platform at the same time as the election software.

Simultaneous processes of concern include: unauthorized network connections, unplanned user logins, and unintended execution or termination of operating system processes. An unauthorized network connection or unplanned user login can host unintended processes and user actions, such as the termination of operating system audit,

1 The italicized text in Section 2.1.5.2 is based on EAC Decision on Request for Interpretation 2008-03, http://www.eac.gov/assets/1/Page/EAC%20Decision%20on%20OS%20Configuration.pdf.

the termination of election software processes, or the deletion of election software audit and logging data. The execution of an operating system process could be a full system scan at a time when that process would adversely affect the election software processes. Operating system processes improperly terminated could be system audit or malicious code detection.

To counter these vulnerabilities, three operating system protections are required on all *multitasking operating* systems. First, authentication **shall** be configured on the local terminal (*e.g.,* display screen and keyboard) and on all external connection devices *(e.g.,* network cards and ports). This ensures that only authorized and identified users affect the system while election software is running.

Second, operating system audit **shall** be enabled for all session openings and closings, for all connection openings and closings, for all process executions and terminations, and for the alteration or deletion of any memory or file object. This ensures the accuracy and completeness of election data stored on the system. It also ensures the existence of an audit record of any person or process altering or deleting system data or election data.

Third, the system **shall** be configured to execute only intended and necessary processes during the execution of election software. The system **shall** also be configured to halt election software processes upon the termination of any critical system process (such as system audit) during the execution of election software.

The manufacturer may use whatever metrics it wishes to establish the correct configuration of multitasking operating systems. To ensure that these metrics are complete and consistent with current best practices for operating system security, the VSTL **shall** evaluate the configuration documentation provided by the manufacturer in order to determine completeness, clarity, and consistency with best practice checklist criteria. The VSTL **shall** provide additional information if any inconsistency exists with the checklist criteria. This information must include any rationale supporting the contention that any inconsistencies with the checklist are either not applicable or have been mitigated.

In its review of the VSTL evaluation of the operating system(s) configuration, the EAC will designate appropriate checklists from the National Vulnerability Database (NVD) System Content Automation Protocol (SCAP) checklist repository as the benchmark for appropriate settings. If the operating system configuration is at variance to the designated SCAP checklist, a justification for the variance **shall** be requested. It is recognized that in some cases variances may be justifiable for optimum security and functionality.

For a given system, some requirements may appropriately be determined to be not applicable to a specific device (e.g., ballot marking devices), depending specifically how the design of a device is implemented and what features are included. Those determinations will be decided on a case-by-case, model by model, revision by revision basis, primarily by the VSTL, and then presented to the EAC for approval.

2.1.6 Election Management System

The Election Management System (EMS) is used to prepare ballots and programs for use in casting and counting votes, and to consolidate, report, and display election results. An EMS **shall** generate and maintain a database, or one or more interactive databases, that enables election officials or their designees to perform the following functions:

- Define political subdivision boundaries and multiple election districts as indicated in the system documentation
- Identify contests, candidates, and issues
- Define ballot formats and appropriate voting options
- Generate ballots and election-specific programs for voting equipment
- Install ballots and election-specific programs
- Test that ballots and programs have been properly prepared and installed
- Accumulate vote totals at multiple reporting levels as indicated in the system documentation
- Generate the post-voting reports required by Subsection 2.4
- Process and produce audit reports of the data as indicated in Subsection 5.5

2.1.7 Vote Tabulating Program

Each voting system **shall** have a vote tabulation program that will meet specific functional requirements.

2.1.7.1 Functions

The vote tabulating program software resident in each voting machine, vote count server, or other devices **shall** include all software modules required to:

a. Monitor system status and generate machine-level audit reports
b. Accommodate device control functions performed by polling place officials and maintenance personnel
c. Register and accumulate votes
d. Accommodate variations in ballot counting logic

2.1.7.2 Voting Variations

There are significant variations among state election laws with respect to permissible ballot contents, voting options, and the associated ballot counting logic. The Technical Data Package accompanying the system **shall** specifically identify which of the following items *can* and *cannot* be supported by the voting system, as well as *how* the voting system can implement the items supported:

- Closed primaries

- Open primaries
- Partisan offices
- Non-partisan offices
- Write-in voting
- Primary presidential delegation nominations
- Ballot rotation
- Straight party voting
- Cross-party endorsement
- Split precincts
- Vote for N of M
- Recall issues, with options
- Cumulative voting
- Ranked order voting
- Provisional or challenged ballots

2.1.8 Ballot Counter

For all voting systems, each piece of voting equipment that tabulates ballots **shall** provide a counter that:

a. Can be set to zero before any ballots are submitted for tally
b. Records the number of ballots cast during a particular test cycle or election
c. Increases the count only by the input of a ballot
d. Prevents or disables the resetting of the counter by any person other than authorized persons at authorized points
e. Is visible to designated election officials

2.1.9 Telecommunications

For all voting systems that use telecommunications for the transmission of data during pre-voting, voting or post-voting activities, capabilities **shall** be provided that ensure data are transmitted with no alteration or unauthorized disclosure during transmission. Such transmissions **shall** not violate the privacy, secrecy, and integrity demands of the *Guidelines*. Section 6 describes telecommunications standards that apply to, at a minimum, the following types of data transmissions:

Voter Authentication: Coded information that confirms the identity of a voter for security purposes for a system that transmit votes individually over a public network

Ballot Definition: Information that describes to voting equipment the content and appearance of the ballots to be used in an election

Vote Transmission to Central Site: For voting systems that transmit votes individually over a public network, the transmission of a vote or votes to the county (or contractor) for consolidation with other vote data

Vote Count: Information representing the tabulation of votes at any one of several levels: polling place, precinct, or central count

List of Voters: A listing of the individual voters who have cast ballots in a specific election

2.1.10 Data Retention

United States Code Title 42, Sections 1974 through 1974e state that election administrators **shall** preserve for 22 months "all records and paper that came into (their) possession relating to an application, registration, payment of poll tax, or other act requisite to voting." This retention requirement applies to systems that will be used at any time for voting of candidates for federal offices (e.g., Member of Congress, United States Senator, and/or Presidential Elector). Therefore, all voting systems **shall** provide for maintaining the integrity of voting and audit data during an election and for a period of at least 22 months thereafter.

Because the purpose of this law is to assist the federal government in discharging its law enforcement responsibilities in connection with civil rights and elections crimes, its scope must be interpreted in keeping with that objective. The appropriate state or local authority must preserve all records that may be relevant to the detection and prosecution of federal civil rights or election crimes for the 22-month federal retention period, if the records were generated in connection with an election that was held in whole or in part to select federal candidates. It is important to note that Section 1974 does not require that election officials generate any specific type or classification of election record. However, if a record is generated, Section 1974 comes into force and the appropriate authority must retain the records for 22 months.

For 22-month document retention, the general rule is that all printed copy records produced by the election database and ballot processing systems **shall** be so labeled and archived. Regardless of system type, all audit trail information spelled out in Subsection 5.5 **shall** be retained in its original format, whether that be real-time logs generated by the system, or manual logs maintained by election personnel. The election audit trail includes not only in-process logs of election-night and subsequent processing of absentee or provisional ballots, but also time logs of baseline ballot definition formats, and system readiness and testing results.

In many voting systems, the source of election-specific data (and ballot formats) is a database or file. In precinct count voting systems, this data is used to program each machine, establish ballot layout, and generate tallying files. It is not necessary to retain this information on electronic media if there is an official, authenticated printed copy of all final database information. However, it is recommended that the state or local jurisdiction also retain electronic records of the aggregate data for each voting machine so that reconstruction of an election is possible without data re-entry. The same requirement and recommendation applies to vote results generated by each precinct count voting machine.

2.2 Pre-voting Capabilities

This subsection defines capabilities required to support functions performed prior to the opening of polls. All voting systems **shall** provide capabilities to support:

- Ballot preparation
- Election programming
- Ballot and program installation and control
- Readiness testing
- Verification at the polling place
- Verification at the central counting place

The standards also include requirements to ensure compatible interfaces with the ballot definition process and the reporting of election results.

2.2.1 Ballot Preparation

Ballot preparation is the process of using election databases to define the specific contests, questions, and related instructions to be contained in ballots and to produce all permissible ballot layouts. Ballot preparation requirements include:

- General capabilities
- Ballot formatting
- Ballot production

2.2.1.1 General Capabilities

All systems **shall** provide the general capabilities for ballot preparation. All systems **shall** be capable of:

a. Enabling the automatic formatting of ballots in accordance with the requirements for offices, candidates, and measures qualified to be placed on the ballot for each political subdivision and election district
b. Collecting and maintaining the following data
    i. Offices and their associated labels and instructions
    ii. Candidate names and their associated labels
    iii. Issues or measures and their associated text
c. Supporting the maximum number of potentially active voting positions as indicated in the system documentation
d. For a primary election, generating ballots that segregate the choices in partisan contests by party affiliation
e. Generating ballots that contain identifying codes or marks uniquely associated with each format
f. Ensuring that vote response fields, selection buttons, or switches properly align with the specific candidate names and/or issues printed on the ballot display, ballot or ballots, or separate ballot pages

Paper-based voting systems **shall** also meet the following requirements applicable to the technology used:

g. Enable voters to make selections by making a mark in areas designated for this purpose upon each ballot sheet
h. For marksense systems, ensure that the timing marks align properly with the vote response fields

2.2.1.2 Ballot Formatting

Ballot formatting is the process by which election officials or their designees use election databases and voting system software to define the specific contests and related instructions contained on the ballot and present them in a layout permitted by state law. All voting systems **shall** provide a capability for:

a. Creation of newly defined elections
b. Rapid and error-free definition of elections and their associated ballot layouts
c. Uniform allocation of space and fonts used for each office, candidate, and contest such that the voter perceives no active voting position to be preferred to any other
d. Simultaneous display of the maximum number of choices for a single contest as indicated by the manufacturer in the system documentation
e. Retention of previously defined formats for an election
f. Prevention of unauthorized modification of any ballot formats
g. Modification by authorized persons of a previously defined ballot format for use in a subsequent election

2.2.1.3 Ballot Production

Ballot production is the process of converting ballot formats to a media ready for use in the physical ballot production or electronic presentation.

The voting system **shall** provide a means of printing or otherwise generating a ballot display that can be installed in all voting equipment for which it is intended. All voting systems **shall** provide the capabilities below.

a. The electronic display or printed document on which the user views the ballot is capable of rendering an image of the ballot in any of the languages required by the Voting Rights Act of 1965, as amended.
b. The electronic display or printed document on which the user views the ballot does not show any advertising or commercial logos of any kind, whether public service, commercial, or political, unless specifically provided for in state law. Electronic displays **shall** not provide connection to such material through hyperlink.
c. The ballot conforms to manufacturer specifications for type of paper stock, weight, size, shape, size and location of mark field used to record votes, folding,

bleed-through, and ink for printing if paper ballot documents or paper displays are part of the system.

Basic Test Methodology[2]

Voting systems **shall** be tested to validate their ability to format and display voter targeted messages in a form consistent with all covered languages. (Incorporate the accents and special characters for Spanish or other languages, display translated text as an image, etc.) The VSTL **shall** also provide a statement in the test report that identifies the level to which the language testing was performed. When appropriate, the VSTL **shall** insert a disclaimer in the report that the translation content was not validated and that jurisdictions need to validate the content and accuracy of all translations. For DREs, basic functional testing of the ballot logic **shall** be repeated for at least one of the set of languages in each of the significant language groups where the manufacturer supports such language groups. For the purpose of this test procedure, the functional language groups are:

a. The default language (English)
b. A secondary language using a Western European font (usually Spanish)
c. Ideographic language (such as Chinese or Korean)
d. Non-written languages requiring audio support

The ballot preparation process **shall** prompt for an audio ballot to associate with each alternate language provided. In addition, a sample of audio ballots in each group should be checked with at least one audio set to confirm that the voter is presented the correct audio ballot for the language selected. The check **shall** exercise full ballot logic and navigational choices including shortcuts to exit or skip candidates or races. Care **shall** be taken to assure that less used navigation paths are checked.

For mark sense/paper ballots, the additional functional tests may be waived if one of the following is true:

e. The operational test deck contains all ballot styles including the alternate language ballots as separate styles.
f. It can be demonstrated that the ballot layout is not altered due to a change in language choice. (i.e., all ballot coding and voting mark sense target locations are the same regardless of ballot choices.)

> Discussion: While the voting system need not offer every language covered by Section 203 of the Voting Rights Act, the system must be tested and shown to have the capability to present or display any of the covered languages noted above.

Manufacturer documentation for marksense systems **shall** include specifications for ballot materials to ensure that vote selections are read from only a single ballot at a time,

2 The italicized text in Section 2.2.1.3 is based on EAC Decision on Request for Interpretation 2008-04, http://www.eac.gov/assets/1/Page/EAC%20Decision%20on%20Supported%20Languages.pdf.

without detection of marks from multiple ballots concurrently (e.g., reading of bleed-through from other ballots).

2.2.2 Election Programming

Election programming is the process by which election officials or their designees use election databases and manufacturer system software to logically define the voter choices associated with the contents of the ballots. All systems **shall** provide for the:

a. Logical definition of the ballot, including the definition of the number of allowable choices for each office and contest
b. Logical definition of political and administrative subdivisions, where the list of candidates or contests varies between polling places
c. Exclusion of any contest on the ballot in which the voter is prohibited from casting a ballot because of place of residence, or other such administrative or geographical criteria
d. Ability to select from a range of voting options to conform to the laws of the jurisdiction in which the system will be used
e. Generation of all required master and distributed copies of the voting program, in conformance with the definition of the ballots for each voting device and polling place, and for each tabulating device

2.2.3 Ballot and Program Installation and Control

All systems **shall** provide a means of installing ballots and programs on each piece of polling place or central count equipment in accordance with the ballot requirements of the election and the requirements of the jurisdiction in which the equipment will be used. All systems **shall** include the following at the time of ballot and program installation:

a. A detailed work plan or other documentation providing a schedule and steps for the software and ballot installation, which includes a table outlining the key dates, events and deliverables
b. A capability for automatically verifying that the software has been properly selected and installed in the equipment or in programmable memory devices, and for indicating errors
c. A capability for automatically validating that software correctly matches the ballot formats that it is intended to process, for detecting errors, and for immediately notifying an election official of detected errors

2.2.4 Readiness Testing

Election personnel conduct voting equipment and voting system readiness tests prior to the start of an election to ensure that the voting system functions properly, to confirm that

voting equipment has been properly integrated, and to obtain equipment status reports. All voting systems **shall** provide the capabilities to:

a. Verify that voting equipment and precinct count equipment is properly prepared for an election, and collect data that verifies equipment readiness
b. Obtain status and data reports from each set of equipment
c. Verify the correct installation and interface of all voting equipment
d. Verify that hardware and software function correctly
e. Generate consolidated data reports at the polling place and higher jurisdictional levels
f. Segregate test data from actual voting data, either procedurally or by hardware/software features

Resident test software, external devices, and special purpose test software connected to or installed in voting equipment to simulate operator and voter functions may be used for these tests provided that the following standards are met:

g. These elements **shall** be capable of being tested separately, and **shall** be proven to be reliable verification tools prior to their use
h. These elements **shall** be incapable of altering or introducing any residual effect on the intended operation of the voting device during any succeeding test and operational phase

Paper-based systems **shall**:

i. Support conversion testing that uses all potential ballot positions as active positions
j. Support conversion testing of ballots with active position density for systems without pre-designated ballot positions

2.2.5 Verification at the Polling Place

Election officials perform verification at the polling place to ensure that all voting systems and voting equipment function properly before and during an election. All voting systems **shall** provide a formal record of the following, in any media, upon verification of the authenticity of the command source:

a. The election's identification data
b. The identification of all equipment units
c. The identification of the polling place
d. The identification of all ballot formats
e. The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain only zeros)
f. A list of all ballot fields that can be used to invoke special voting options
g. Other information needed to confirm the readiness of the equipment, and to accommodate administrative reporting requirements

To prepare voting devices to accept voted ballots, all voting systems **shall** provide the capability to test each device prior to opening to verify that each is operating correctly. At a minimum, the tests **shall** include:

h. Confirmation that there are no hardware or software failures
i. Confirmation that the device is ready to be activated for accepting votes

If a precinct count system includes equipment for the consolidation of polling place data at one or more central counting locations, it **shall** have means to verify the correct extraction of voting data from transportable memory devices, or to verify the transmission of secure data over secure communication links.

2.2.6 Verification at the Central Location

Election officials perform verification at the central location to ensure that vote counting and vote consolidation equipment and software function properly before and after an election. Upon verification of the authenticity of the command source, any system used in a central count environment **shall** provide a printed record of the following:

a. The election's identification data
b. The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain all zeros)
c. Other information needed to ensure the readiness of the equipment and to accommodate administrative reporting requirements

2.3 Voting Capabilities

All voting systems **shall** support:

- Opening the polls
- Casting a ballot

Additionally, all DRE systems **shall** support:

- Activating the ballot
- Augmenting the election counter
- Augmenting the life-cycle counter

2.3.1 Opening the Polls

a. All vote counters must be zeroed before polls are opened. If a device has a non-zero counter or residual votes, this is a failure to activate correctly and thus a device or system failure. Therefore the device **shall** disable itself from use in the

voting system and election officials **shall** be advised of the proper corrective action.

i. The occurrence **shall** be recorded in the device audit log.
ii. In addition, a clear, unambiguous warning that an attempt has been made to initiate an election with non-zero totals and that the device has been disabled from the system **shall** be documented and communicated to an election official.

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

The other capabilities required for opening the polls are specific to individual voting system technologies. At a minimum, the systems **shall** provide the functional capabilities indicated below.

2.3.1.1 Precinct Count Systems

To allow voting devices to be activated for voting, all precinct count systems **shall** provide:

a. An internal test or diagnostic capability to verify that all of the polling place tests specified in Subsection 2.2.5 have been successfully completed
b. Automatic disabling of any device that has not been tested until it has been tested

2.3.1.2 Paper-based System Requirements

To facilitate opening the polls, all paper-based systems **shall** include:

a. A means of verifying that ballot marking devices are properly prepared and ready to use
b. A voting booth or similar facility, in which the voter may mark the ballot in privacy
c. Secure receptacles for holding voted ballots

In addition to the above requirements, all paper-based precinct count equipment **shall** include a means of:

d. Activating the ballot counting device
e. Verifying that the device has been correctly activated and is functioning properly
f. Identifying device failure and corrective action needed

2.3.1.3 DRE System Requirements

To facilitate opening the polls, all DRE systems **shall** include:

a. A security seal, a password, or a data code recognition capability to prevent the inadvertent or unauthorized actuation of the poll-opening function
b. A means of enforcing the execution of steps in the proper sequence if more than one step is required
c. A means of verifying the system has been activated correctly
d. A means of identifying system failure and any corrective action needed

2.3.2 Activating the Ballot

To activate the ballot, all DRE systems and all electronically-assisted ballot markers (EBMs) **shall**:

a. Enable election officials to control the content of the ballot presented to the voter, whether presented in printed form or electronic display, such that each voter is permitted to record votes only in contests in which that voter is authorized to vote
b. Enable the selection of the ballot that is appropriate to the party affiliation declared by the voter in a primary election
c. Activate all portions of the ballot upon which the voter is entitled to vote
d. Disable all portions of the ballot upon which the voter is not entitled to vote

In addition, all DRE systems **shall**:

e. Allow each eligible voter to cast a ballot
f. Prevent a voter from voting on a ballot to which he or she is not entitled
g. Prevent a voter from casting more than one ballot in the same election
h. Activate the casting of a ballot in a general election

2.3.3 Casting a Ballot

Some required capabilities for casting a ballot are common to all systems. Others are specific to individual voting technologies or intended use. Systems must provide additional functional capabilities that enable accessibility to disabled voters as defined in Subsection 3.2.

2.3.3.1 Common Requirements

To facilitate casting a ballot, all systems **shall**:

a. Provide text that is at least 3 millimeters high and provide the capability to adjust or magnify the text to an apparent size of 6.3 millimeters

b. Protect the secrecy of the vote such that the system cannot reveal any information about how a particular voter voted, except as otherwise required by individual state law
c. Record the selection and non-selection of individual vote choices for each contest and ballot measure
d. Record the voter's selection of candidates whose names do not appear on the ballot, if permitted under state law, and record as many write-in votes as the number of candidates the voter is allowed to select
e. In the event of a failure of the main power supply external to the voting system, provide the capability for any voter who is voting at the time to complete casting a ballot, allow for the successful shutdown of the voting system without loss or degradation of the voting and audit data, and allow voters to resume voting once the voting system has reverted to back-up power
f. Provide the capability for voters to continue casting ballots in the event of a failure of a telecommunications connection within the polling place or between the polling place and any other location

2.3.3.2 Paper-based System Requirements

All paper-based systems **shall**:

a. Allow the voter to easily identify the voting field that is associated with each candidate or ballot measure response
b. Allow the voter to mark the ballot to register a vote
c. Allow either the voter or the appropriate election official to place the voted ballot into the ballot counting device (for precinct count systems) or into a secure receptacle (for central count systems)
d. Protect the secrecy of the vote throughout the process

In addition to the above requirements, all paper-based precinct count systems **shall**:

e. Provide feedback to the voter that identifies specific contests for which he or she has made no selection or fewer than the allowable number of selections (e.g., undervotes)
f. Notify the voter if he or she has made more than the allowable number of selections for any contest (e.g., overvotes)
g. Notify the voter before the ballot is cast and counted of the effect of making more than the allowable number of selections for a contest
h. Provide the voter opportunity to correct the ballot for either an undervote or overvote before the ballot is cast and counted

2.3.3.3 DRE and EBM System Requirements

In addition to the above common requirements, DRE and EBM systems **shall**:

a. Prohibit the voter from accessing or viewing any information on the display screen that has not been authorized by election officials and preprogrammed into the voting system (i.e., no potential for display of external information or linking to other information sources)
b. Enable the voter to easily identify the selection button or switch, or the active area of the ballot display, that is associated with each candidate or ballot measure response
c. Allow the voter to select his or her preferences on the ballot in any legal number and combination
d. Indicate that a selection has been made or canceled
e. Indicate to the voter when no selection, or an insufficient number of selections, has been made for a contest (e.g., undervotes)
f. Notify the voter if he or she has made more than the allowable number of selections for any contest (e.g., overvotes)
g. Notify the voter before the ballot is cast or printed of the effect of making more than the allowable number of selections for a contest
h. Provide the voter opportunity to correct the ballot for either an undervote or overvote before the ballot is cast or printed
i. Notify the voter when the selection of candidates and measures is completed
j. Allow the voter, before the ballot is cast or printed, to review his or her choices and, if the voter desires, to delete or change his or her choices before the ballot is cast or printed
k. Prompt the voter to confirm the voter's choices before casting or printing his or her ballot
l. Provide sufficient computational performance to provide responses back to each voter entry in no more than three seconds
m. Ensure that the votes stored or printed accurately represent the actual votes cast
n. Protect the secrecy of the vote throughout the voting process

In addition, DREs **shall**:

o. Signify to the voter that casting the ballot is irrevocable and direct the voter to confirm the voter’s intention to cast the ballot before it is cast
p. Notify the voter after the vote has been stored successfully that the ballot has been cast
q. Notify the voter that the ballot has not been cast successfully if it is not stored successfully, including storage of the ballot image, and provide clear instruction as to the steps the voter should take to cast his or her ballot should this event occur
r. Prevent modification of the voter’s vote after the ballot is cast
s. Provide a capability to retrieve ballot images in a form readable by humans [in accordance with the requirements of Subsections 2.1.2 (f) and 2.1.4 (k) and (l)]
t. Increment the proper ballot position registers or counters
u. Prohibit access to voted ballots until after the close of polls
v. Provide the ability for election officials to submit test ballots for use in verifying the end-to-end integrity of the voting system
w. Isolate test ballots such that they are accounted for accurately in vote counts and are not reflected in official vote counts for specific candidates or measures

2.4 Post-Voting Capabilities

All voting systems **shall** provide capabilities to accumulate and report results for the jurisdiction and to generate audit trails. In addition, precinct count voting systems must provide a means to close the polls including generating appropriate reports. If the system provides the capability to broadcast results, additional standards apply.

2.4.1 Closing the Polls

These requirements for closing the polls and locking voting systems against future voting are specific to precinct count systems. The voting system **shall** provide the means for:

a. Preventing the further casting of ballots once the polls have closed
b. Providing an internal test that verifies that the prescribed closing procedure has been followed, and that the device status is normal
c. Incorporating a visible indication of system status
d. Producing a diagnostic test record that verifies the sequence of events, and indicates that the extraction of voting data has been activated
e. Precluding the unauthorized reopening of the polls once the poll closing has been completed for that election

2.4.2 Consolidating Vote Data

All systems **shall** provide a means to consolidate vote data from all polling places, and optionally from other sources such as absentee ballots, provisional ballots, and voted ballots requiring human review (e.g., write-in votes).

2.4.3 Producing Reports

All systems **shall** be able to create reports summarizing the vote data on multiple levels.

All systems **shall** provide capabilities to:

a. Support geographic reporting, which requires the reporting of all results for each contest at the precinct level and additional jurisdictional levels
b. Produce a printed report of the number of ballots counted by each tabulator
c. Produce a printed report for each tabulator of the results of each contest that includes the votes cast for each selection, the count of undervotes, and the count of overvotes
d. Produce a consolidated printed report of the results for each contest of all votes cast (including the count of ballots from other sources supported by the system as specified by the manufacturer) that includes the votes cast for each selection, the count of undervotes, and the count of overvotes

e. Be capable of producing a consolidated printed report of the combination of overvotes for any contest that is selected by an authorized official (e.g., the number of overvotes in a given contest combining candidate A and candidate B, combining candidate A and candidate C, etc.)
f. Produce all system audit information required in Subsection 5.4 in the form of printed reports, or in electronic memory for printing centrally
g. Prevent data from being altered or destroyed by report generation, or by the transmission of results over telecommunications lines

*For all systems, there **shall** be a complete accounting of undervotes for N of M contests as well as races involving only one voting choice*[3]*. In a "vote for N" contest, where L votes are recorded and L<N, the undervotes = N−L. In a "vote for 3" contest, votes would be recorded as follows:*

- *A vote for no candidates = 3 undervotes.*
- *A vote for 1 candidate = 2 undervotes.*
- *A vote for 2 candidates = 1 undervote.*

In addition, all precinct count voting systems **shall**:

h. Prevent the printing of reports and the unauthorized extraction of data prior to the official close of the polls
i. Provide a means to extract information from a transportable programmable memory device or data storage medium for vote consolidation
j. Consolidate the data contained in each unit into a single report for the polling place when more than one voting machine or precinct tabulator is used
k. Prevent data in transportable memory from being altered or destroyed by report generation, or by the transmission of official results over telecommunications lines

2.4.4 Electronic Reports

Electronic reports for voting systems are used to support audits. Typically, the electronic reports needed include: vote counts, counts of ballots recorded, information that identifies the electronic record, event logs and other records of important events or details of how the election was run on this device, and election archive information. The following requirements specify what information needs to be captured in electronic reports used to support voting system audits and how to protect the electronic reports from modification and verify their source and authenticity.

3 The italicized text in Section 2.4.3 is based on EAC Decision on Request for Interpretation 2007-06, http://www.eac.gov/assets/1/Page/EAC%20Decision%20on%20Battery%20Backup%20for%20Central%20Count.pdf.

2.4.4.1 Voting system Electronic Reports

The following requirements apply to electronic reports produced by the voting system for any exchange of information between devices, support of auditing procedures, or reporting of final results.

The voting system **shall** provide the capability to export electronic reports to files formatted in a non-restrictive, publicly-available format. Manufacturers **shall** provide a specification describing how they have implemented the format with respect to the manufacturer's specific voting devices and data, including such items as descriptions of elements, attributes, constraints, extensions, syntax and semantics of the format, and definitions for data fields and schemas.

The voting system **shall** provide the ability to produce printed forms of electronic reports. The printed forms of the electronic reports **shall** retain all required information as specified for each report type other than digital signatures. The printing of the electronic reports MAY be done from a different component of the voting system that produced the electronic report. It **shall** be possible to print electronic reports produced by the central tabulator or EMS on a different device.

Voting systems **shall** digitally sign electronic reports using NIST approved algorithms with a security strength of at least 112 bits implemented within a FIPS 140-2 level 1 or higher validated cryptographic module operating in FIPS mode.

2.4.4.2 Tabulator electronic reports

The following requirements apply to electronic reports produced by tabulators, such as DREs and optical scanners, for exchange of information between devices, transmission of results to the EMS, support of auditing procedures, or reporting of intermediate election results.

Each tabulator **shall** produce a Tabulator Summary Count report including the following information:

a. Identifier of the tabulator;
b. Time and date of summary record;
c. The following, both in total and broken down by ballot style and precinct:
    i. Number of read ballots;
    ii. Number of counted ballots;
    iii. Number of rejected electronic CVRs; and
    iv. For each N-of-M (including 1-of-M) or cumulative voting contest appearing in any ballot style handled by the tabulator:
        - Number of counted ballots that included that contest;
        - Vote totals for each non-write-in contest choice;
        - Number of write-in votes;
        - Number of overvotes; and
        - Number of undervotes.

v. When ballots span more than one piece of media (such as paper sheets for optical scanners), number of read media.

In producing the Tabulator Summary Count report, the tabulator **shall** assume that no provisional or challenged ballots are accepted.

The tabulator **shall**:

a. Transmit the summary count report to the EMS with the other electronic reports;
b. Store the summary count report in the election archive, if available; and
c. Store the summary count report in the voting systems event log.

Tabulators should produce a report of ballot images that includes:

a. Time and date of creation of complete ballot image report; and
b. Ballot images recorded in randomized order by the DRE for the election. NIST Special Publication 800-90: Recommendation for Random Number Generation Using Deterministic Random Bit Generators specifies techniques for the generation of random numbers that can be used to randomize the order of ballot images in a cryptographically sound way. For each voted ballot, this includes:
    i. Ballot style and reporting context;
    ii. For each contest:
        - The choice recorded, including undervotes and write-ins; and
        - Any information collected electronically about each write-in;
    iii. Information specifying whether the ballot is provisional, type of provisional ballot, and providing a unique identifier for the ballot. Types of provisional ballots (such as "regular provisional", "extended hours provisional", and "regular extended hours") are jurisdiction-dependent.

DREs **shall** produce a report of ballot images that includes:

a. Time and date at poll closing; and
b. Ballot images recorded in randomized order by the DRE for the election. NIST Special Publication 800-90: Recommendation for Random Number Generation Using Deterministic Random Bit Generators specifies techniques for the generation of random numbers that can be used to randomize the order of ballot images in a cryptographically sound way. For each voted ballot, this includes:
    i. Ballot style and reporting context;
    ii. For each contest:
        - The choice recorded, including undervotes and write-ins; and
        - Any information collected electronically about each write-in;
    iii. Information specifying whether the ballot is provisional, type of provisional ballot, and providing a unique identifier for the ballot. Types of provisional ballots (such as "regular provisional", "extended hours provisional", and "regular extended hours") are jurisdiction-dependent.

Tabulators that produce the collection of ballot images report **shall**:

a. Transmit the collection of ballot images report to the EMS with the other electronic reports;
b. Store the collection of ballot images report in the election archive, if available; and
c. Store the collection of ballot images report in the voting systems event log.

The tabulator **shall** digitally sign the event log, transmit the signed event log to an EMS, and retain a record of the transmission. The tabulator digital signature **shall** be generated using a NIST approved algorithm with a security strength of at least 112 bits implemented within a FIPS 140-2 level 1 or higher validated cryptographic module operating in FIPS mode.

2.4.4.3 EMS electronic reports

The following requirements apply to the reports produced by an EMS. EMSs include both DREs used as accumulators in the polling place, called a Precinct EMS, as well as EMSs used as jurisdiction-wide accumulators. All of the requirements for tabulators apply to EMSs. This section addresses additional requirements based on an EMSs role as an accumulator of ballot counts and vote totals.

Each EMS **shall** produce a Tabulator Summary Count report including the following information:

a. Identifiers for each tabulator contained in the summary;
b. For tabulators with public keys:
    i. The public key for each tabulator in the summary and
    ii. Signed tabulator summary count report.
c. Summary ballot counts and vote totals by tabulator, precinct, and polling place.
    i. Precinct totals include subtotals from each tabulator used in the precinct.

The EMS **shall** be capable of combining tabulator reports to protect voter privacy.

The EMS **shall** produce a report for each precinct including:

a. Each tabulator included in the precinct with its identifier;
b. Number of read ballots;
c. Number of counted ballots; and
d. For each N-of-M (including 1-of-M) or cumulative voting contest appearing in any ballot style handled by the tabulator:
    i. Number of counted ballots that included that contest;
    ii. Vote totals for each non-write-in contest choice; and
    iii. Number of write-in votes

The EMS **shall** produce a report showing the changes made to each contest based on the resolution of provisional ballots, challenged ballots, write-in choices, and the date and time of the report.

For each tabulator producing electronic reports, the EMS **shall** verify the digital signature on the report is correct using the public key associated with the tabulator.

2.4.5 Election Night Reporting

Some voting systems offer the capability to make unofficial results available to external organizations such as the news media, political party officials, and others. Although this capability is not required, systems that make unofficial results available **shall**:

a. Provide only aggregated results, and not data from individual ballots
b. Provide no access path from unofficial electronic reports or files to the storage devices for official data
c. Clearly indicate on each report or file that the results it contains are unofficial

2.5 Maintenance, Transportation, and Storage

All systems **shall** be designed and manufactured to facilitate preventive and corrective maintenance, conforming to the hardware standards described in Subsection 4.1. All vote casting and tally equipment designated for storage between elections **shall**:

a. Function without degradation in capabilities after transit to and from the place of use, as demonstrated by meeting the performance standards described in Subsection 4.1
b. Function without degradation in capabilities after storage between elections, as demonstrated by meeting the performance standards described in Subsection 4.1

3 Usability and Accessibility Requirements

Table of Contents

3 Usability, Accessibility, and Privacy Requirements

3.1 Overview

The importance of usability and accessibility in the design of voting systems has become increasingly apparent. It is not sufficient that the internal operation of these systems be correct; in addition, voters and poll workers must be able to use them effectively. There are some particular considerations for the design of usable and accessible voting systems:

- The voting task itself can be fairly complex; the voter may have to navigate an electronic ballot, choose multiple candidates in a single contest, or decide on abstrusely worded referenda
- Voting is performed infrequently, so there is limited opportunity for voters and poll workers to gain familiarity with the process
- Jurisdictions may change voting equipment, thus obviating whatever familiarity the voter might have acquired
- Usability and accessibility requirements include a broad range of factors, including physical abilities, language skills, and technology experience

3.1.1 Purpose

The challenge, then, is to provide a voting system that voters can use comfortably, efficiently, and with confidence that they have cast their votes correctly. The requirements within this section are intended to serve that goal. Three broad principles motivate this section:

a. All eligible voters **shall** have access to the voting process without discrimination.

The voting process **shall** be accessible to individuals with disabilities. The voting process includes access to the polling place, instructions on how to vote, initiating the voting session, making ballot selections, review of the ballot, final submission of the ballot, and getting help when needed.

b. Each cast ballot **shall** accurately capture the selections made by the voter.

The ballot **shall** be presented to the voter in a manner that is clear and usable. Voters should encounter no difficulty or confusion regarding the process for recording their selections.

c. The voting process **shall** preserve the secrecy of the ballot.

The voting process **shall** preclude anyone else from determining the content of a voter's ballot without the voter's cooperation. If such a determination is made against the wishes of the voter, then his or her privacy has been violated.

All the requirements in this section have the purpose of improving the quality of interaction between voters and voting systems.

Note that these principles refer to the entire voting process. The VVSG applies only to voting systems; other aspects of the process (such as administrative rules and procedures) are outside the scope of the VVSG, but are nonetheless crucial for the full achievement of the principles.

3.1.2 Special terminology

The following terms are used frequently in this chapter; they are defined in Appendix A of Volume 1:

- Accessible Voting Station (Acc-VS)
- Alert time
- Audio-Tactile Interface (ATI)
- Common Industry Format (CIF)
- Completed system response time
- Direct Record Electronic (DRE)
- Electronically-assisted Ballot Marker (EBM)
- Initial system response time
- Precinct Count Optical Scanner (PCOS)
- Precinct Tabulator
- Summative Usability Testing
- Voter inactivity time

3.1.3 Interaction of usability and accessibility requirements

All the requirements in Section 3 have the purpose of improving the quality of interaction between voters and voting systems. Please note how Sections 3.2 and 3.3 work together:

- The requirements for general usability in Section 3.2 apply to ALL voting systems, including the Acc-VS. They cover the features that are applicable both to the general population and to voters with disabilities. In particular, note that both DREs and EBMs are classified as Acc-VS. Requirements for any alternative languages required by state or federal law are also included under Section 3.2.
- The requirements for accessibility in Section 3.3 cover only those features that are mandatory for the Acc-VS in addition to the general usability requirements. For instance, an audio tactile interface would be of interest mainly to those with vision or other reading disabilities, but not to those who can use a visual interface. Therefore, to determine what usability features are required of the Acc-VS, one must examine both Sections 3.2 and 3.3. *The features of the Acc-VS may also*

assist those not usually described as having a disability, e.g., voters with poor reading vision or somewhat limited dexterity[4].

3.2 General usability requirements

The voting process **shall** provide a high level of usability for voters. Accordingly, voters **shall** be able to negotiate the process effectively, efficiently, and comfortably. The goal is that the resulting ballot accurately reflects the intention of the voter. The mandatory voting system standards mandated in HAVA Section 301 relate to the interaction between the voter and the voting system:

---

a. Requirements.--Each voting system used in an election for federal office shall meet the following requirements:

1. In general.--

A. Except as provided in subparagraph (B), the voting system (including any lever voting system, optical scanning voting system, or direct recording electronic system) shall--

i. Permit the voter to verify (in a private and independent manner) the votes selected by the voter on the ballot before the ballot is cast and counted;

ii. Provide the voter with the opportunity (in a private and independent manner) to change the ballot or correct any error before the ballot is cast and counted (including the opportunity to correct the error through the issuance of a replacement ballot if the voter was otherwise unable to change the ballot or correct any error); and

iii. If the voter selects votes for more than one candidate for a single office -

I. Notify the voter that the voter has selected more than one candidate for a single office on the ballot;

II. Notify the voter before the ballot is cast and counted of the effect of casting multiple votes for the office; and

III. Provide the voter with the opportunity to correct the ballot before the ballot is cast and counted.

4 The italicized text in Section 3.1.3 is based on EAC Decision on Request for Interpretation 2007-01, http://www.eac.gov/assets/1/Page/EAC%20Decision%20on%20Accessible%20Design.pdf.

> B. A state or jurisdiction that uses a paper ballot voting system, a punch card voting system, or a central count voting system (including mail-in absentee ballots and mail-in ballots), may meet the requirements of subparagraph (A)(iii) by -
>
> > i. Establishing a voter education program specific to that voting system that notifies each voter of the effect of casting multiple votes for an office; and
> >
> > ii. Providing the voter with instructions on how to correct the ballot before it is cast and counted (including instructions on how to correct the error through the issuance of a replacement ballot if the voter was otherwise unable to change the ballot or correct any error).
>
> C. The voting system shall ensure that any notification required under this paragraph preserves the privacy of the voter and the confidentiality of the ballot.

The requirements of this section are intended to support these basic usability standards of HAVA.

3.2.1 General usability

The voting system **shall** support voters in the task of effectively completing their ballots. The features of the voting system **shall** not contribute to the commission of voter error within the voting session.

a. The vendor **shall** submit a report of their summative usability tests on the voting system using individuals who are representative of the general population.
b. The report **shall** be submitted in the Common Industry Format.
c. The report **shall** contain the results of the summative usability tests.

Discussion: Voting system developers are required to conduct realistic usability tests on their product before submitting the system to conformance testing. This is to encourage early detection and resolution of usability problems. *The manufacturer must submit the usability test report to the VSTL as part of their TDP. The VSTL will then check the technical data package to ensure that the report is present and reported in the Common Industry Format and contains the results from a summative usability test*[5].

3.2.2 Functional capabilities

The usability of the voting process is enhanced by the presence of certain functional capabilities. These capabilities differ somewhat depending on whether or not the system presents an editable interface within which voters can easily change their votes (typically an electronic screen) or an interface in which voters must obtain a new ballot to make changes (typically a manually-marked paper ballot).

a. If the voter selects more than the allowable number of choices within a contest, the voting system **shall** notify the voter of the effect of this action before the ballot is cast and counted.

Discussion: In the case of manual systems, this may be achieved through appropriately placed instructions. This requirement has no force for electronic ballot interfaces, since they prevent overvoting in the first place.

b. The voting system **shall** allow the voter, at the voter's choice, to submit an undervoted ballot without correction.
c. The voting system **shall** provide the voter the opportunity to correct the ballot for either an undervote or overvote before the ballot is cast and counted.

Discussion: In the case of manual systems, this may be achieved through appropriately placed written instructions. Some corrections may require the voter to obtain a new paper ballot from a poll worker. Also, note the requirements on precinct-count optical scanners in Section 3.2.2.2 below.

d. If and only if the voter successfully casts or prints the ballot, then the electronic ballot interface or PCOS system **shall** so notify the voter.

5 The italicized text in Section 3.2.1 is based on EAC Decision on a Request for Interpretation 2007-03, http://www.eac.gov/assets/1/Page/EAC%20Decision%20on%20Summative%20Usability%20Testing.pdf.

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.

3.2.2.1 Editable electronic ballot interfaces

Voting systems such as DREs and EBMs present voters with an editable interface, allowing them to easily change their votes prior to final casting of the ballot.

a. The electronic ballot interface **shall** prevent voters from selecting more than the allowable number of choices for each contest.

Discussion: This requirement does not specify exactly how the system must respond when a voter attempts to select an "extra" candidate. For instance, the system may prevent the selection and issue a warning, or, in the case of a single-choice contest, simply change the vote.

b. The electronic ballot interface **shall** provide feedback to the voter, before final casting or printing of the ballot, that identifies specific contests for which the voter has selected fewer than the allowable number of choices (i.e., undervotes).

Discussion: For electronic ballot interface systems, no allowance is made for disabling this feature. Also, see the plain language requirement below on clarity of warnings 3.2.4c.i.

c. The electronic ballot interface **shall** provide the voter the opportunity to correct the ballot before it is cast or printed. This correction process **shall** not require external assistance. The corrections to be supported include modifying an undervote and changing a vote from one candidate to another.
d. The electronic ballot interface **shall** allow the voter to change a vote within a contest before advancing to the next contest.

Discussion: The point here is that voters using an editable interface should not have to wait for a final ballot review screen in order to change a vote.

e. The electronic ballot interface **shall** provide navigation controls that allow the voter to advance to the next contest or go back to the previous contest before completing a vote on the contest(s) currently being presented (whether visually or aurally).

Discussion: For example, voters should not be forced to proceed sequentially through all the contests before going back to check their votes within a previous contest.

f. If the voter takes the appropriate action to cast a ballot, but the DRE does not accept and record it successfully, including failure to store the ballot image, then the DRE **shall** so notify the voter and provide clear instruction as to the steps the voter should take to cast the ballot.

> Discussion: If a DRE fails at the point of casting a ballot, it must clearly indicate to the voter and to election officials responding to the failure whether or not the ballot was cast. Otherwise, election officials may be unable to provide substantial confirmation that the vote was or was not counted, possibly resulting in disenfranchisement or the casting of more than one ballot by a single voter. A device that "freezes" when the voter attempts to cast the ballot, providing no evidence one way or the other whether the ballot was cast would violate this requirement.

g. If the electronic ballot interface 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 **shall** allow the voter to verify that record using the same access features used by the voter to vote the ballot.

> Discussion: While paper records generally provide a simple and effective means for technology-independent vote verification, their use can present difficulties for voters who use large font, high contrast, alternative languages, and other settings described in Section 3.2. The purpose of this requirement is to ensure that all voters have a similar opportunity for vote verification. Note that this requirement addresses the special difficulties that may arise with the use of paper. Verification is part of the voting process, and all the other general requirements apply to verification, in particular those dealing with dexterity (e.g. 3.3.4 c), blindness (e.g. 3.3.3 e) and poor vision issues (e.g. 3.2.5 g). 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. See also requirement 3.3.1.e.

3.2.2.2 Non-Editable ballot interfaces

Non-Editable interfaces, such as manually-marked paper ballots, do not have the same flexibility as do editable interfaces. Nonetheless, certain features are required, especially in the case of precinct-based optical scanners.

a. The PCOS system **shall** be capable of providing feedback to the voter that identifies specific contests for which the voter has made more than the allowable number of votes (i.e., overvotes).
b. The PCOS system **shall** be capable of providing feedback to the voter that identifies specific contests for which the voter has made fewer than the allowable number of votes (i.e., undervotes). The system **shall** provide a means for an

authorized election official to deactivate this capability entirely and by contest. However, if a ballot is submitted with all the contests on one side left blank, notification to the voter is performed as described in requirement 3.2.2.2 c

c. The PCOS system **shall** be capable of notifying the voter that he or she has submitted a paper ballot that is blank on one or both sides. The system **shall** provide a means for an authorized election official to deactivate this capability.

> Discussion: One purpose of this feature is to detect situations in which the voter might be unaware that the ballot is two-sided. This feature is distinct from the ability to detect and warn about undervoting.

d. If the PCOS system has notified the voter that a potential error condition (such as an overvote, undervote, or blank ballot) exists, the system **shall** then allow the voter to correct the ballot or to submit it as is.

> Discussion: This requirement mandates that the system be capable of allowing either correction or immediate submission. For instance, a questionable paper ballot might be physically ejected for possible correction. This requirement does not constrain the procedures that jurisdictions might adopt for handling such situations (e.g., whether poll worker intervention is required).

e. Paper-based precinct tabulators **shall** be able to identify a ballot containing marginal marks. When such a ballot is detected, the tabulator **shall**:

- Return the ballot to the voter;
- Provide feedback to the voter that identifies the specific contests for which a marginal mark was detected; and
- Allow the voter either to correct the ballot or to submit the ballot "as is" without correction.

> Discussion: Basically, a marginal mark is one that, according to the manufacturer specifications, is neither clearly countable as a vote nor clearly countable as a non-vote. The purpose of this requirement is to provide more certainty about the handling of poorly-marked ballots. If a given candidate or option is clearly marked as chosen, or left completely unmarked, then there is no ambiguity to resolve. However, each manufacturer should define a "gray area" (with respect to location, darkness, etc.) in which marks will be actively flagged as ambiguous.

f. Software used to format optical scan ballots **shall** constrain the size and contrast of all target areas to conform to the following requirements:
   i. The target **shall** be no less than 3 mm across in any direction
   ii. The contrast ratio between the target area boundaries and the surrounding space **shall** be no less than 10:1.

Discussion: For example, this applies to the oval or box outline delineating the target area, as well as the broken arrow designating the target area.

g. If the voter takes the appropriate action to cast a ballot, but the PCOS system does not accept and record it successfully, including failure to read the ballot or to transport it into the ballot box, the PCOS **shall** so notify the voter.

Discussion: This requirement means that PCOS systems must detect and report electrical and mechanical failures within the system itself. It does not require the detection of errors on the part of the voter.

3.2.3 Voter privacy

The voting process must preclude anyone else from determining the content of a voter's ballot without the voter's cooperation. Privacy ensures that the voter can cast votes based solely on his or her own preferences without intimidation or inhibition.

3.2.3.1 Privacy at the polls

a. The voting system **shall** prevent others from determining the contents of a ballot.

Discussion: The voting system itself provides no means by which others can "determine" how one has voted. Of course voters could simply tell someone else for whom they voted, but the system provides no evidence for such statements, and therefore voters cannot be coerced into providing such evidence. It is assumed that the system is deployed according to the installation instructions provided by the manufacturer. Whether the configuration of the voting system protects privacy may well depend on proper setup.

b. The voting system **shall** support ballot privacy during the voting session and ballot submission.

Discussion: This requirement may involve different approaches for electronic and paper interfaces. In both cases, appropriate shielding of the voting station is important. When a paper record with ballot information needs to be transported by the voter, devices such as privacy sleeves may 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.

c. During the voting session, the audio interface of the voting system **shall** be audible only to the voter.

Discussion: Voters who are hard of hearing but need to use an audio interface may also need to increase the volume of the audio. Such situations require headphones with low sound leakage.

d. The voting system **shall** issue all warnings in a way that preserves the privacy of the voter and the confidentiality of the ballot.

Discussion: HAVA 301 (a)(1)(C) mandates that the voting system must notify the voter of an attempted overvote in a way that preserves the privacy of the voter and the confidentiality of the ballot. This requirement generalizes that mandate.

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

3.2.3.2 No recording of alternative format usage

When voters use non-typical ballot interfaces, such as large print or alternative languages, their anonymity may be vulnerable. To the extent possible, only the logical contents of their ballots should be recorded, not the special formats in which they were rendered. However, in the case of paper ballots, where the interface is the record, some format information is unavoidably preserved.

a. No information **shall** be kept within an electronic cast voter record that identifies any alternative language feature(s) used by a voter.
b. No information **shall** be kept within an electronic cast voter record that identifies any accessibility feature(s) used by a voter.

3.2.4 Voter instructions, plain language, and information presentation

The features specified in this section are intended to minimize cognitive difficulties for voters. Voters should always be able to operate the voting system and understand the effect of their actions. Note that the "should" requirements in this section must be adhered to unless there is strong justification provided for making an exception.

a. The voting system **shall** provide instructions for all its valid operations.

Discussion: If an operation is available to the voter, it must be documented. Examples include how to change a vote, how to navigate among contests, how to cast a straight party vote, how to cast a write-in vote, and how to adjust display and audio characteristics.

b. The voting system **shall** provide a means for the voter to get help directly from the system at any time during the voting session.

> Discussion: The voter should always be able to get context-sensitive help from the system when needed. The purpose is to minimize the need for assistance from the poll worker. Electronic ballot interface systems may provide this with a distinctive "help" button. In addition to context-sensitive help, any voting system may provide written instructions that are separate from the ballot.

c. Instructional material for the voter **shall** conform to norms and best practices for plain language.

> Discussion: Although part of general usability, the use of plain language is also expected to assist voters with cognitive disabilities. 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. For specific guidance on how to implement this requirement, see: "Guidelines for Writing Clear Instructions and Messages for Voters and Poll Workers" at http://vote.nist.gov/032906PlainLanguageRpt.pdf.

i. Warnings and alerts issued by the voting system **shall** be distinguishable from other information and should clearly state:

- The nature of the problem;
- Whether the voter has performed or attempted an invalid operation or whether the voting system itself has malfunctioned in some way; and
- The set of responses available to the voter.

> 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 a poll worker.

ii. When an instruction is based on a condition, the condition should be stated first, and then the action to be performed.

> Discussion: For instance, use "In order to change your vote, do X", rather than "Do X, in order to change your vote."

iii. The voting system should use familiar, common words and avoid technical or specialized words that voters are not likely to understand.

Discussion: For instance, "... there are more contests on the other side ..." rather than "...additional contests are presented on the reverse ..."

iv. Each distinct instruction should be separated spatially from other instructions for visual or tactile interfaces, and temporally for auditory interfaces.

Discussion: This implies not "burying" several unrelated instructions in a single long paragraph.

v. The voting system should issue instructions on the correct way to perform actions, rather than telling voters what not to do.

Discussion: 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.”

vi. The system's instructions should address the voter directly rather than use passive voice constructions.

Discussion: For example, "remove and retain this ballot stub" rather than "this ballot stub must be removed and retained by the voter."

vii. The voting system should avoid the use of gender-based pronouns.

Discussion: For example, "...write in your choice directly on the ballot..." rather than "... write in his name directly on the ballot..."

d. Consistent with election law, the voting system **shall** support a process that does not introduce bias for or against any of the contest choices to be presented to the voter. In both visual and aural formats, the choices **shall** be presented in an equivalent manner.

Discussion: Certain differences in presentation are mandated by state law, such as the order in which candidates are listed and provisions for voting for write-in candidates. However, comparable characteristics such as font size or voice volume and speed must be the same for all choices.

e. The voting system **shall** provide the capability to design a ballot with a high level of clarity and comprehensibility.
   i. The voting system should not visually present a single contest spread over two pages or two columns.

> Discussion: Such a visual separation poses the risk that the voter may perceive one contest as two, or fail to see additional choices. If a contest has a large number of candidates, it may be infeasible to observe this guideline.

ii. The ballot **shall** clearly indicate the maximum number of candidates for which one can vote within a single contest.
iii. The relationship between the name of a candidate and the mechanism used to vote for that candidate **shall** be consistent throughout the ballot.

> Discussion: For example, the response field where voters indicate their votes must not be located to the left of some candidates' names, and to the right of others'.

iv. The voting system should present instructions near to where they are needed.

> Discussion: For instance, only general instructions should be grouped at the beginning of the ballot; those pertaining to specific situations should be presented where and when needed.

f. The use of color by the voting system **shall** agree with common conventions: (a) green, blue or white is used for general information or as a normal status indicator; (b) amber or yellow is used to indicate warnings or a marginal status; (c) red is used to indicate error conditions or a problem requiring immediate attention.
g. When an icon is used to convey information, indicate an action, or prompt a response, it **shall** be accompanied by a corresponding linguistic label.

> Discussion: While icons can be used for emphasis when communicating with the voter, they must not be the sole means by which information is conveyed, since there is no widely accepted "iconic" language and therefore not all voters may understand a given icon.

3.2.5 Visual display characteristics

The requirements of this section are designed to minimize perceptual difficulties for the voter. Some of these requirements are designed to assist voters with poor reading vision. These are voters who might have some difficulty in reading normal text, but are not typically classified as having a visual disability and thus might not be inclined to use the Acc-VS.

a. If the voting system uses an electronic display screen as the primary visual interface for the voter, the display **shall** have the following characteristics:

- Flicker frequency NOT between 2 Hz and 55 Hz.
- Minimum display brightness: 130 cd/m^2
- Minimum display darkroom 7×7 checkerboard contrast: 150:1
- Minimum display pixel pitch: 85 pixels/inch (0.3 mm/pixel)
- Minimum display area 700 cm^2
- Antiglare screen surface that shows no distinct virtual image of a light source
- Minimum uniform diffuse ambient contrast ratio for 500 lx illuminance: 10:1

Discussion: Aside from usability concerns, this requirement protects voters from having visually-induced seizures.

b. Any aspect of the voting system voter interface that is adjustable by either the voter or poll worker, including font size, color, contrast, audio volume, or rate of speech, **shall** automatically reset to a standard default value upon completion of that voter's session. For the Acc-VS with an electronic image display, the aspects include synchronized audio/video mode and non-manual input mode.

Discussion: This ensures that the voting system presents the same initial appearance to every voter.

c. If any aspect of a voting system is adjustable by either the voter or poll worker, there **shall** be a mechanism to allow the voter to reset all such aspects to their default values while preserving the current votes.

Discussion: The purpose is to allow a voter or poll worker who has adjusted the system into an undesirable state to reset all the aspects and begin again.

d. For all text intended for voters or poll workers, the voting system **shall** provide a font with the following characteristics

- Height of capital letters at least: 3.0 mm
- x-height of a least: 70% of cap height
- Stroke width at least: 0.35 mm.

e. A voting system that uses an electronic image display **shall** be capable of showing all information in at least two font sizes:

- 3.0-4.0 mm cap height, with a corresponding x-height at least 70% of the cap height and a minimum stroke width of 0.35 mm;
- 6.3-9.0 mm cap height, with a corresponding x-height at least 70% of the cap height and a minimum stroke width of 0.7 mm; under control of the voter. The system **shall** allow the voter to adjust font size throughout the voting session while preserving the current votes.

Discussion: While larger font sizes may assist most voters with poor vision, certain disabilities such as tunnel vision are best addressed by smaller font sizes. Larger font sizes may also assist voters with cognitive disabilities. This requirement mandates the availability of at least two font sizes, but additional choices (including continuous variability) are allowed.

f. Text intended for the voter should be presented in a sans serif font.

Discussion: In general, sans serif fonts are easier to read on-screen, they look reasonably good when their size is reduced, and they tend to retain their visual appeal across different platforms.

g. Voting systems using paper ballots or paper verification records **shall** provide features that assist in the reading of such ballots and records by voters with poor reading vision.

Discussion: While this requirement may be satisfied by one of its sub-requirements, other innovative solutions are not precluded.

i. The voting system may achieve legibility of paper records by supporting the printing of those records in at least two font sizes, 3.0-4.0mm and 6.3-9.0mm.

Discussion: Although the system may be capable of printing in several font sizes, the use of various font sizes in an actual election may be governed by local or state laws and regulations.

ii. The system may achieve legibility of paper records by supporting magnification of those records. This magnification may be done by optical or electronic devices. The manufacturer may either: 1) provide the magnifier itself as part of the system, or 2) provide the make and model number of readily available magnifiers that are compatible with the system.

Discussion: The magnifier(s) either provided or cited must, of course, provide legibility for the paper as actually presented on the system. For instance, if the paper record is under a transparent cover to prevent the voter from touching it, the means of magnification must be compatible with this configuration. "Straight edge" magnifiers, which allow the user to read an entire line, may be especially suitable for the voting task.

h. The default color coding **shall** support correct perception by voters and poll workers with color vision deficiencies.

Discussion: There are many types of color vision deficiencies or "color blindness" and no color coding can, by itself, guarantee correct perception for everyone. However, designers should take into account such factors as: red-green color blindness is the most common form; high luminosity contrast will help colorblind voters to recognize visual features; and color-coded graphics can also use shape to improve the ability to distinguish certain features. For specific guidance on how to implement this requirement, please see: "NISTIR 7537: Guidelines for Using Color in Voting Systems" at http://www.nist.gov/itl/vote/upload/NISTIR-7537.pdf

i. The default visual display for voters and poll workers of a voting station with an electronic display **shall** have a luminosity contrast ratio between the foreground text and background color of at least 10:1 for all elements that visually convey information such as text, controls, and infographics or icons. For paper ballots, the contrast ratio **shall** be at least 10:1 as measured based on ambient lighting of at least 300 lx.

Discussion: 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. Note that this is higher than the general web requirements of 4.5:1 in WCAG 2.0 Checkpoint 1.4.6 (Level AAA) to accommodate a wider range of visual disabilities. There are several free tools available to test color luminosity contrast, including http://juicystudio.com/services/luminositycontrastratio.php

ii. A voting station with an electronic display screen **shall** be capable of showing all elements that visually convey information, such as text, controls, and infographics or icons, in a high contrast mode either as an initial setting or under the control of the voter. If the system allows the voter to adjust contrast during the voting session it **shall** preserve the current votes. High contrast is a luminosity contrast ratio between the foreground text and background color of at least 20:1. The high contrast mode **shall** use at least one of the following color combinations:

- Black text on a white background
- White text on a black background
- Yellow text on a black background
- Light cyan text on a black background

Discussion: A high contrast mode ensures that there is an option for the visual presentation for people with color vision deficiencies or whose vision requires high contrast.

i. Color coding **shall** not be used as the sole means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.

Discussion: While color can be used for emphasis, some other non-color mode must also be used. 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 rule and a label to group elements on the ballot.

3.2.6 Voter-interface interaction

The requirements of this section are designed to minimize interaction difficulties for the voter.

a. The electronic ballot interface **shall** not require page scrolling by the voter.

Discussion: That is, the page of displayed information must fit completely within the physical screen presenting it. Scrolling is not an intuitive operation for those unfamiliar with the use of computers. Even those experienced with computers often do not notice a scroll bar and miss information at the bottom of the "page." Voting systems may require voters to move to the next or previous "page."

b. The voting system **shall** provide unambiguous feedback regarding the voter's selection, such as displaying a checkmark beside the selected option or conspicuously changing its appearance.
c. Voting system input mechanisms **shall** be designed to prevent accidental activation.

Discussion: There are at least two kinds of accidental activation. One is when a control is activated as it is being "explored" by the voter because the control is overly sensitive to the touch. A second issue is the problem of having a control in a location where it can easily be activated unintentionally. An example would be a button in the very bottom left corner of the screen where a voter might hold the unit for support.

i. On touch screens, the sensitive touch areas **shall** have a minimum height of 0.5 inches and minimum width of 0.7 inches. The vertical distance between the centers of adjacent areas **shall** be at least 0.6 inches, and the horizontal distance at least 0.8 inches. Touch areas **shall** not overlap.
ii. No key or control on a voting system **shall** have a repetitive effect as a result of being held in its 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.

3.2.6.1 Timing

These requirements address how long the system and voter wait for each other to interact.

a. The initial system response time of the electronic ballot interface **shall** be no greater than 0.5 seconds.

> 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 auditory and visual voting system responses.

b. When the voter performs an action to record a single vote, the completed system response time of the electronic ballot interface **shall** be no greater than one second in the case of a visual response, and no greater than five seconds in the case of an audio response.

> Discussion: 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".

c. The completed system response time during a voter interaction with the visual display of the electronic ballot interface **shall** be no greater than 10 seconds.

> Discussion: Even for "large" operations such as initializing the ballot or painting a new screen, the system must never take more than 10 seconds. In the case of audio systems, no upper limit is specified, since certain operations may take longer, depending on the length of the text being read (e.g., reading out a long list of candidates running in a contest).

d. If the electronic ballot interface has not completed its visual response within one second, it **shall** present to the voter, within 0.5 seconds of the voter's action, some indication that it is preparing its response.

> Discussion: 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).

e. The electronic ballot interface **shall** detect and warn about lengthy voter inactivity during a voting session. Each electronic ballot interface **shall** have a defined and documented voter inactivity time, and that time **shall** be between two and five minutes.

Discussion: Each type of system must have a given inactivity time that is consistent among and within all voting sessions. This ensures that all voters are treated equitably.

f. Upon expiration of the voter inactivity time, the electronic ballot interface **shall** issue an alert and provide a means by which the voter may receive additional time. The alert time **shall** be between 20 and 45 seconds. If the voter does not respond to the alert within the alert time, the electronic ballot interface **shall** go into an inactive state requiring poll worker intervention.

3.2.7 Alternative languages

HAVA Section 301 (a)(4) states that the voting system **shall** provide alternative language accessibility pursuant to the requirements of Section 203 of the Voting Rights Act of 1965 (42 U.S.C. 1973aa-1a). Ideally every voter would be able to vote independently and privately, regardless of language. As a practical matter, alternative language access is mandated under the Voting Rights Act of 1975, subject to certain thresholds (e.g., if the language group exceeds 5% of the voting age population). Thus, election officials must ensure that the voting system they deploy is capable of handling the languages meeting the legal threshold within their districts.

While the following requirements support this process, it should be noted that they are requirements only for voting systems to be certified. It is anticipated that jurisdictions will apply additional requirements appropriate for their particular circumstances for procurement and deployment.

a. The voting system **shall** be capable of presenting the ballot, contest choices, review screens, vote verification records, and voting instructions in any language declared by the manufacturer to be supported by the system.

Discussion: For example, if the manufacturer claims that a given system is capable of supporting Spanish and Chinese, then it must do so. Presentation of the ballot includes both visual and audio formats. Both written and unwritten languages are within the scope of this requirement [6].

i. The electronic ballot interface should allow the voter to select among the available languages throughout the voting session while preserving the current votes. When presenting a choice of languages to the voter, the electronic ballot interface **shall** use the native name of each language.

6 The italicized text in Section 3.2.7 is based on EAC Decision on Request for Interpretation 2007-04, http://www.eac.gov/assets/1/Page/EAC%20Decision%20on%20Presentation%20of%20Alternative%20Language.pdf. See also 2009-02, http://www.eac.gov/assets/1/Page/EAC Decision on Alternate Languages.pdf

Discussion: For instance, a voter may initially choose an English version of the ballot, but then wish to switch to another language in order to read a referendum question.

ii. Information presented to the voter in the typical case of English-literate voters (including instructions, warnings, messages, contest choices, and vote verification information) **shall** also be presented when an alternative language is being used, whether the language is written or an unwritten language presented aurally.

Discussion: Therefore, it may not be sufficient simply to present the ballot per se in the alternative language, especially in the case of electronic ballot interface systems. All the supporting information must also be available in the alternative language.

iii. Any records, including paper ballots and paper verification records, **shall** have the information required to support auditing by poll workers and others who can read only English.

Discussion: Even though the system must be easily available to voters without a command of English, any persistent records of the vote must also be fully available to English-only readers for auditing purposes. In the case of paper, this does not imply a fully bi-lingual ballot. For instance, the full text of a referendum question might appear only in the alternative language, but the content of the vote (e.g., "yes" on ballot question 106) needs to be readable by English-only readers.

iv. The manufacturer **shall** conduct summative usability tests for each of the voting system's supported languages, using subjects who are fluent in those languages but not fluent in English and **shall** report the test results, using the Common Industry Format, as part of the TDP. In addition, the usability test report **shall** be submitted to the EAC as part of the documentation manufacturers are required to file with the application to test a voting system.

3.2.8 Usability for poll workers

Voting systems are used not only by voters to record their votes, but also by poll workers who are responsible for set-up, operation while polls are open, light maintenance, and poll closing. Because of the wide variety of implementations, it is impossible to specify detailed design requirements for these functions. The requirements below describe general capabilities that all systems must support.

a. Messages generated by the voting system for poll workers in support of the operation, maintenance, or safety of the system **shall** adhere to the requirements for clarity in Section 3.2.4 “Cognitive issues”.

3.2.8.1 Operation

Poll workers are responsible for opening polls, keeping the polls open and running smoothly during voting hours, and closing the polls afterwards. Operations may be categorized in three phases:

Setup includes all the steps necessary to take the system from its state as normally delivered to the polling place, to the state in which it is ready to record votes. It does not include ballot definition.

Polling includes such functions as:

- voter identification and authorization;
- preparing the system for the next voter;
- assistance to voters who wish to change their ballots or need other help;
- system recovery in the case of voters who abandon the voting session without having cast a ballot; and routine hardware operations, such as installing a new roll of paper.

Shutdown includes all the steps necessary to take the system from the state in which it is ready to record votes to its normal completed state in which it has captured all the votes cast and the voting information cannot be further altered.

a. Voting system setup, polling, and shutdown, as documented by the manufacturer, **shall** be reasonably easy for the typical poll worker to learn, understand, and perform.

> Discussion: This requirement covers procedures and operations for those aspects of system operation normally performed by poll workers and other "non-expert" operators. It does not address inherently complex operations such as ballot definition or system repair. While a certain amount of complexity is unavoidable, these "normal" procedures should not require any special expertise. The procedures may require a reasonable amount of training.

b. The manufacturer **shall** conduct summative usability tests on the voting system using individuals who are representative of the general population and **shall** report the test results, using the Common Industry Format, as part of the TDP. The tasks to be covered in the test **shall** include setup, operation, and shutdown. In addition, the usability test report **shall** be submitted to the EAC as part of the documentation manufacturers are required to file with the application to test a voting system.

c. The voting system **shall** include clear, complete, and detailed instructions and messages for setup, polling, and shutdown.

> Discussion: This requirement covers documentation for those aspects of system operation normally performed by poll workers and other "non-expert" operators. It does not address inherently complex operations such as ballot definition. The instructions would usually be in the form of a written manual, but could 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 poll worker as he or she attempts to perform a setup, polling, or shutdown operation. For specific guidance on how to implement this requirement, please see: "NISTIR 7519: Style Guide for Voting System Documentation" at http://www.nist.gov/itl/vote/upload/NISTIR-7519.pdf.

i. The documentation required for normal voting system operation **shall** be presented at a level appropriate for poll workers who are not experts in voting system and computer technology.

> Discussion: For instance, the documentation should not presuppose familiarity with personal computers.

ii. The documentation **shall** be in a format suitable for use in the polling place.

> Discussion: For instance, 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.

iii. The instructions and messages **shall** enable the poll worker to verify that the voting system

- Has been set up correctly (setup);
- Is in correct working order to record votes (polling); and
- Has been shut down correctly (shutdown).

> Discussion: The poll worker should not have to guess whether an operation has been performed correctly. The documentation should make it clear what the system "looks like" when correctly configured.

3.2.8.2 Safety

All voting systems and their components must be designed so as to eliminate hazards to personnel or to the equipment itself. Hazards include, but are not limited to:

- fire hazards;
- electrical hazards;
- potential for equipment tip-over (stability);
- potential for cuts and scrapes (e.g., sharp edges);
- potential for pinching (e.g., tight, spring-loaded closures); and
- potential for hair or clothing entanglement.

a. Devices associated with the voting system **shall** be certified in accordance with the requirements of UL 60950-1, Information Technology Equipment – Safety – Part 1 by a certification organization accredited by the Department of Labor, Occupational Safety and Health Administration's Nationally Recognized Testing Laboratory program. The certification organization's scope of accreditation **shall** include IEC/UL 60950-1.

Discussion: IEC/UL 60950 is a comprehensive standard for IT equipment and addresses all the hazards discussed above under Safety.

3.3 Accessibility requirements

HAVA Section 301 (a) (3) [HAVA02] reads, in part:

ACCESSIBILITY FOR INDIVIDUALS WITH DISABILITIES.--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;

(B) satisfy the requirement of subparagraph (A) through the use of at least one direct recording electronic voting system or other voting system equipped for individuals with disabilities at each polling place;

The voting process is to be accessible to voters with disabilities through the use of a specially equipped voting station. A machine so equipped is referred to herein as an accessible voting station (Acc-VS).

The requirements in this section are intended to address this HAVA mandate. Ideally, every voter would be able to vote independently and privately. As a practical matter, there may be some number of voters who, because of the nature of their disabilities, will need personal assistance with any system. Nonetheless, these requirements are meant to make the voting system independently accessible to as many voters as possible. This includes access across all voting processes: capabilities to generate, verify and cast an official ballot must be provided.

This section is organized according to system features that accommodate a variety of disabilities. A feature intended primarily to address a specific disability may very well assist voters with other types of disabilities. Moreover, this organization in no way implies that the various sets of requirements are optional or mutually exclusive. In order to conform, an Acc-VS must fulfill all the requirements of all the sub-sections of Chapter 3.3.

There are many other requirements, such as the general usability requirements, that apply to the Acc-VS besides those in this section. Please see Section 3.1.3 "Interaction of usability and accessibility requirements" for a full explanation.

3.3.1 General accessibility

The requirements[7] of this section are relevant to a wide variety of disabilities.

a. The Acc-VS **shall** be integrated into the manufacturer's complete voting system so as to support accessibility for disabled voters throughout the voting session.

> Discussion: This requirement ensures accessibility to the voter throughout the entire session. Not only must individual system components (such as ballot markers, paper records, and optical scanners) be accessible, but also they must work together to support this result.

   i. The manufacturer **shall** supply documentation describing 1) recommended procedures that fully implement accessibility for voters with disabilities and 2) how the Acc-VS 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.

b. When the provision of accessibility for the Acc-VS involves an alternative format for ballot presentation, then all information presented to non-disabled voters, including instructions, warnings, error and other messages, and contest choices, **shall** be presented in that alternative format.
c. The support provided to voters with disabilities **shall** be intrinsic to the Acc-VS. It **shall** not be necessary for the Acc-VS to be connected to any personal assistive device of the voter in order for the voter to operate it correctly. This does not apply to personal assistive technology required to comply with 3.3.4 b.

7 For additional clarification, see EAC Decision on Request for Interpretation 2010-06, http://www.eac.gov/assets/1/AssetManager/RFI 2010-06.Applying_Accessbility_requirements_to_BMD.FINAL.pdf

Discussion: This requirement does not preclude the Acc-VS from providing interfaces to assistive technology. (See definition of "personal assistive devices" in Appendix A.) Its purpose is to assure that disabled voters are not required to bring special devices with them in order to vote successfully. The requirement does not assert that the Acc-VS will eliminate the need for a voter's ordinary non-interfacing devices, such as eyeglasses or canes.

d. If a voting system provides for voter identification or authentication by using biometric measures that require a voter to possess particular biological characteristics, then the Acc-VS **shall** provide a secondary means that does not depend on those characteristics.

Discussion: For example, if fingerprints are used for voter identification, another mechanism must be provided for voters without usable fingerprints.

e. If the Acc-VS 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 **shall** allow the voter to verify that record using the same access features used by the voter to vote the ballot.

Discussion: While paper records generally provide a simple and effective means for technology-independent vote verification, their use can present difficulties for voters with certain types of disabilities. The purpose of this requirement is to ensure that all voters have a similar opportunity for vote verification.[8] Note that this requirement addresses the special difficulties that may arise with the use of paper. Verification is part of the voting process, and all the other general requirements apply to verification, in particular those dealing with dexterity (e.g. 3.3.4 c), blindness (e.g. 3.3.3 e) and poor vision issues (e.g. 3.2.5 g). 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. See also requirement 3.2.2.1.g.

3.3.2 Enhanced visual interfaces

These requirements specify the features of the Acc-VS designed to make the visual interface easier to see, in particular for voters with vision deficiencies, and synchronized with audio for voters with various language, reading, or some cognitive disabilities.

8 For additional clarification, see EAC Decision on Request for Interpretation 2009-01, http://www.eac.gov/assets/1/Page/EAC Decision on VVPAT Accessibility.pdf

In general, low vision is defined as having a visual acuity worse than 20/70. Low (or partial) vision also includes dimness of vision, haziness, film over the eye, foggy vision, extreme near-sightedness or far-sightedness, distortion of vision, color distortion or blindness, visual field defects, spots before the eyes, tunnel vision, lack of peripheral vision, abnormal sensitivity to light or glare and night blindness.

People with tunnel vision can see only a small part of the ballot at one time. For these users it is helpful to have letters at the lower end of the font size range in order to allow them to see more letters at the same time. Thus, there is a need to provide font sizes at both ends of the range.

People with low vision or color blindness benefit from high contrast and from a selection of color combinations appropriate for their needs. Between 7% and 10% of all men have color vision deficiencies. Certain color combinations in particular cause problems. Therefore, use of color combinations with good contrast is required. Note also the general Requirement 3.2.5 j.

However, some users are very sensitive to very bright displays and cannot use them for long. An overly bright background causes a visual white-out that makes these users unable to distinguish individual letters. Thus, use of non-saturated color options is an advantage for some people.

It is important to note that some of the requirements in 3.2.5 “Visual display characteristics” also provide support for voters with certain kinds of vision problems.

a. The manufacturer **shall** conduct summative usability tests on the Acc-VS using individuals with low vision and **shall** report the test results, using the Common Industry Format, as part of the TDP. In addition, the usability test report **shall** be submitted to the EAC as part of the documentation manufacturers are required to file with the application to test a voting system.
b. An Acc-VS with a color electronic image display **shall** allow the voter to adjust the color saturation throughout the voting session while preserving the current votes. Two options **shall** be available: 1) black text on white background and 2) white text on black background.
c. Groups of buttons and controls which perform different functions on the Acc-VS **shall** be distinguishable by both shape and color. This applies to buttons and controls implemented either "on-screen" or in hardware. This requirement does not apply to sizeable groups of keys in wide use by individuals with disabilities, such as a full alphabetic keyboard.

Discussion: The redundant cues assist those with low vision. They also help individuals who may have difficulty reading the text on the screen, those who are blind but have some residual vision, and those who use the controls on an Acc-VS because of limited dexterity. While this requirement is primarily focused on those with low vision, a feature intended primarily to address one kind of disability may very well assist voters with other kinds[9]. The TRACE Center's EZ Access design is an example of button functions distinguishable by both shape and color: http://trace.wisc.edu/ez/

d. If the Acc-VS has an electronic image display, the Acc-VS **shall** provide synchronized audio output to convey the same information as that which is displayed on the screen There **shall** be a means by which the voter can disable either the audio or the video output, resulting in a video-only or audio-only presentation, respectively. The system **shall** allow the voter to switch among the three modes (synchronized audio/video, video-only, or audio-only) throughout the voting session while preserving the current votes.

Discussion: This feature may also assist voters with cognitive disabilities.

3.3.3 Audio-tactile interfaces

These requirements specify the features of the Acc-VS designed to not only assist voters who are blind, but also those voters who would benefit from an auditory, rather than a purely visual, interface.

a. The manufacturer **shall** conduct summative usability tests on the Acc-VS using individuals who are blind and **shall** report the test results, using the Common Industry Format, as part of the TDP. In addition, the usability test report **shall** be submitted to the EAC as part of the documentation manufacturers are required to file with the application to test a voting system.
b. The Acc-VS **shall** provide an audio-tactile interface (ATI) that supports the full functionality of the visual ballot interface.

Discussion: Note the necessity of both audio output and tactilely discernible controls for voter input. Full functionality includes at least:

- Instructions and feedback on initial activation of the ballot (such as insertion of a smart card), if applicable;
- Instructions and feedback to the voter on how to operate the accessible voting station, including settings and options (e.g., volume control, repetition);

9 The italicized text in Section 3.3.2 is based on EAC Decision on Request for Interpretation 2007-01, http://www.eac.gov/assets/1/Page/EAC%20Decision%20on%20Accessible%20Design.pdf.

- Instructions and feedback for navigation of the ballot;
- Instructions and feedback for contest choices, including write-in candidates;
- Instructions and feedback on confirming and changing votes; and
- Instructions and feedback on final submission of ballot.

i. The ATI **shall** provide the same capabilities to vote and cast a ballot as are provided by its visual interface.

Discussion: For example, if a visual ballot supports voting a straight party ticket and then changing the vote for a single contest, so must the ATI.

ii. The ATI **shall** allow the voter to have any information provided by the voting system repeated.

Discussion: This feature may also be useful to voters with cognitive disabilities.

iii. The ATI **shall** allow the voter to pause and resume the audio presentation.

Discussion: This feature may also be useful to voters with cognitive disabilities.

iv. The ATI **shall** allow the voter to skip to the next contest or return to previous contests.

Discussion: This is analogous 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.

v. The ATI **shall** allow the voter to skip over the reading of a referendum so as to be able to vote on it immediately.

Discussion: This is analogous to the ability of sighted voters to skip over the wording of a referendum on which they have already made a decision prior to the voting session (e.g., "Vote yes on proposition #123").

c. Voting stations that provide audio presentation of the ballot **shall** do so in a usable way, as detailed in the following sub-requirements.

Discussion: These requirements apply to all voting system audio output, not just to the ATI of an Acc-VS.

i. The ATI **shall** provide its audio signal through an industry standard connector for private listening using a 3.5mm stereo headphone jack to allow voters to use their own audio assistive devices.
ii. If the ATI utilizes a telephone style handset or headphone to provide audio information, it **shall** provide a wireless T-Coil[10] coupling for assistive hearing devices so as to provide access to that information for voters with partial hearing. That coupling **shall** achieve at least a category T4 rating as defined by [ANSI01] American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19.

Discussion: Note that Requirement 3.3.6 c protects the use of hearing devices.

iii. A sanitized headphone or handset **shall** be made available to each voter.

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

iv. The audio system **shall** set the initial volume for each voting session between 60 and 70 dB SPL.

Discussion: A voter does not "inherit" the volume as set by the previous user of the voting station. See requirement 3.2.5 b.

v. The audio system **shall** allow the voter to control the volume throughout the voting session while preserving the current votes. The volume **shall** be adjustable from a minimum of 20dB SPL up to a maximum of 100 dB SPL, in increments no greater than 10 dB.
vi. The audio system **shall** 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.

vii. The audio presentation of verbal information should be readily comprehensible by voters who have normal hearing and are proficient in the language. This includes such characteristics as proper enunciation, normal intonation, appropriate rate of speech, and low background noise. Candidate names should be pronounced as the candidate intends.

10 For additional clarification, see EAC Decision on Request for Interpretation 2009-05, http://www.eac.gov/assets/1/Page/EAC Decision on T-Coil Requirements.pdf

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 the audio presentation is determined by election officials designing the ballot, it is beyond of the scope of this requirement.

viii. The audio system **shall** allow the voter to control the rate of speech throughout the voting session while preserving the current votes. The range of speeds supported **shall** include 75% to 200% of the nominal rate. Adjusting the rate of speech **shall** not affect the pitch of the voice.

Discussion: Many blind voters are accustomed to interacting with accelerated speech. This feature may also be useful to voters with cognitive disabilities.

d. If the Acc-VS supports ballot activation for non-blind voters, then it **shall** also provide features that enable voters who are blind to perform this activation.

Discussion: For example, smart cards might provide tactile cues so as to allow correct insertion.

e. If the Acc-VS supports ballot submission or vote verification for non-blind voters, then it **shall** also provide features that enable voters who are blind to perform these actions.

Discussion: For example, if voters using this station normally perform paper-based verification, or if they feed their own optical scan ballots into a reader, blind voters must also be able to do so.

f. Mechanically operated controls or keys, or any other hardware interface on the Acc-VS available to the voter **shall** be tactilely discernible without activating those controls or keys.

Discussion: A blind voter should be able to operate the Acc-VS by “feel” alone. This means that vision should not be necessary for such operations as inserting a smart card or plugging into a headphone jack. Note also the more general Requirement 3.2.5 c. against accidental activation of controls.

g. The status of all locking or toggle controls or keys (such as the "shift" key) for the Acc-VS **shall** be visually discernible, and also discernible through either touch or sound.

3.3.4 Enhanced input and control characteristics

These requirements specify the features of the Acc-VS designed to assist voters who lack fine motor control or use of their hands.

a. The manufacturer **shall** conduct summative usability tests on the Acc-VS using individuals lacking fine motor control and **shall** report the test results, using the Common Industry Format, as part of the TDP. In addition, the usability test report **shall** be submitted to the EAC as part of the documentation manufacturers are required to file with the application to test a voting system.
b. The Acc-VS **shall** provide a 3.5 mm industry standard jack used to connect a personal assistive technology switch to the Acc-VS. This jack **shall** not allow data other than the switch state to be transmitted to the voting system. The voting system **shall** accept switch input that is functionally equivalent to tactile input. All the functionality of the Acc-VS (e.g., straight party voting, write-in candidates) that is available through the conventional forms of input, such as tactile, **shall** also be available through this non-manual input mechanism.

> Discussion: This requirement ensures that the Acc-VS is operable by individuals who do not have the use of their hands. Examples of non-manual controls include "sip and puff" switches. 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.

c. The Acc-VS **shall** provide features that 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.

> Discussion: For example, if voters using this station normally perform paper-based verification, or if they feed their own optical scan ballots into a reader, voters with dexterity disabilities must also be able to do so. Note that the general requirement for privacy when voting (Requirement part 1:3.2.3.1 a.) still applies.

d. Keys, controls, and other manual operations on the Acc-VS **shall** be operable with one hand and **shall** not require tight grasping, pinching, or twisting of the wrist. The force required to activate controls and keys **shall** be no greater 5 lbs. (22.2 N).

> Discussion: Controls are to be operable without excessive force. This includes operations such as inserting an activation card, and inserting and removing ballots.

e. The Acc-VS controls **shall** not require direct bodily contact or for the body to be part of any electrical circuit.

Discussion: This requirement ensures that controls are operable by individuals using prosthetic devices.

3.3.5 Design for mobility aids

These requirements specify the features of the Acc-VS designed to assist voters who use mobility aids, including wheelchairs. Many of the requirements of this section are based on the ADA Accessibility Guidelines for Buildings and Facilities (ADAAG).

a. The Acc-VS **shall** provide a clear floor space of 30 inches minimum by 48 inches minimum for a stationary mobility aid. The clear floor space **shall** be designed for a forward approach or a parallel approach.
b. When deployed according to the installation instructions provided by the manufacturer, the Acc-VS **shall** allow adequate room for an assistant to the voter. This includes clearance for entry to and exit from the area of the voting station.

Discussion: Disabled voters sometimes prefer to have an assistant help them vote. The setup of the Acc-VS should not preclude this.

c. Labels, displays, controls, keys, audio jacks, and any other part of the Acc-VS necessary for the voter to operate the voting system **shall** be legible and visible to a voter in a wheelchair with normal eyesight (no worse than 20/40, corrected) who is in an appropriate position and orientation with respect to the Acc-VS.

Discussion: There are a number of factors that could make relevant parts of the Acc-VS difficult to see, such as: small lettering; controls and labels tilted at an awkward angle from the voter's viewpoint; and glare from overhead lighting.

3.3.5.1 Controls within reach

The requirements of this section ensure that the controls, keys, audio jacks and any other part of the Acc-VS necessary for its operation are within easy reach. Note that these requirements have meaningful application mainly to controls in a fixed location. A hand-held tethered control panel is another acceptable way of providing reachable controls.

a. If the Acc-VS has a forward approach with no forward reach obstruction then the high reach **shall** be 48 inches maximum and the low reach **shall** be 15 inches minimum. See Part 1: Figure 3-1.
b. If the Acc-VS has a forward approach with a forward reach obstruction, the following sub-requirements **shall** apply. (See Part 1: Figure 3-2).
    i. The forward obstruction for the Acc-VS **shall** be no greater than 25 inches in depth, its top no higher than 34 inches and its bottom surface no lower than 27 inches.

ii. If the obstruction for the Acc-VS is no more than 20 inches in depth, then the maximum high reach **shall** be 48 inches, otherwise it **shall** be 44 inches.
iii. Space under the obstruction between the finish floor or ground and 9 inches above the finish floor or ground **shall** be considered toe clearance and **shall** comply with the following provisions for the Acc-VS:

1. Toe clearance depth **shall** extend 25 inches maximum under the obstruction;
2. The minimum toe clearance depth under the obstruction **shall** be either 17 inches or the depth required to reach over the obstruction to operate the Acc-VS, whichever is greater; and
3. Toe clearance width **shall** be 30 inches minimum.

iv. Space under the obstruction between 9 inches and 27 inches above the finish floor or ground **shall** be considered knee clearance and **shall** comply with the following provisions:

1. Knee clearance depth **shall** extend 25 inches maximum under the obstruction at 9 inches above the finish floor or ground;
2. The minimum knee clearance depth at 9 inches above the finish floor or ground **shall** be either 11 inches or 6 inches less than the toe clearance, whichever is greater;
3. Between 9 inches and 27 inches above the finish floor or ground, the knee clearance depth **shall** be permitted to reduce at a rate of 1 inch in depth for each 6 inches in height. (It follows that the minimum knee clearance at 27 inches above the finish floor or ground **shall** be 3 inches less than the minimum knee clearance at 9 inches above the floor.); and
4. Knee clearance width **shall** be 30 inches minimum.

c. If the Acc-VS has a parallel approach with no side reach obstruction then the maximum high reach **shall** be 48 inches and the minimum low reach **shall** be 15 inches. See Part 1: Figure 3-3.
d. If the Acc-VS has a parallel approach with a side reach obstruction, the following sub-requirements **shall** apply. See Part 1: Figure 3-4.

Discussion: Since this is a parallel approach, no clearance under the obstruction is required.

i. The side obstruction for the Acc-VS **shall** be no greater than 24 inches in depth and its top no higher than 34 inches.
ii. If the obstruction is no more than 10 inches in depth, then the maximum high reach **shall** be 48 inches, otherwise it **shall** be 46 inches.

Figures 1-4 Unobstructed reach measurements

Dimensions shown in inches above the line, SI units (in millimeters) below the line

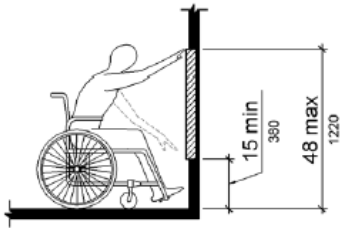

Figure 1: Unobstructed forward reach

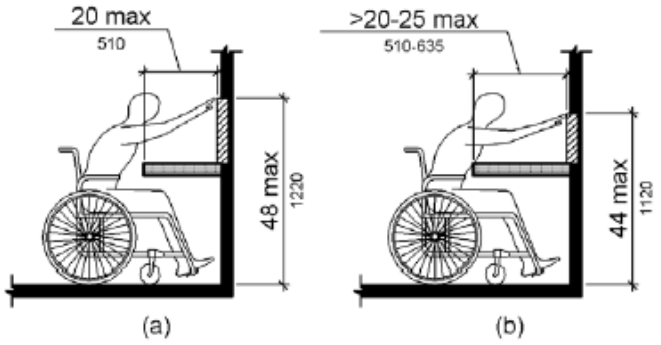

Figure 2: Obstructed forward reach

(a) for an obstruction depth of up to 20 inches
(b) for an obstruction depth of up to 25 inches

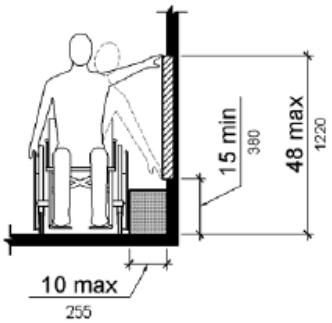

Figure 3: Unobstructed side reach with an allowable obstruction less than 10 inches deep

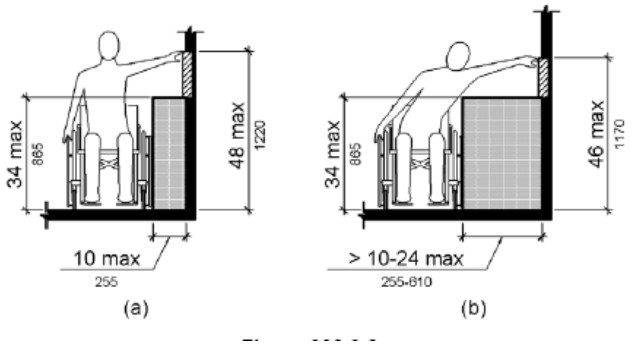

Figure 4: Obstructed side reach

(a) for an obstruction depth of up to 10 inches
(b) for an obstruction depth of up to 24 inches

3.3.6 Enhanced auditory interfaces

These requirements specify the features of the Acc-VS designed to assist voters with hearing disabilities.

a. The Acc-VS **shall** incorporate the features listed under Requirement 3.3.3 c for voting systems that provide audio presentation of the ballot.

Discussion: Note especially the requirements for volume initialization and control.

b. If the Acc-VS provides sound cues as a method to alert the voter, the tone **shall** be accompanied by a visual cue, unless the station is in audio-only mode.

Discussion: For instance, the voting equipment might beep if the voter attempts to overvote. If so, there would have to be an equivalent visual cue, such as the appearance of an icon, or a blinking element. If the Acc-VS has been set to audio-only mode, there would be no visual cue.

c. No voting device **shall** cause electromagnetic interference with assistive hearing devices that would substantially degrade the performance of those devices. The voting device, measured as if it were a wireless device, **shall** achieve at least a category T4 rating as defined by [ANSI01] American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19.

Discussion: "Hearing devices" include hearing aids and cochlear implants.

3.3.7 Design in support of cognitive disabilities

These requirements specify the features of the Acc-VS designed to assist voters with cognitive disabilities.

a. The Acc-VS should provide support to voters with cognitive disabilities.

Discussion: Because of the highly varied nature of disabilities falling within the "cognitive" category, there are no design features uniquely aimed at helping those with such disabilities. However, many of the features designed primarily for other disabilities and for general usability are also highly relevant to these voters:

- The synchronization of audio with the displayed screen information (Requirement 3.3.2 d.);
- Requirement 3.2.4 and, in particular, the use of plain language (Requirement 3.2.4 c.);
- Large font sizes and legibility of paper (Requirement 3.2.5 e and 3.2.5 g.); and
- The ability to control various aspects of the audio presentation (Requirement 3.3.3 b. and 3.3.3 c) such as pausing, repetition, and speed.

3.3.8 English proficiency

These requirements specify the features of the Acc-VS designed to assist voters who lack proficiency in reading English.

a. For voters who lack proficiency in reading English, the Acc-VS **shall** provide an audio interface for instructions and ballots as described in 3.3.3 b.

3.3.9 Speech not required

a. The voting system **shall** not require voter speech for its operation.

> Discussion: This does not preclude voting systems from offering speech input as an option, but speech must not be the only means of input.

4 Hardware Requirements

Table of Contents

4 Hardware Requirements

This section contains the requirements for the machines and manufactured devices that are part of a voting system. It specifies minimum values for certain performance characteristics; physical characteristics; and design, construction, and maintenance characteristics for the hardware and selected related components of all voting systems, such as:

- Ballot printers
- Ballots
- Ballot displays
- Voting devices, including ballot marking devices and DRE recording devices
- Voting booths and enclosures
- Ballot boxes and ballot transfer boxes
- Ballot readers
- Computers used to prepare ballots, program elections, consolidate and report votes, and perform other elections management activities
- Electronic ballot recorders
- Electronic precinct vote control units
- Removable electronic data storage media
- Servers
- Printers

This section applies to the **combination of software and hardware** to accomplish specific performance and system control requirements. Standards that are specific to software alone are provided in Section 5.

The requirements of this section apply generally to all hardware used in voting systems, including:

- Hardware provided by the voting system manufacturer and its suppliers
- Hardware furnished by an external provider (for example, providers of commercial-off-the-shelf equipment) where the hardware may be used in any way during voting system operation
- Hardware provided by the voting jurisdiction

The requirements presented in this section are organized as follows:

Performance Requirements: These requirements address the combined operational capabilities of the voting system hardware and software across a broad range of parameters

Physical Requirements: These requirements address the size, weight and transportability of the voting system

Design, Construction, and Maintenance Requirements: These requirements address the reliability and durability of materials, product marking, quality of system

workmanship, safety, and other attributes to ensure smooth system operation in the voting environment

4.1 Performance Requirements

The performance requirements address a broad range of parameters, encompassing:

- Accuracy requirements, where requirements are specified for distinct processing functions of paper-based and DRE systems
- Environmental requirements, where no distinction is made between requirements for paper-based and DRE systems, but requirements for precinct and central count are described
- Vote data management requirements, where no differentiation is made between requirements for paper-based and DRE systems
- Vote recording requirements, where separate and distinct requirements are delineated for paper-based and DRE systems
- Conversion requirements, which apply only to paper-based systems
- Processing requirements, where separate and distinct requirements are delineated for paper-based and DRE systems
- Reporting requirements, where no distinction is made between requirements for paper-based and DRE systems, but where differences between precinct and central count systems are readily apparent based on differences of their reporting

The performance requirements include such attributes as ballot reading and handling requirements; system accuracy; memory stability; and the ability to withstand specified environmental conditions. These characteristics also encompass system-wide requirements for shelter, electrical supply, and compatibility with data networks.

Performance requirements for voting systems represent the combined operational capability of both system hardware and software. Accuracy, as measured by data error rate, and operational failure are treated as distinct attributes in performance testing. All systems **shall** meet the performance requirements under operating conditions and after storage under non-operating conditions.

4.1.1 Accuracy Requirements

The following requirements are intended to allow tolerance for unpreventable hardware-related errors that occur rarely and randomly as a result of physical phenomena affecting optical scanning sensors. They are not intended to allow tolerance of software faults that result in systematic miscounting of votes. Section 2.1.2 includes a requirement for logical accuracy.

a. All systems **shall** achieve a report total error rate of no more than one in 125,000 (8×10^{-6}).
b. Given a set of vote data reports, the observed cumulative report total error rate **shall** be calculated as follows.

i. Define a "report item" as any one of the numeric values (totals or counts) that must appear in any of the vote data reports. Each ballot count, each vote, overvote, and undervote total for each contest, and each vote total for each contest choice in each contest is a separate report item. The required report items are detailed in Volume I Chapters 2 and 4.
ii. For each report item, compute the "report item error" as the absolute value of the difference between the correct value and the reported value. Special cases: If a value is reported that should not have appeared at all (spurious item), or if an item that should have appeared in the report does not (missing item), assess a report item error of one. Additional values that are reported as a manufacturer extension to the standard are not considered spurious items.
iii. Compute the "report total error" as the sum of all of the report item errors from all of the reports.
iv. Compute the "report total volume" as the sum of all of the correct values for all of the report items that are supposed to appear in the reports. Special cases: When the same logical contest appears multiple times, e.g. when results are reported for each ballot configuration and then combined or when reports are generated for multiple reporting contexts, each manifestation of the logical contest is considered a separate contest with its own correct vote totals in this computation.
v. Compute the observed cumulative report total error rate as the ratio of the report total error to the report total volume. Special cases: If both values are zero, the report total error rate is zero. If the report total volume is zero but the report total error is not, the report total error rate is infinite.

The benchmark of one in 125,000 (8×10^{-6}) is derived from the "maximum acceptable error rate" used as the lower test benchmark in the 2005 Voluntary Voting System Guidelines Version 1.0. That benchmark was defined as a ballot position error rate of one in 500,000 (2×10^{-6}). The benchmark of one in 125,000 is expressed in terms of votes[11], however it is consistent with the previous benchmark in that the estimated ratio of votes to ballot positions is ¼.

Given that there is no "typical" ratio of votes to ballot positions with such diversity among the many jurisdictions, it is nevertheless necessary to base the benchmark on some rough estimates in order that it may be in the correct order of magnitude, albeit not optimal for every case. The estimated ratio was derived as follows. In a presidential election, there would be approximately 20 contests with a vote for 1 on each ballot with an average of 4 candidates, including the write-in position, per contest. (Some states would have fewer contests and some more. A few contests, like President, would have 8–13 candidates; most would have 3 candidates including the write-in, and a few would have 2 candidates.) Thus, the estimated ratio of votes to ballot positions is ¼.

11 The error rate was originally defined in Volume 1 of the 2002 Voting System Standards and is prescribed by Sec. 301(a)(5) of the Help America Vote Act of 2002. Expressing this benchmark in terms of votes instead of ballot positions provides a more precise metric for the evaluation of accuracy.

4.1.2 Environmental Requirements

The environmental requirements for voting systems include shelter, space, furnishings and fixtures, supplied energy, environmental control, and external telecommunications services. Environmental conditions applicable to the design and operation of voting systems consist of the following categories:

- Natural environment, including temperature, humidity, and atmospheric pressure
- Induced environment, including proper and improper operation and handling of the system and its components during the election processes
- Transportation and storage
- Electromagnetic signal environment, including exposure to and generation of radio frequency energy

a. All voting systems **shall** be designed to withstand the environmental conditions contained in the appropriate test procedures of the Guidelines. These procedures will be applied to all devices for casting, scanning and counting ballots, except those that constitute COTS devices that have not been modified in any manner to support their use as part of a voting system and that have a documented record of performance under conditions defined in the Guidelines.
b. The Technical Data Package supplied by the manufacturer **shall** include a statement of all requirements and restrictions regarding
    i. Environmental protection
    ii. Electrical service
    iii. Recommended auxiliary power
    iv. Telecommunications service
    v. Any other facility or resource required for the proper installation and operation of the system.

4.1.2.1 Shelter Requirements

All precinct count systems **shall** be designed for storage and operation in any enclosed facility ordinarily used as a warehouse or polling place, with prominent instructions as to any special storage requirements.

4.1.2.2 Space Requirements

There is no restriction on space allowed for the installation of voting systems, except that the arrangement of these systems **shall** not impede performance of their duties by polling place officials, the orderly flow of voters through the polling place or the ability for the voter to vote in private.

4.1.2.3 Furnishings and Fixtures

Any furnishings or fixtures provided as a part of voting systems, and any components provided by the manufacturer that are not a part of the voting system but that are used to support its storage, transportation or operation, **shall** comply with the safety design of Subsection 4.3.8.

4.1.2.4 Electrical Supply

Components of voting systems that require an electrical supply **shall** meet the following standards:

a. Precinct count voting systems **shall** operate with the electrical supply ordinarily found in polling places (Nominal 120 Vac/60Hz/1 phase)
b. Central count voting systems **shall** operate with the electrical supply ordinarily found in central tabulation facilities or computer room facilities (Nominal 120 Vac/60Hz/1, nominal 208 Vac/60Hz/3 or nominal 240 Vac/60Hz/2)
c. Precinct count[12] voting machines **shall** also be capable of operating for a period of at least 2 hours on backup power, such that no voting data is lost or corrupted nor normal operations interrupted. When backup power is exhausted the voting machine **shall** retain the contents of all memories intact

> Discussion: All forms of voting equipment, including optical scan, **shall** include battery backup[13].

The backup power capability is not required to provide lighting of the voting area.

Central count systems are not required to have a 2 hour battery backup. A central count system **shall** provide for a graceful shutdown to allow switching to an alternate power source. The shutdown can be implemented either by means of a user controlled intervention or an automatic systematic operation. The graceful shutdown **shall** meet the following requirements:[14]

d. The alert to the user that the system has lost power and is shutting down (systematic) or needs to be shut down (user intervention) should be easily

12 The italicized text in Section 4.1.2.4 is based on EAC Decision on Request for Interpretation 2008-06, http://www.eac.gov/assets/1/Page/EAC%20Decision%20on%20Battery%20Backup%20for%20Central%20Count.pdf.
13 The italicized text in the discussion box is based specifically on EAC Decision on Request for Interpretation 2008-02, http://www.eac.gov/assets/1/Page/EAC%20Decision%20on%20Battery%20Backup%20for%20Optical%20Scan%20Voting%20Machines.pdf.
14 The remaining italicized text is based on EAC Decision on Request for Interpretation 2008-06, http://www.eac.gov/assets/1/Page/EAC%20Decision%20on%20Battery%20Backup%20for%20Central%20Count.pdf, and 2009-03, http://www.eac.gov/assets/1/Page/EAC%20Decision%20on%20Battery%20Back%20Up%20for%20Central%20Count%20Systems.pdf.

recognizable and documentation should be provided to illustrate the proper course of action that needs to be taken.

e. All ballots **shall** reside in either the input or output hopper with no ballots in process at the end of the shutdown process.
f. All ballots in the output hopper **shall** be fully read and saved.
g. All actions taken by the system or the user to initiate the shut down are considered "events" and **shall** be logged per Requirements 2.1.4 g & i.
h. A report, including the final state of all ballots, timestamps and of the final state of the unit, **shall** be printed or saved in a file. The report **shall** be part of the permanent election record and **shall** be available when power is restored to the system.
i. The system **shall** be capable of resuming operation from the point it stopped once power is restored.

Testing for the graceful shutdown **shall** maintain ballots in the input hopper through the shutdown process. The purpose of this requirement is to confirm that the system will stop processing further ballots, complete ballots in process and save a report that accurately identifies the final state of the ballots and the system. The second part of the test **shall** restore power to the system and confirm that the system restarts properly and that the status report reflects accurately the state of the ballots and the system.

4.1.2.5 Electrical Power Disturbance

Vote scanning and counting equipment for paper-based voting systems, and all DRE voting equipment, **shall** be able to withstand, without disruption of normal operation or loss of data:

a. Voltage dip of 30% of nominal @10 ms;
b. Voltage dip of 60% of nominal @100 ms & 1 sec
c. Voltage dip of >95% interrupt @5 sec
d. Surges of ±15% line variations of nominal line voltage
e. Electric power increases of 7.5% and reductions of 12.5% of nominal specified power supply for a period of up to four hours at each power level

4.1.2.6 Electrical Fast Transient

Vote scanning and counting equipment for paper-based systems, and all DRE equipment, **shall** be able to withstand, without disruption of normal operation or loss of data, electrical fast transients of:

a. +2 kV and −2 kV on External Power lines (both AC and DC)
b. +1 kV and −1 kV on Input/Output lines(signal, data, and control lines) longer than 3 meters
c. Repetition Rate for all transient pulses will be 100 kHz

4.1.2.7 Lightning Surge

Vote scanning and counting equipment for paper-based systems, and all DRE equipment, **shall** be able to withstand, without disruption of normal operation or loss of data, surges of:

a. ±2 kV AC line to line
b. ±2 kV AC line to earth
c. + or – 0.5 kV DC line to line >10m
d. + or – 0.5 kV DC line to earth >10m
e. ±1 kV I/O sig/control >30m

4.1.2.8 Electrostatic Disruption

Vote scanning and counting equipment for paper-based systems, and all DRE equipment, **shall** be able to withstand ±15 kV air discharge and ±8 kV contact discharge without damage or loss of data. The equipment may reset or have momentary interruption so long as normal operation is resumed without human intervention or loss of data. Loss of data means votes that have been completed and confirmed to the voter.

4.1.2.9 Electromagnetic Emissions

All voting equipment **shall** comply with the Rules and Regulations of the Federal Communications Commission, Part 15, Class B requirements for both radiated and conducted emissions.

4.1.2.10 Electromagnetic Susceptibility

Vote scanning and counting equipment for paper-based systems, and all DRE equipment, **shall** be able to withstand an electromagnetic field of 10 V/m modulated by a 1 kHz 80% AM modulation over the frequency range of 80 MHz to 1000 MHz, without disruption of normal operation or loss of data.

4.1.2.11 Conducted RF Immunity

Vote scanning and counting equipment for paper-based systems, and all DRE equipment, **shall** be able to withstand, without disruption of normal operation or loss of data, conducted RF energy of:

a. 10V rms over the frequency range 150 KHz to 80 MHz with an 80% amplitude modulation with a 1 KHz sine wave AC & DC power

b. 10V sig/control >3 m over the frequency range 150 KHz to 80 MHz with an 80% amplitude modulation with a 1 KHz sine wave

4.1.2.12 Magnetic Fields Immunity

Vote scanning and counting equipment for paper-based systems, and all DRE equipment, **shall** be able to withstand, without disruption of normal operation or loss of data, AC magnetic fields of 30 A/m at 60 Hz.

4.1.2.13 Environmental Control - Operating Environment

Voting systems **shall** be capable of operation in temperatures ranging from 41 °F to 104 °F (5 °C to 40 °C) and relative humidity from 5% to 85%, non-condensing. If the system documentation states that the system can operate in humidity higher or lower than the required range, the system **shall** be tested to the level of humidity asserted in the documentation.

For testing information, see Volume II, section 4.7.1.

4.1.2.14 Environmental Control - Transit and Storage

Equipment used for vote casting or for counting votes in a precinct count system, **shall** meet these specific minimum performance standards that simulate exposure to physical shock and vibration associated with handling and transportation by surface and air common carriers, and to temperature conditions associated with delivery and storage in an uncontrolled warehouse environment:

a. High and low storage temperatures ranging from -4 to +140 degrees Fahrenheit, equivalent to MIL-STD-810D, Methods 501.2 and 502.2, Procedure I-Storage
b. Bench handling equivalent to the procedure of MIL-STD-810D, Method 516.3, Procedure VI
c. Vibration equivalent to the procedure of MIL-STD-810D, Method 514.3, Category 1- Basic Transportation, Common Carrier
d. Uncontrolled humidity equivalent to the procedure of MIL-STD-810D, Method 507.2, Procedure I-Natural Hot-Humid

4.1.2.15 Data Network Requirements

Voting systems may use a local or remote data network. If such a network is used, then all components of the network **shall** comply with the telecommunications requirements described in Section 6 and the Security requirements described in Section 7.

4.1.3 Election Management System Requirements

The Election Management System (EMS) requirements address electronic hardware and software used to conduct the pre-voting functions defined in Section 2 with regard to ballot preparation, election programming, ballot and program installation, readiness testing, verification at the polling place, and verification at the central location.

4.1.3.1 Recording Requirements

Voting systems **shall** accurately record all election management data entered by the user, including election officials or their designees.

For recording accuracy, all systems **shall**:

a. Record every entry made by the user
b. Add permissible voter selections correctly to the memory components of the device
c. Verify the correctness of detection of the user selections and the addition of the selections correctly to memory
d. Add various forms of data entered directly by the election official or designee, such as text, line art, logos, and images
e. Verify the correctness of detection of data entered directly by the user and the addition of the selections correctly to memory
f. Preserve the integrity of election management data stored in memory against corruption by stray electromagnetic emissions, and internally generated spurious electrical signals
g. Log corrected data errors by the voting system

4.1.3.2 Memory Stability

Memory devices used to retain election management data **shall** have demonstrated error-free data retention for a period of 22 months.

4.1.4 Vote Recording Requirements

The vote recording requirements address the enclosure, equipment, and supplies used by voters to vote.

4.1.4.1 Common Requirements

All voting systems **shall** provide voting booths or enclosures for poll site use. Such booths or enclosures may be integral to the voting system or supplied as components of the voting system, and **shall**:

a. Be integral to, or make provision for, the installation of the voting machine
b. Ensure by its structure stability against movement or overturning during entry, occupancy, and exit by the voter
c. Provide privacy for the voter, and be designed in such a way as to prevent observation of the ballot by any person other than the voter
d. Be capable of meeting the accessibility requirements of Subsection 3.2

4.1.4.2 Paper-based Recording Requirements

The paper-based recording requirements govern:

- Ballots, sheets, and pages or assemblies of pages containing ballot field identification data
- Ballot marking devices
- Frames or fixtures to hold the ballot while it is being marked
- Compartments or booths where voters record selections
- Secure containers for the collection of voted ballots

a. Paper ballots used by paper-based voting systems **shall** meet the following standards:
    i. Marks that identify the unique ballot format **shall** be outside the area in which votes are recorded, so as to minimize the likelihood that these marks will be mistaken for vote responses and the likelihood that recorded votes will obliterate these marks
    ii. If printed alignment marks are used to locate the vote response fields on the ballot, these marks **shall** be outside the area in which votes are recorded, so as to minimize the likelihood that these marks will be mistaken for vote responses and the likelihood that recorded votes will obliterate these marks
    iii. The Technical Data Package **shall** specify the required paper stock, size, shape, opacity, color, watermarks, field layout, orientation, size and style of printing, size and location of mark fields used for vote response fields and to identify unique ballot formats, placement of alignment marks, ink for printing, and folding and bleed-through limitations for preparation of ballots that are compatible with the system
b. The Technical Data Package **shall** specify marking devices, which, if used to make the prescribed form of mark, produce readable marked ballots such that the system meets the performance requirements for accuracy in Subsection 4.1.1. Marking devices can be either manual (such as pens or pencils) or electronic. These specifications **shall** identify:
    i. Specific characteristics of marking devices that affect readability of marked ballots

ii. Performance capabilities with regard to each characteristic
iii. For marking devices manufactured by multiple external sources, a listing of sources and model numbers that are compatible with the system

c. A frame or fixture for printed ballots is optional. However, if such a device is provided, it **shall**:
   i. Be of any size and shape consistent with its intended use
   ii. Position the card properly
   iii. Hold the ballot securely in its proper location and orientation for voting
   iv. Comply with the requirements for design and construction contained in Subsection 4.3

d. Ballot boxes and ballot transfer boxes, which serve as secure containers for the storage and transportation of voted ballots, shall:
   i. Be of any size, shape, and weight commensurate with their intended use
   ii. Incorporate locks or seals, the specifications of which are described in the system documentation
   iii. Provide specific points where ballots are inserted, with all other points on the box constructed in a manner that prevents ballot insertion
   iv. For precinct count systems, contain separate compartments for the segregation of unread ballots, ballots containing write-in votes or any irregularities that may require special handling or processing. In lieu of compartments, the conversion processing may mark such ballots with an identifying spot or stripe to facilitate manual segregation

4.1.4.3 DRE System Recording Requirements

The DRE system recording requirements address the detection and recording of votes, including the logic and data processing functions required to determine the validity of voter selections, to accept and record valid selections, and to reject invalid selections. The requirements also address the physical environment in which ballots are cast.

a. DRE systems shall include an audible or visible activity indicator providing the status of each voting device. This indicator **shall**:
   i. Indicate whether the device has been activated for voting
   ii. Indicate whether the device is in use

b. To ensure vote recording accuracy and integrity while protecting the anonymity of the voter, all DRE systems **shall**:
   i. Contain all mechanical, electromechanical, and electronic components; software; and controls required to detect and record the activation of selections made by the voter in the process of voting and casting a ballot
   ii. Incorporate redundant memories to detect and allow correction of errors caused by the failure of any of the individual memories
   iii. Provide at least two processes that record the voter's selections that:

      - To the extent possible, are isolated from each other
      - Designate one process and associated storage location as the main vote detection, interpretation, processing and reporting path

iv. Use a different process to store ballot images, for which the method of recording may include any appropriate encoding or data compression procedure consistent with the regeneration of an unequivocal record of the ballot as cast by the voter
v. Provide a capability to retrieve ballot images in a form readable by humans
vi. Ensure that all processing and storage protects the anonymity of the voter

c. DRE systems **shall** meet the following requirements for recording accurately each vote and ballot cast:
   i. Detect every selection made by the voter
   ii. Correctly add permissible selections to the memory components of the device
   iii. Verify the correctness of the detection of the voter selections and the addition of the selections to memory
   iv. Maintain absolute correctness (introduce no errors) in the recording, tabulating, and reporting of votes by software, firmware, and hardwired logic (per Requirement 2.1.2.g)
   v. Achieve an error rate that enables satisfaction of the system-level [hardware] accuracy requirement indicated in Subsection 4.1.1
   vi. Preserve the integrity of voting data and ballot images (for DRE machines) stored in memory for the official vote count and audit trail purposes against corruption by stray electromagnetic emissions, and internally generated spurious electrical signals
   vii. Maintain a log of corrected data

4.1.5 Paper-based Conversion Requirements

The paper-based conversion requirements address the ability of the system to read the ballot and to translate its pattern of marks into electronic signals for later processing. These capabilities may be built into the voting system in an integrated fashion, or may be provided by one or more components that are not unique to the system, such as a general purpose data processing ballot reader or read head suitably interfaced to the system. These requirements address two major functions: ballot handling and ballot reading.

4.1.5.1 Ballot Handling

Ballot handling consists of a ballot's acceptance, movement through the read station, and transfer into a collection station or receptacle.

a. The capacity to convert the marks on individual ballots into signals is uniquely important to central count systems. The capacity for a central count system **shall** be documented by the manufacturer. This documentation **shall** include the capacity for individual components that impact the overall capacity
b. When ballots are unreadable or some condition is detected requiring that the ballots be segregated from normally processed ballots for human review (e.g. write-ins), all central count paper-based systems **shall** do one of the following:
   i. Outstack the ballot

ii. Stop the ballot reader and display a message prompting the election official or designee to remove the ballot
iii. Mark the ballot with an identifying mark to facilitate its later identification

c. Additionally, the system **shall** provide a capability that can be activated by an authorized election official to identify ballots containing overvotes, blank ballots, and ballots containing undervotes in a designated contest. If enabled, these capabilities **shall** perform one of the above actions in response to the indicated condition.
d. When ballots are unreadable or when some condition is detected requiring that the ballots be segregated from normally processed ballots for human review (e.g. write-in votes) all precinct count systems **shall**:
    i. In response to an unreadable or blank ballot, return the ballot and provide a message prompting the voter to examine the ballot
    ii. In response to a ballot with a write-in vote, segregate the ballot or mark the ballot with an identifying mark to facilitate its later identification
    iii. In response to a ballot with an overvote the system **shall**:

        - Provide a capability to identify an overvoted ballot
        - Return the ballot
        - Provide an indication prompting the voter to examine the ballot
        - Allow the voter to correct the ballot
        - Provide a means for an authorized election official to deactivate this capability entirely and by contest

    iv. In response to a ballot with an undervote, the system **shall**:

        - Provide a capability to identify an undervoted ballot
        - Return the ballot
        - Provide an indication prompting the voter to examine the ballot
        - Allow the voter to correct the ballot
        - Allow the voter to submit the ballot with the undervote
        - Provide a means for an authorized election official to deactivate this capability

e. Ballot readers **shall** prevent multiple feed or detect and provide an alarm indicating multiple feed. Multiple feed occurs when a ballot reader attempts to read more than one ballot at a time.
    i. If multiple feed is detected, the ballot reader **shall** halt in a manner that permits the operator to remove the unread ballots causing the error, and reinsert them in the input hopper

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

f. All paper-based tabulators and EBMs **shall** achieve a misfeed rate of no more than 0.002 (1⁄500).
g. The observed cumulative misfeed rate **shall** be calculated as follows:

i. Compute the "misfeed total" as the number of times that unforced multiple feed, misfeed (jam), or rejection of a ballot that meets all manufacturer specifications has occurred during the execution of tests. It is possible for a given ballot to misfeed more than once; each misfeed would be counted.
ii. Compute the "total ballot volume" as the number of successful feeds of ballot pages during the execution of tests. (If the pages of a multi-page ballot are fed separately, each page counts; but if both sides of a two-sided ballot are read in one pass through the tabulator, it only counts once.)
iii. Compute the observed cumulative misfeed rate as the ratio of the misfeed total to the total ballot volume. Special cases: If both values are zero, the misfeed rate is zero. If the total ballot volume is zero but the misfeed total is not, the misfeed rate is infinite.

4.1.5.2 Ballot Reading Accuracy

This paper-based system requirement governs the conversion of the physical ballot into electronic data. Reading accuracy for ballot conversion refers to the ability to:

a. Recognize vote punches or marks, or the absence thereof, for each possible selection on the ballot
b. Discriminate between valid punches or marks and extraneous perforations, smudges, and folds
c. Convert the vote punches or marks, or the absence thereof, for each possible selection on the ballot into digital signals

To ensure accuracy, paper-based systems **shall**:

d. Detect marks that conform to manufacturer specifications with an error rate that enables satisfaction of the system-level accuracy requirement indicated in Subsection 4.1.1
e. Ignore, and not record, extraneous perforations, smudges, and folds

4.1.6 Tabulation Processing Requirements

Tabulation processing requirements apply to the hardware and software required to accumulate voting data for all candidates and measures within voting machines and polling places, and to consolidate the voting data at a central level or multiple levels. These requirements also address the generation and maintenance of audit records, the detection and disabling of improper use or operation of the system, and the monitoring of overall system status. Separate and distinct requirements for paper-based and DRE voting systems are presented below.

4.1.6.1 Paper-based System Processing Requirements

The paper-based processing requirements address all mechanical devices, electromechanical devices, electronic devices, and software required to perform the logical and numerical functions of interpreting the electronic image of the voted ballot, and assigning votes to the proper memory registers.

a. The ability of the system to produce and receive electronic signals from the scanning of the ballot, perform logical and numerical operations upon these data, and reproduce the contents of memory when required **shall** be sufficiently free of error to enable satisfaction of the system-level accuracy requirement indicated in Subsection 4.1.1.
b. Paper-based system memory devices, used to retain control programs and data, **shall** have demonstrated error-free data retention for a period of 22 months, under the environmental conditions for operation and non-operation (i.e., storage).

4.1.6.2 DRE System Processing Requirements

The DRE voting systems processing requirements address all mechanical devices, electromechanical devices, electronic devices, and software required to process voting data after the polls are closed.

a. DRE voting systems **shall** meet the following requirements for processing speed:
    i. Operate at a speed sufficient to respond to any operator input without perceptible delay (no more than three seconds). Processing speed requirements for response to voter input are in Section 3.2.6.1.
    ii. If the consolidation of polling place data is done locally, perform this consolidation in a time not to exceed five minutes for each device in the polling place
b. Processing accuracy is defined as the ability of the system to process voting data stored in DRE voting devices or in removable memory modules installed in such devices. Processing includes all operations to consolidate voting data after the polls have been closed. DRE voting systems **shall**:
    i. Produce reports that are completely consistent, with no discrepancy among reports of voting device data produced at any level
    ii. Produce consolidated reports containing absentee, provisional or other voting data that are similarly error-free. Any discrepancy, regardless of source, is resolvable to a procedural error, to the failure of a non-memory device or to an external cause
c. DRE system memory devices used to retain control programs and data **shall** have demonstrated error-free data retention for a period of 22 months. Error-free retention may be achieved by the use of redundant memory elements, provided that the capability for conflict resolution or correction among elements is included.

4.1.7 Reporting Requirements

The reporting requirements govern all mechanical, electromechanical, and electronic devices required for voting systems to print audit record entries and results of the tabulation. These requirements also address data storage media for transportation of data to other sites.

4.1.7.1 Removable Storage Media

In voting systems that use storage media that can be removed from the system and transported to another location for readout and report generation, these media **shall** use devices with demonstrated error-free retention for a period of 22 months under the environmental conditions for operation and non-operation contained in Subsection 4.1.2. Examples of removable storage media include: programmable read-only memory (PROM), random access memory (RAM) with battery backup, magnetic media or optical media.

4.1.7.2 Printers

All printers used to produce reports of the vote count **shall** be capable of producing:

a. Alphanumeric headers
b. Election, office and issue labels
c. Alphanumeric entries generated as part of the audit record

4.1.8 Vote Data Management Requirements

The vote data management requirements for all systems address capabilities that manage, process, and report voting data after the data has been consolidated at the polling place or other jurisdictional levels.

These capabilities allow the system to:

- Consolidate voting data from polling place data memory or transfer devices
- Report polling place summaries
- Process absentee ballots, data entered manually, and administrative ballot definition data

The requirements address all hardware and software required to generate output reports in the various formats required by the using jurisdiction.

4.1.8.1 Data File Management

All voting systems **shall** provide the capability to:

a. Integrate voting data files with ballot definition files
b. Verify file compatibility
c. Edit and update files as required

4.1.8.2 Data Report Generation

All voting systems **shall** include report generators for producing output reports at the device, polling place, and summary level, with provisions for administrative and judicial subdivisions as required by the using jurisdiction.

4.2 Physical Characteristics

This subsection covers physical characteristics of all voting systems and components that affect their general utility and suitability for election operations.

4.2.1 Size

There is no numerical limitation on the size of any voting equipment, but the size of each voting machine should be compatible with its intended use and the location at which the equipment is to be used.

4.2.2 Weight

There is no numerical limitation on the weight of any voting equipment, but the weight of each voting machine should be compatible with its intended use and the location at which the equipment is to be used.

4.2.3 Transport and Storage of Precinct Systems

All precinct voting systems **shall**:

a. Provide a means to safely and easily handle, transport, and install voting equipment, such as wheels or a handle or handles
b. Be capable of using, or be provided with, a protective enclosure rendering the equipment capable of withstanding:
    i. Impact, shock and vibration loads associated with surface and air transportation

ii. Stacking loads associated with storage

4.3 Design, Construction, and Maintenance Characteristics

This subsection covers voting system materials, construction workmanship, and specific design characteristics important to the successful operation and efficient maintenance of the voting system.

4.3.1 Materials, Processes, and Parts

The approach to system design is unrestricted, and may incorporate any form or variant of technology capable of meeting the voting systems requirements and standards.

Precinct count systems **shall** be designed in accordance with best commercial practice for microcomputers, process controllers, and their peripheral components. Central count voting systems and equipment used in a central tabulating environment **shall** be designed in accordance with best commercial and industrial practice.

All voting systems **shall**:

a. Be designed and constructed so that the frequency of equipment malfunctions and maintenance requirements are consistent with the reliability requirements of Section 4.3.3 and are furthermore reduced to the lowest levels consistent with cost constraints
b. Include, as part of the accompanying Technical Data Package, an approved parts list
c. Exclude parts or components not included in the approved parts list

4.3.2 Durability

All voting systems **shall** be designed to withstand normal use without deterioration and without excessive maintenance cost for a period of ten years.

4.3.3 Reliability

4.3.3.1 Terms

The following terms are used as defined in Appendix A: failure, critical failure, user-serviceable failure, non-user-serviceable failure.

4.3.3.2 Use case (informative)

The August 31, 2007 draft of VVSG Recommendations to the EAC included a detailed use case in the derivation of benchmarks that were expressed in terms of failures per unit of volume. Failures were divided into three categories: user-serviceable, non-user-serviceable, and "disenfranchisement." "Disenfranchisement," defined as any failure that results in all cast vote records pertaining to a given ballot becoming unusable or that makes it impossible to determine whether or not a ballot was cast, was assigned a benchmark of zero (i.e., can't happen). For the other two categories, limits were determined for the number of such failures that would be tolerated in an election (e.g., by substituting spare equipment), and benchmarks were derived based on a 1 % risk of exceeding those limits.

The following table summarizes significant estimates derived from the VVSG Recommendations use case. The estimates for accessible voting stations (Acc-VS) have been adjusted to reflect the fact that Acc-VS may be deployed at the rate of one per polling place in jurisdictions where the remainder of the voting volume is handled with manually-marked paper ballots, resulting in more stringent reliability requirements for the Acc-VS. (The VVSG Recommendations instead assumed that they would always be deployed in numbers sufficient for all voters to use them, which has not been the case.)

Device class	Population including spares	Manageable number of non-user-serviceable failures	Manageable number of user-serviceable failures
EMS	1	0	2
Central tabulator	9	1	N/A
Precinct tabulator	61	1	3
Accessible voting station (Acc-VS)	61	1	3
Other electronic vote-capture device	606	6	18
Activation device	61	1	N/A
Activation media/token (e.g. smart card)	1236	36	N/A

4.3.3.3 Basis of requirements (informative)

Benchmarks in the next section are derived from the VVSG Recommendations use case. Specific benchmarks cannot be reused from the VVSG Recommendations because the metric has changed from failures per unit of volume to the probability of failure in an election.

Manufacturers are now required to apply best practices to assure reliability. In the manufacturer's reliability analysis, each specific, individual, identified failure mode would be assigned a probability, and the system probability of failure would then be derived mathematically. As a trivial example, if a device has only two failure modes,

each has probability 0.01 of occurring, and they are independent of one another, the probability of failure is $1 - 0.99^2 = 0.0199$. Since the underlying probabilities are likely to depend on the volume that a device is expected to handle in the course of the election, minimum values for the assumed volume per device per election, from Table 6-1 of the VVSG Recommendations, are specified in a requirement.

The category of critical failures is used in lieu of "disenfranchisement." It is not possible for a reliability analysis to yield a failure probability of zero, so for the critical failures benchmark, a "very low" probability (10^{-6}) is used instead. (Note that probabilities on the order of 10^{-9} are used in civil aviation.)

For other benchmarks, the VVSG Recommendations' 1 % level of risk for exceeding the manageable number of failures is retained. Given N devices, each with independent probability of failure p, the probability of n or more of them failing in the same election is given by the Binomial probability sum

$$P = \sum_{x=n}^{N} \binom{N}{x} p^x (1-p)^{N-x} \quad \texttt{= 1-binocdf(n-1,N,p)}$$

Determining values of p that limit P to 1 % for each combination of n and N in the previous table is straightforward except for EMS. Tolerance of multiple failures per election per EMS cannot be expressed in the terms of the metric used here. Instead, the benchmark is set to the value such that, if there were two EMSs, the probability of both of them failing in a given election would be 1 %.

Since the types of failures identified form a hierarchy of impact—i.e., a non-user-serviceable failure automatically causes as much trouble as a user-serviceable failure, and then some—additive probabilities are used for the lower-rank benchmarks. Using this approach, the meaningless question of whether a critical failure is user-serviceable or not has no impact on the results and need never arise.

4.3.3.4 Requirements

a. The manufacturer **shall** assure the reliability of the voting system by applying best reliability engineering practices and standard reliability analysis methods such as failure modes and effects analysis (FMEA).
b. Letting F_C be the set of critical failure modes, F_N the set of non-user-serviceable failure modes, and F_S the set of user-serviceable failure modes, voting devices **shall** satisfy the following limits on the probabilities of failures (per election):

Device class	**Probability of critical failure** (F_C)	**Probability of critical or non-user-serviceable failure**	**Probability of failure** ($F_C \cup F_N \cup F_S$)

		$(F_C \cup F_N)$	
EMS or election results reporting device	$\leq 10^{-6}$	$\leq 10^{-6}$	≤ 0.1
Central tabulator	$\leq 10^{-6}$	≤ 0.01735	≤ 0.01735
Precinct tabulator	$\leq 10^{-6}$	≤ 0.002452	≤ 0.01374
Accessible voting station (Acc-VS)	$\leq 10^{-6}$	≤ 0.002452	≤ 0.01374
Other electronic vote-capture device	$\leq 10^{-6}$	≤ 0.003856	≤ 0.01718
Activation device	$\leq 10^{-6}$	≤ 0.002452	≤ 0.002452
Activation media/token (e.g. smart card)	$\leq 10^{-6}$	≤ 0.01978	≤ 0.01978

c. In calculating the probabilities of failures, the assumed volume per device per election **shall** be no less than the maximum tabulation rate times 8 hours for a central tabulator, 2000 ballots for a precinct tabulator, 2000 ballot activations for an activation device, 480 transactions for an EMS, 70 voting sessions for an EBM, or 200 voting sessions for any other electronic vote-capture device (including DREs).
d. If a voting device combines functions of more than one of the device classes listed in the previous requirements, such as a DRE that also accumulates and reports election results uploaded from other devices, its performance of these different functions **shall** satisfy the respective benchmarks. In the event that two different benchmarks would apply to the same function, the more stringent benchmark (lower probability, higher volume) **shall** prevail.

4.3.4 Product Marking

All voting systems **shall**:

a. Display on each device a separate data plate containing a schedule for and list of operations required to service or to perform preventive maintenance
b. 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

4.3.5 Workmanship

To help ensure proper workmanship, all manufacturers of voting systems **shall**:

a. Adopt and adhere to practices and procedures to ensure that their products are free from damage or defect that could make them unsatisfactory for their intended purpose
b. Ensure that components provided by external suppliers are free from damage or defect that could make them unsatisfactory for their intended purpose

4.3.6 Safety

All voting systems **shall** meet the following requirements for safety:

a. All voting systems and their components **shall** be designed to eliminate hazards to personnel or to the equipment itself
b. Defects in design and construction that can result in personal injury or equipment damage must be detected and corrected before voting systems and components are placed into service
c. Equipment design for personnel safety **shall** be equal to or better than the appropriate requirements of the Occupational Safety and Health Act, Code of Federal Regulations, Title 29, Part 1910

In order to meet these safety requirements, voting system manufacturers **shall** submit their systems for review to a Nationally Recognized Testing Laboratory (NRTL.)[15]

> Discussion: NRTL laboratories are specifically accredited by OSHA to identify relevant safety standards for a product and to conduct testing that ensures specific products meet the requirements of the product safety standards identified. Although this standard does not require that a voting system carry a Product Safety Listing (Label), voting system manufacturers may voluntarily choose to implement such labeling in order to meet such requirements implemented by State or local election jurisdictions. EAC accredited VSTLs remain responsible for non-core testing performed by third party laboratories as noted in Section 2.10.4.3 of the EAC Voting System Test Laboratory Program Manual, Version 1.0

15 The italicized text in Section 4.3.8 is based on EAC Decision on the Request for Interpretation 2008-09, http://www.eac.gov/assets/1/Page/EAC%20Decision%20on%20Safety%20Testing.pdf.

5 Software Requirements

Table of Contents

5 Software Requirements

5.1 Software Configuration

Configuration of software, both operating systems and applications, is critical to proper system functioning. Correct test design and sufficient test execution must account for the intended and proper configuration of all system components. Therefore, the manufacturers **shall** submit a record of all user selections made during software installation as part of the Technical Data Package. The manufacturer **shall** also submit a record of all configuration changes made to the software following its installation. The VSTL **shall** confirm the propriety and correctness of these user selections and configuration changes.

5.2 Software Design and Coding Standards

This section describes essential design and performance characteristics of the logic used in voting systems. The requirements of this section are intended to ensure that voting system logic is reliable, robust, testable, and maintainable.

The general requirements of this section apply to logic used to support the entire range of voting system activities. Although this section emphasizes software, the standards described also influence hardware design considerations.

While there is no best way to design logic, the use of outdated and ad hoc practices is a risk factor for unreliability, unmaintainability, etc. Consequently, these guidelines require the use of modern programming practices. The use of widely recognized and proven logic design methods will facilitate the analysis and testing of voting system logic.

5.2.1 Scope

The terms *application logic, border logic, third-party logic, configuration data,* and *COTS* are defined in Appendix A and are used carefully in this section to specify the applicability of requirements.

The requirements of this section that constrain programming practices—design requirements—apply to all application logic, regardless of the ownership of the logic or the ownership and location of the hardware on which the logic is installed or operates. Although it would be desirable for COTS software to conform to the design requirements on software workmanship, its conformity to those requirements could not be assessed without access to the source code; hence, the design requirements are scoped to exclude

COTS software. In contrast, requirements that can be tested without access to source code, such as the requirement to detect and respond to invalid input without crashing (5.2.8.a), apply to COTS software in exactly the same way as they apply to non-COTS software.

Regardless of its source, software, firmware, or hardwired logic that has been modified for use in voting systems or has no application other than in voting systems **shall not** be deemed COTS.

Third-party logic, border logic, and configuration data are not required to conform to the design requirements on software workmanship, but manufacturers **shall** supply that source code and data to the VSTL to enable a complete review of the application logic.

Notably, the distinction between software, firmware, and hardwired logic does not impact the level of scrutiny that a component receives; nor are the requirements applying to application logic relaxed in any way if that logic is realized in firmware or hardwired logic instead of software.

The following table summarizes the scoping considerations for software requirements and testing.

CATEGORIES	LEVEL OF SCRUTINY	TESTED?	SOURCE CODE/DATA REQUIRED?	CODING STANDARDS ENFORCED?
COTS	Black-box	Yes	No	No
third-party logic, border logic, configuration data	White-box	Yes	Yes	No
application logic	Coding standards	Yes	Yes	Yes

5.2.2 Selection of programming languages

Application logic **shall** be produced in a high-level programming language that has all of the following control constructs:

a. Sequence;
b. Loop with exit condition (e.g., for, while, do-loops, and/or foreach);
c. If/Then/Else conditional;
d. Case conditional; and
e. Block-structured exception handling (e.g., try/throw/catch).

The intent of this requirement is clarified in Volume I Section 5.2.5 with discussion and examples of specific programming languages.

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, e.g. by wrapping it in callable units expressed in the prevailing language, to minimize the number of places that special code appears. C.f. MISRA-C:2004[16] Rule 2.1: "Assembly language **shall** be encapsulated and isolated."

Acceptable programming languages are also constrained by Requirements 5.2.7.a.iii and iv, which effectively prohibit the invention of new languages.

The above requirement may be satisfied by using COTS extension packages to add missing control constructs to languages that could not otherwise conform. For example, C11[17] does not support block-structured exception handling, but the construct can be retrofitted using (e.g.) cexcept[18] or another COTS package.

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 VSTL 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.

5.2.3 Selection of general coding standard

Note: The requirements of this section attempt to clarify the "published, reviewed, and industry-accepted" language appearing in previous iterations of the Guidelines, but the intent of the requirements is unchanged.

Application logic **shall** adhere to a published, credible set of coding rules, conventions or standards (herein simply called the "coding standard") that enhance the workmanship, security, integrity, testability, and maintainability of applications. Coding standards that are excessively specialized or simply inadequate may be rejected on the grounds that they do not enhance one or more of workmanship, security, integrity, testability, and maintainability.

Coding standards **shall** be considered published if and only 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. Following are examples of

16 MISRA-C:2004: Guidelines for the use of the C language in critical systems, MIRA Limited, U.K., 2004-10.
17 ISO/IEC 9899:2011, Programming languages—C. Available from ISO, http://www.iso.org/.
18 CEXCEPT (exception handling in C), software package, 2000. Available at http://cexcept.sourceforge.net/.

published coding standards (links valid as of 2012-04-05). These are only examples and are not necessarily the best available for the purpose.

> **Ada:** Ada Quality and Style Guide; Guidelines for Professional Programmers. http://en.wikibooks.org/wiki/Ada_Style_Guide
>
> **C++:** Mats Henricson and Erik Nyquist, Industrial Strength C++, Prentice-Hall, 1997. Content available at http://hem.passagen.se/erinyq/industrial/.
>
> **C#:** "Design Guidelines for Developing Class Libraries," Microsoft. http://msdn.microsoft.com/en-us/library/ms229042.aspx.
>
> **Java:** "Code Conventions for the Java™ Programming Language," Sun Microsystems. http://www.oracle.com/technetwork/java/codeconv-138413.html

Coding standards **shall** be considered credible if and only 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 time within the three years before conformity assessment was first sought.

Coding standards evolve, and it is desirable for voting systems to be aligned with modern practices. If the "three year rule" was satisfied at the time that a system was first submitted for testing, it is considered satisfied for the purpose of subsequent reassessments of that system. However, new systems must meet the three year rule as of the time that they are first submitted for testing, even if they reuse parts of older systems.

5.2.4 Software modularity and programming

a. Application logic **shall** be designed in a modular fashion. Each module **shall** have a specific function that can be tested and verified independently of the remainder of the code. In practice, some additional modules (such as library modules) may be needed to compile the module under test, but the modular construction allows the supporting modules to be replaced by special test versions that support test objectives.
b. Callable units **shall** have cyclomatic complexity[19] less than 20.

5.2.5 Structured programming

Specific programming languages are identified to support the discussion. In no case does such identification imply recommendation or endorsement, nor does it imply that the programming languages identified are necessarily the best or only languages acceptable for voting system use.

19 T. McCabe, "A Complexity Measure," IEEE Transactions on Software Engineering Vol. SE-2, No. 4, pp. 308-320 (December 1976).

Concept	VSS[20],[21] / VVSG[22]	Ada[23],[24]	C[25],[26]	C++[27],[28]	C#[29],[30]	Java[31],[32]	Visual Basic 2005 (VB 8.0)[33]
Sequence	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Loop with exit condition	Yes	Yes	Yes	Yes	Yes	Yes	Yes
If/Then/Else conditional	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Case conditional	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Named block exit	No	Yes	No	No	No	Yes	No[34]
Block-structured exception handling	No	Yes	No	Yes	Yes	Yes	Yes

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

Prominent among the requirements addressing logical transparency is the requirement to use high-level control constructs and to refrain from using the low-level arbitrary branch (a.k.a. goto). As is reflected in the above table, most high-level concepts for control flow were established by the time the first edition of the Guidelines was published and are supported by all of the programming languages that were examined as probable

---

20 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. Available at http://josephhall.org/fec_vss_1990_pdf/1990_VSS.pdf.
21 2002 Voting Systems Standards, available from http://www.eac.gov/testing_and_certification/voluntary_voting_system_guidelines.aspx.
22 2005 Voluntary Voting System Guidelines, Version 1.0, 2006-03-06, available from http://www.eac.gov/testing_and_certification/voluntary_voting_system_guidelines.aspx.
23 ISO/IEC 8652:1987, Programming languages—Ada.
24 ISO/IEC 8652:1995, Information technology—Programming languages—Ada. Available from ISO, http://www.iso.org/.
25 ISO/IEC 9899:1990, Programming languages—C.
26 ISO/IEC 9899:1999, Programming languages—C. Available from ISO, http://www.iso.org/.
27 ISO/IEC 14882:1998, Programming languages—C++.
28 ISO/IEC 14882:2003, Programming languages—C++. Available from ISO, http://www.iso.org/.
29 ISO/IEC 23270:2003, Information technology—C# language specification.
30 ISO/IEC 23270:2006, Information technology—Programming languages—C#. Available from ISO, http://www.iso.org/.
31 The Java Language Specification, Third Edition, 2005. Available at http://docs.oracle.com/javase/specs.
32 The Java Language Specification, Java SE 7 Edition, 2011. Available at http://docs.oracle.com/javase/specs.
33 Paul Vick, The Microsoft® Visual Basic® Language Specification, Version 8.0, 2005. Available from Microsoft Download Center, http://go.microsoft.com/fwlink/?linkid=62990.
34 Visual Basic 8 does not support named block exit, but it does support specifying the kind of block (do loop, for loop, while loop, select, subroutine, function, etc.) from which to exit, which need not be the innermost block.

candidates for voting system use as of this iteration. However, two additional concepts have been slower to gain universal support.

The first additional concept, called here the "named block exit," is the ability to exit a specific block from within an arbitrary number of nested blocks, as opposed to only being able to exit the innermost block, without resorting to goto. The absence of named block exit from some languages is not cause for concern here because deeply nested blocks are themselves detrimental to the transparency of logic and most coding standards encourage restructuring them into separate callable units.

The second additional concept, called here "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).[35]) 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."[36]

Previous Guidelines required voting systems to handle such errors by some means, preferably using programming language exceptions (2005 VVSG 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 for. Additionally, these Guidelines require block-structured exception handling because, like all unstructured programming, unstructured exception handling obfuscates logic and makes its verification by the VSTL 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."[37]

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 a below).

---

35 Matt Pietrek, "A Crash Course on the Depths of Win32™ Structured Exception Handling," Microsoft Systems Journal, 1997-01. Available at http://www.microsoft.com/msj/0197/exception/exception.aspx.
36 ISO/IEC TR 15942:2000, Information technology—Programming languages—Guide for the use of the Ada programming language in high integrity systems. Available from ISO, http://www.iso.org/.
37 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.

a. Application logic **shall** handle exceptions using block-structured exception handling constructs. 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 **shall** be wrapped in callable units that check for the relevant error conditions and translate them into exceptions, and the remainder of application logic **shall** use only the wrapped version. For example, if an application written in C99 + cexcept used the malloc function of libc, which returns a null pointer in case of failure instead of throwing an exception, the malloc function would need to be wrapped. Here is one possible implementation:

```
void *checkedMalloc (size_t size) {
  void *ptr = malloc (size);
  if (!ptr)
    Throw bad_alloc;
  return ptr;
}
#define malloc checkedMalloc
```

Wrapping legacy functions avoids the need to check for errors after every invocation, which both obfuscates the application logic and creates a high likelihood that some or many possible errors will not be checked for.

In C++, it would be preferable to use one of the newer mechanisms that already throw exceptions on failure and avoid use of legacy functions altogether.

b. Application logic **shall** contain no unstructured control constructs.
   i. Arbitrary branches (a.k.a. gotos) are prohibited.
   ii. Exceptions **shall** only be used for abnormal conditions. Exceptions **shall** not be used to redirect the flow of control in normal ("non-exceptional") conditions. "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.
   iii. Unstructured exception handling (e.g., On Error GoTo, setjmp/longjmp, or explicit tests for error conditions after every executable statement) is prohibited. 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 a, is allowed. Analogously, 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.

c. Application logic **shall** not compile or interpret configuration data or other input data as a programming language. 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: it is permissible for configuration data to contain a template that

informs a report generating application as to the form and content of a report that it should generate, but it is not permissible for configuration data to 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 (1) mingling code and data is bad design, and (2) embedding logic within configuration data is an evasion of the conformity assessment process for application logic.

5.2.6 Header comments

Header comments and other commenting standards should be specified by the selected coding standard in a manner consistent with the idiom of the programming language chosen. If the coding standard specifies a coding style and commenting standard that make header comments redundant, then they may be omitted. Otherwise, in the event that the coding standard fails to specify the content of header comments, application logic modules should include header comments that provide at least the following information for each callable unit (function, method, operation, subroutine, procedure, etc.):

a. The purpose of the unit and how it works (if not obvious);
b. A description of input parameters, outputs and return values, exceptions thrown, and side-effects;
c. Any protocols that must be observed (e.g., unit calling sequences);
d. File references by name and method of access (read, write, modify, append, etc.);
e. Global variables used (if applicable);
f. Audit event generation;
g. Date of creation; and
h. Change log (revision record). Change logs need not cover the nascent period, but they must go back as far as the first baseline or release that is submitted for testing, and should go back as far as the first baseline or release that is deemed reasonably coherent.

5.2.7 Executable code and data integrity[38]

a. Subrequirements i through iv apply to application logic (and only to application logic):
    i. Self-modifying code is prohibited.
    ii. Application logic **shall** be free of race conditions, deadlocks, livelocks, and resource starvation.

38 Portions of this section are derived from Section 5.6.2.2 of IEEE Draft Standard for the Evaluation of Voting Equipment, draft P1583/D5.3.2b, 2005-01-04. This material is from an unapproved draft of a proposed IEEE Standard, P1583. As such, the material is subject to change in the final standard. Because this material is from an unapproved draft, the IEEE recommends that it not be utilized for any conformance/compliance purposes. It is used at your own risk.

iii. If compiled code is used, it **shall** only be compiled using a COTS compiler. This prohibits the use of arbitrary, nonstandard compilers and consequently the invention of new programming languages.
iv. If interpreted code is used, it **shall** only be run under a specific, identified version of a COTS runtime interpreter. This ensures (1) that no arbitrary, nonstandard interpreted languages are used, and (2) that the software tested and approved during the conformity assessment process does not change behavior because of a change to the interpreter.

b. All programmed devices **shall** prevent replacement or modification of executable or interpreted code (e.g., 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 prepare authorized software and equipment for use. This requirement may be partially satisfied through a combination of read-only memory (ROM), the memory protection implemented by most popular COTS operating systems, error checking as described in Volume I Section 5.2.8, and access and integrity controls.
c. All voting devices **shall** prevent access to or manipulation of configuration data, vote data or audit records (e.g., by physical 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. This requirement may be partially satisfied through a combination of the memory protection implemented by most popular COTS operating systems, error checking as described in Volume I Section 5.2.8, and access and integrity controls. Systems using mechanical counters to store vote data must protect the counters from tampering. If vote data are stored on paper, the paper must be protected from tampering. Modification of audit records after they are created is never necessary.
d. All programmed devices **shall** provide the capability to monitor the transfer quality of I/O operations, reporting the number and types of errors that occur and how they were corrected.
e. Application logic and border logic **shall** contain no inaccessible code (dead code) other than defensive code (including exception handlers) that is provided to defend against the occurrence of failures and “can't happen” conditions.

5.2.8 Error checking[39]

This section contains requirements for application logic to avoid, detect, and prevent well-known types of errors that could compromise voting integrity and security. Additional advice from the security perspective is available at the CERT® Coordination Center, Secure Coding homepage, http://www.cert.org/secure-coding/, and related sites, esp. Department of Homeland Security, Build Security In homepage, https://buildsecurityin.us-cert.gov/.

39 Portions of this section are derived from Sections 5.6.2.2 and 6.6.4.2 of IEEE Draft Standard for the Evaluation of Voting Equipment, draft P1583/D5.3.2b, 2005-01-04. This material is from an unapproved draft of a proposed IEEE Standard, P1583. As such, the material is subject to change in the final standard. Because this material is from an unapproved draft, the IEEE recommends that it not be utilized for any conformance/compliance purposes. It is used at your own risk.

a. All programmed devices **shall** check information inputs, whether from manual entry or other external source, for completeness and validity and ensure that incomplete or invalid inputs do not lead to irreversible error.
   i. At any point where it is possible for a user (voter, poll worker, etc.) to enter a scalar or enumerated type value that is outside the range of values that is valid in the context of the device's logic, that input **shall** be range-checked. This applies to inputs of values of numeric types, character types, temporal types, and any other types for which the concept of range is well-defined.
   ii. At any point where it is possible for a user to enter a character string or list of values that is longer than the maximum or shorter than the minimum length that is valid in the context of the device's logic, that input **shall** be length-checked.
   iii. The device **shall** respond to an invalid input by notifying the user of the error and enabling the user to correct the erroneous input before consequential errors and/or loss of program integrity occur.

b. All application logic that is vulnerable to the following types of errors **shall** check for these errors at run time and respond defensively (as specified by Requirement f) when they occur: (1) out-of-bounds accesses of arrays or strings (includes buffers used to move data); (2) stack overflow errors; (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 overflows; (6) known programming language specific vulnerabilities.
   i. 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 **shall** be ranged-checked on every access. Range checking code should not be duplicated before each access. Clean implementation approaches include: (1) consistently using dedicated accessors (functions, methods, operations, subroutines, procedures, etc.) that range-check the indices; (2) defining and consistently using a new data type or class that encapsulates the range-checking logic; (3) declaring the array using a template that causes all accessors to be range-checked; or (4) 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 may be provided by the programming environment or they may be defined in application logic. If acceptable values of the index do not form a contiguous range, a map structure may be more appropriate than a vector.
   ii. If stack overflow does not automatically result in an exception, the application logic **shall** explicitly check for and prevent stack overflow. Embedded system developers use a variety of techniques for avoiding stack overflow. Commonly, the stack is monitored and warnings and exceptions are thrown when thresholds are crossed. In non-embedded contexts, stack overflow often manifests as a CPU-level exception related to memory segmentation, in which case it can be handled pursuant to Requirement b.iii.
   iii. The application logic **shall** implement such handlers as are needed to detect and respond to CPU-level exceptions. 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.

iv. All scalar or enumerated type parameters whose valid ranges as used in a callable unit (function, method, operation, subroutine, procedure, etc.) do not cover the entire ranges of their declared data types **shall** be range-checked on entry to the unit. 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 and/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 differs from Requirement a. Requirement a deals with user input, which is expected to contain errors, while this requirement deals with program internal parameters, which are expected to conform to the expectations of the designer. User input errors are a normal occurrence; the errors discussed here are grounds for throwing exceptions.

v. 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 **shall** be checked for overflow. This requirement should be approached in a manner similar to Requirement b.i. Overflow checking should be encapsulated as much as possible.

c. All application logic that is vulnerable to the following types of errors should check for these errors at run time and respond defensively (as specified by Requirement f) when they occur: (1) pointer variable errors; (2) dynamic memory allocation and management errors.

   i. If application logic uses pointers or a similar mechanism for specifying absolute memory locations, the application logic should validate pointers or addresses before they are used. Improper overwriting should be prevented in general as required by Requirements 5.2.7.b and c. Nevertheless, 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.

d. Application logic should be instrumented and/or analyzed with a COTS tool for detecting the kinds of errors enumerated in requirements b and c above.

e. If pointers are used, any pointer variables that remain within scope after the memory they point to is deallocated **shall** be set to null or marked as invalid (pursuant to the idiom of the programming language used) after the memory they point to is deallocated. 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::unique_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.

f. The detection of any of the errors enumerated in Requirements b and c **shall** be treated as a complete failure of the callable unit in which the error was detected. An appropriate exception **shall** be thrown and control **shall** pass out of the unit forthwith.

g. Error checks detailed in Requirements b and c **shall** remain active in production code. These errors are incompatible with voting integrity, so masking them is unacceptable. Manufacturers should not implement error checks using the C/C++ assert() macro. It is often disabled, sometimes automatically, when software is compiled in production mode. Furthermore, it does not appropriately throw an exception, but instead aborts the program.
h. Exceptions resulting from failed error checks or CPU-level exceptions **shall** require intervention by an election official or administrator before voting can continue. These errors are incompatible with voting integrity, so masking them is unacceptable.
i. Electronic devices **shall** include a means of identifying device failure and any corrective action needed.
j. Electronic devices should proactively detect equipment failures and alert an election official or administrator when they occur.
k. Electronic devices **shall** proactively detect or prevent basic violations of election integrity (e.g., stuffing of the ballot box or the accumulation of negative votes) and alert an election official or administrator if they occur. Equipment can verify only those conditions that are within the scope of what the equipment does. This provides defense-in-depth to supplement procedural controls and auditing practices.

5.3 Data and Document Retention

All systems **shall**:

a. Maintain the integrity of voting and audit data during an election, and for at least 22 months thereafter, a time sufficient to resolve most contested elections and support other activities related to the reconstruction and investigation of a contested election
b. Protect against the failure of any data input or storage device at a location controlled by the jurisdiction or its contractors, and against any attempt at improper data entry or retrieval

5.4 Audit Record Data

Audit trails are essential to ensure the integrity of a voting system. Operational requirements for audit trails are described in Subsection 2.1.5.1. Audit record data are generated by these procedures. The audit record data in the following subsections are essential to the complete recording of election operations and reporting of the vote tally. This list of audit records may not reflect the design constructs of some systems. Therefore, manufacturers **shall** supplement it with information relevant to the operation of their specific systems.

5.4.1 Pre-election Audit Records

During election definition and ballot preparation, the system **shall** audit the preparation of the baseline ballot formats and modifications to them, a description of these modifications, and corresponding dates.

The log **shall** include:

a. The allowable number of selections a contest
b. The combinations of voting patterns permitted or required by the jurisdiction
c. The inclusion or exclusion of contests as the result of multiple districting within the polling place
d. Any other characteristics that may be peculiar to the jurisdiction, the election or the polling place location
e. Manual data maintained by election personnel
f. Samples of all final ballot formats
g. Ballot preparation edit listings

5.4.2 System Readiness Audit Records

The following minimum requirements apply to system readiness audit records:

a. Prior to the start of ballot counting, a system process **shall** verify hardware and software status and generate a readiness audit record. This record **shall** include the identification of the software release, the identification of the election to be processed, and the results of software and hardware diagnostic tests
b. In the case of systems used at the polling place, the record **shall** include polling place identification
c. The ballot interpretation logic **shall** test and record the correct installation of ballot formats on voting devices
d. The software **shall** check and record the status of all data paths and memory locations to be used in vote recording to protect against contamination of voting data
e. Upon the conclusion of the tests, the software **shall** provide evidence in the audit record that the test data have been expunged
f. If required and provided, the ballot reader and arithmetic-logic unit **shall** be evaluated for accuracy, and the system **shall** record the results. It **shall** allow the processing or simulated processing of sufficient test ballots to provide a statistical estimate of processing accuracy
g. For systems that use a public network, provide a report of test ballots that includes:
    i. Number of ballots sent
    ii. When each ballot was sent
    iii. Machine from which each ballot was sent
    iv. Specific votes or selections contained in the ballot

5.4.3 In-process Audit Records

In-process audit records document system operations during diagnostic routines and the casting and tallying of ballots. At a minimum, the in-process audit records **shall** contain:

a. Machine generated error and exception messages to demonstrate successful recovery. Examples include, but are not necessarily limited to:
    i. The source and disposition of system interrupts resulting in entry into exception handling routines
    ii. All messages generated by exception handlers
    iii. The identification code and number of occurrences for each hardware and software error or failure
    iv. Notification of system login or access errors, file access errors, and physical violations of security as they occur, and a summary record of these events after processing
    v. Other exception events such as power failures, failure of critical hardware components, data transmission errors or other types of operating anomalies
b. Critical system status messages other than informational messages displayed by the system during the course of normal operations. These items include, but are not limited to:
    i. Diagnostic and status messages upon startup
    ii. The “zero totals” check conducted before opening the polling place or counting a precinct centrally
    iii. For paper-based systems, the initiation or termination of optical scanner and communications equipment operation
    iv. For DRE machines at controlled voting locations, the event (and time, if available) of activating and casting each ballot (i.e., each voter's transaction as an event). This data can be compared with the public counter for reconciliation purposes
c. Non-critical status messages that are generated by the machine's data quality monitor or by software and hardware condition monitors
d. System generated log of all normal process activity and system events that require operator intervention, so that each operator access can be monitored and access sequence can be constructed

5.4.4 Vote Tally Data

In addition to the audit requirements described above, other election-related data is essential for reporting results to interested parties, the press, and the voting public, and is vital to verifying an accurate count.

Voting systems **shall** meet these reporting requirements by providing software capable of obtaining data concerning various aspects of vote counting and producing printed reports. At a minimum, vote tally data **shall** include:

a. Number of ballots cast, using each ballot configuration, by tabulator, by precinct, and by political subdivision

b. Candidate and measure vote totals for each contest, by tabulator
c. The number of ballots read within each precinct and for additional jurisdictional levels, by configuration, including separate totals for each party in primary elections
d. Separate accumulation of overvotes and undervotes for each contest, by tabulator, precinct and for additional jurisdictional levels (no overvotes would be indicated for DRE voting devices)
e. For paper-based systems only, the total number of ballots both able to be processed and unable to be processed; and if there are multiple card ballots, the total number of cards read

For systems that produce an electronic file containing vote tally data, the contents of the file **shall** include the same minimum data cited above for printed vote tally reports.

5.5 Vote Secrecy on DRE and EBM Systems

All DRE and EBM systems **shall** ensure vote secrecy by,

a. Immediately after the ballot is recorded to persistent electronic storage or printed, erasing the selections from the device's display, working memory, and all other storage, including all forms of temporary storage
b. Immediately after the voter chooses to cancel his or her ballot, erasing the selections from the display and all other storage, including buffers and other temporary storage

6 Telecommunications Requirements

Table of Contents

6 Telecommunications Requirements

6.1 Scope

This section contains the performance, design, and maintenance characteristics of the telecommunications components of voting systems and the acceptable levels of performance against these characteristics. For the purpose of the *Guidelines*, telecommunications is defined as the capability to transmit and receive data electronically using hardware and software components over distances both within and external to a polling place.

The requirements in this section represent acceptable levels of combined telecommunications hardware and software function and performance for the transmission of data that is used to operate the system and report election results. Where applicable, this section specifies minimum values for critical performance and functional attributes involving telecommunications hardware and software components.

This section does not apply to other means of moving data, such as the physical transport of data recorded on paper-based media or the transport of physical devices, such as memory cards, that store data in electronic form.

Voting systems may include network hardware and software to transfer data among systems. Major network components are local area networks (LANs), wide area networks (WANs), workstations (desktop computers), servers, data, and applications. Workstations include voting stations, precinct tabulation systems, and voting supervisory terminals. Servers include systems that provide registration forms and ballots and accumulate and process voter registrations and cast ballots.

Desirable network characteristics include simplicity, flexibility (especially in routing, to maintain good response times) and maintainability (including availability, provided primarily through redundancy of resources and connections, particularly of connections to public infrastructure).

A wide area network (WAN) public telecommunications component consists of the hardware and software to transport information, over shared public (i.e., commercial or governmental) circuitry or among private systems. For voting systems, the telecommunications boundaries are defined as the transport circuitry, on one side of which exists the public telecommunications infrastructure, outside the control of voting system supervisors. On the other side of the transport circuitry are the local area network (LAN) resources, workstations, servers, data and applications controlled by voting system supervisors.

Local area network (LAN) components consist of the hardware and software infrastructure used to transport information between users in a local environment,

typically a building or group of buildings. Typically a LAN connects workstations with a local server.

An application may be a single program or a group of programs that work together to provide a function to an end user, who may be a voter or an election administrator. Voter programs may include voter registration, balloting, and status checking. Administrator programs may include ballot preparation, registration for preparation, registration approval, ballot vetting, ballot processing, and election processing.

This section is intended to complement the network security requirements found in Section 7, which include requirements for voter and administrator access, availability of network service, data confidentiality, and data integrity. Most importantly, security services must restrict access to local election system components from public resources, and these services must also restrict access to voting system data while it is in transit through public networks.

6.1.1 Types of Components

This section addresses telecommunications hardware and software across a broad range of technologies including, but not limited to:

- Dial-up communications technologies including standard landline, wireless, microwave, Very Small Aperture Terminal, Integrated Services Digital Network, Digital Subscriber Line
- Public and private high-speed telecommunications lines including FT-1, T-1, T-3; frame relay; private line
- Cabling technologies including Universal Twisted Pair cable (CAT 5 or higher) or Ethernet hub/switch
- Wireless including radio frequency and infrared
- Communications routers
- Modems, whether internal and external to personal computers, servers, and other voting system components installed at the polling place or central count location
- Modem drivers, dial-up networking software
- Channel service units and Data service units installed at the polling place or central count location
- Dial-up networking applications software

6.1.2 Telecommunications Operations and Providers

This section applies to voting-related transmissions over public networks, such as those provided by local distribution and long distance carriers. This section also applies to private networks regardless of whether the network is owned and operated by the election jurisdiction.

For systems that transmit official data over public networks, this section applies to telecommunications components installed and operated at locations supervised by election officials, such as polling places or central offices. This includes:

- Components acquired by the jurisdiction for the purpose of voting, including components installed at the polling place or a central office (including central site facilities operated by manufacturers or contractors)
- Components acquired by others (such as school systems, libraries, military installations and other public organizations) that are used at locations supervised by election officials, including minimum configuration components required by the manufacturer but that the manufacturer permits to be acquired from third party sources not under the manufacturer's control (e.g., router or modem card manufacturer or supplier)

6.1.3 Data Transmission

These requirements apply to the use of telecommunications to transmit data for the preparation of the system for an election, the execution of an election, and the preservation of the system data and audit trails during and following an election. While this section does not assume a specific model of voting system operations and does not assume a specific model for the use of telecommunications to support such operations, it does address the following types of data, where applicable:

Voter Authentication: Coded information that confirms the identity of a voter for security purposes for a system that transmits votes individually over a public network

Ballot Definition: Information that describes to a voting machine the content and appearance of the ballots to be used in an election

Vote Transmission to Central Site: For voting systems that transmit votes individually over a public network, the transmission of a vote or votes to the county (or contractor) for consolidation with other vote data

Vote Count: Information representing the tabulation of votes at any level within the control of the jurisdiction, such as the polling place, precinct or central count

List of Voters: A listing of the individual voters who have cast ballots in a specific election

Additional data transmissions used to operate a voting system in the conduct of an election, but not explicitly listed above, are also subject to the requirements of this section.

For systems that transmit data using public networks, this section applies to telecommunications hardware and software for transmissions within and among all combinations of senders and receivers located at polling places, precinct count facilities and central count facilities (whether operated by the jurisdiction or a contractor).

6.2 Design, Construction, and Maintenance Requirements

Design, construction, and maintenance requirements for telecommunications represent the operational capability of both system hardware and software. These capabilities **shall** be considered basic to all data transmissions.

6.2.1 Accuracy

The telecommunications components of all voting systems **shall** meet the accuracy requirements of Subsection 4.1.1.

6.2.2 Durability

The telecommunications components of all voting systems **shall** meet the durability requirements of Subsection 4.3.2.

6.2.3 Reliability

The telecommunications components of all voting systems **shall** meet the reliability requirements of Subsection 4.3.3.

6.2.4 Integrity

For WANs using public telecommunications, boundary definition and implementation **shall** meet the requirements below.

a. Outside service providers and subscribers of such providers **shall** not be given direct access or control of any resource inside the boundary.
b. Voting system administrators **shall** not require any type of control of resources outside this boundary. Typically, an end point of a telecommunications circuit will be a subscriber termination on a Digital Service Unit/Customer Service Unit although the specific technology configuration may vary. Regardless of the technology used, the boundary point must ensure that everything on the voting system side is locally configured and controlled by the election jurisdiction while everything on the public network side is controlled by an outside service provider.
c. The system **shall** be designed and configured such that it is not vulnerable to a single point of failure in the connection to the public network which could cause total loss of voting capabilities at any polling place.

6.2.5 Confirmation

Confirmation occurs when the system notifies the user of the successful or unsuccessful completion of the data transmission, where successful completion is defined as accurate receipt of the transmitted data. To provide confirmation, the telecommunications components of a voting system **shall** notify the user of the successful or unsuccessful completion of the data transmission. In the event of unsuccessful transmission the user **shall** be notified of the action to be taken.

7 Security Requirements

Table of Contents

7 Security Requirements

7.1 Scope

This section describes essential security capabilities for a voting system, encompassing the system's hardware, software, communications and documentation. No predefined set of security standards will address and defeat all conceivable or theoretical threats. The *Guidelines* articulate requirements to achieve acceptable levels of integrity and reliability. The objectives of the security standards for voting systems are:

- To protect critical elements of the voting system
- To establish and maintain controls to minimize errors
- To protect the system from intentional manipulation, fraud and malicious mischief
- To identify fraudulent or erroneous changes to the voting system
- To protect secrecy in the voting process

The *Voting System Performance Guidelines* (Volume I of the *VVSG*) are intended to address a broad range of risks to the integrity of a voting system. While it is not possible to identify all potential risks, Volume I identifies several types of risks that must be addressed. These include:

- Unauthorized changes to system capabilities for:
    - Defining ballot formats
    - Casting and recording votes
    - Calculating vote totals consistent with defined ballot formats
    - Reporting vote totals
- Alteration of voting system audit trails
- Changing, or preventing the recording of, a vote
- Introducing data for a vote not cast by a registered voter
- Changing calculated vote totals
- Preventing access to vote data--including individual votes and vote totals--by unauthorized individuals
- Preventing access to voter identification data and data for votes cast by the voter such that an individual can determine the content of specific votes

The requirements apply to the broad range of hardware, software, communications components, and documentation that comprises a voting system. These requirements apply to those components that are:

- Provided by the voting system manufacturer and the manufacturer's suppliers

- Furnished by an external provider (i.e., providers of personal computers and COTS operating systems) where the components are capable of being used during voting system operation
- Developed by a voting jurisdiction

The requirements apply to all software used in any manner to support any voting-related activity, regardless of the ownership of the software or the ownership and location of the hardware on which the software is installed or operated. These requirements apply to software that operates on:

- Voting devices and vote counting devices installed at polling places under the control or authority of the voting jurisdiction
- Ballot printers, vote counting devices, and other hardware typically installed at central or precinct locations (including contractor facilities)

7.1.1 Elements of Security Outside Manufacturer Control

The requirements of this section apply to the capabilities of a voting system that must be provided by the manufacturer. However, an effective security program requires well-defined security practices by the purchasing jurisdiction and the personnel managing and operating the system. These practices include:

- Administrative and management controls for the voting system and election management--including access controls
- Internal security procedures
- Adherence to, and enforcement of, operational procedures (e.g., effective password management)
- Security of physical facilities
- Organizational responsibilities and personnel screening

Because implementation of these elements is not under the control of the manufacturer, they are addressed in the Election Management Guidelines that describes the procedural aspects of conducting elections and managing the operation of voting systems. However, manufacturers must provide appropriate system capabilities to enable the implementation of management controls.

7.1.2 Organization of This Section

The guidelines presented in this section are organized as follows:

Access Control: These standards address procedures and system capabilities that limit or detect access to critical system components in order to guard against loss of system integrity, availability, confidentiality, and accountability.

Physical Security: These standards address physical security measures and procedures that prevent disruption of the voting process at the polling place and corruption of voting data.

Software Security: These standards address the installation of software, including firmware, in the voting system and the protection against malicious software. It should be noted that computer-generated audit controls facilitate system security and are an integral part of software capability. These audit requirements are presented in Subsection 5.4.

Telecommunications and Data Transmission: These standards address security for the electronic transmission of data between system components or locations over private, public, and wireless networks.

Use of Public Communications Networks: These standards address security for systems that communicate individual votes or vote totals over public communications networks.

Wireless Communications: These standards address the security of the voting system and voting data when wireless is used.

Independent Verification Systems: This section provides an introduction to the concept of independent verification as a method to demonstrate voting system integrity. This discussion provides the context for the requirements for DREs with voter verifiable paper audit trails.

Direct-Recording Electronic Systems with Voter Verifiable Paper Audit Trails (optional): This capability is not required for national certification. These guidelines are provided for use by states that require this feature for DRE systems.

7.2 Access Control

Access controls are procedures and system capabilities that detect or limit access to system components in order to guard against loss of system integrity, availability, confidentiality, and accountability. Access controls provide reasonable assurance that system resources such as data files, application programs, and computer-related facilities and equipment are protected against unauthorized operation, modification, disclosure, loss or impairment. Unauthorized operations include modification of compiled or interpreted code, run-time alteration of flow control logic or of data, and abstraction of raw or processed voting data in any form other than a standard output report by an authorized operator.

Access controls may include physical controls, such as keeping computers in locked rooms to limit physical access, and technical controls, such as security software programs designed to prevent or detect unauthorized access to sensitive files. The access controls described in this section are limited to those controls required to be provided by system manufacturers.

7.2.1 General Access Control

General requirements address the high-level functionality of a voting system. These are the fundamental access control requirements upon which other requirements in this section are based.

a. Voting system equipment **shall** provide access control mechanisms designed to permit authorized access to the voting system and to prevent unauthorized access to the voting system.
    i. Access control mechanisms on the EMS **shall** be capable of identifying and authentication individuals permitted to perform operations on the EMS.
b. Voting system equipment **shall** provide controls that permit or deny access to the device's software and files.
c. The default access control permissions **shall** implement the minimum permissions needed for each role or group identified by a device.
d. The voting device **shall** prevent a lower-privileged process from modifying a higher-privileged process.
e. An administrator of voting system equipment **shall** authorize privileged operations.
f. Voting system equipment **shall** prevent modification to or tampering with software or firmware through any means other than the documented procedure for software upgrades.

7.2.2 Access Control Identification

Identification requirements provide controls for accountability when operating and administering a voting system.

a. The voting system **shall** identify users and processes to which access is granted and the specific functions and data to which each entity holds authorized access.
b. Voting system equipment that implement role-based access control **shall** support the recommendations for Core RBAC in the ANSI INCITS 359-2004 American National Standard for Information Technology- Role Based Access Control document.
c. Voting system equipment **shall** allow the administrator group or role to configure the permissions and functionality for each identity, group, or role to include account and group/role creation, modification, and deletion.

7.2.3 Access Control Authentication

Authentication establishes the validity of the identity of the user, application, or process interacting with the voting system. Authentication is based on the identification provided by the user, application, or process interacting with the voting system. User authentication is generally classified in one of the following three categories:

- Something the user knows – this is usually a password, pass phrase, or PIN
- Something the user has – this is usually a token that may be either hardware or software based, such as a smart card
- Something the user is – this is usually a fingerprint, retina patter, voice pattern or other biometric data

Traditional password authentication is a single factor authentication method. A more secure method of authentication combines the various methods of authentication into two-factor authentication, or multi-factor authentication. For example, a user may use an authentication token and a passphrase for authentication. Using multi-factor provides stronger authentication than single factor. There are also cryptographic-based authentication methods such as digital signatures and challenge-response authentication, which are either software or hardware-based based tokens.

The following authentication requirements apply to all voting system equipment.

a. Voting system equipment **shall** authenticate users prior to granting them access to system functions or data.
b. When private or secret authentication data is stored in voting system equipment, the data **shall** be protected to ensure that the confidentiality and integrity of the data is not violated.
c. Voting system equipment **shall** allow the administrator group or role to set and change passwords, pass phrases, and keys.
d. Voting system equipment **shall** allow privileged groups or roles to be disabled and allow new individual privileged groups or roles to be created.
e. Voting system equipment **shall** lock our groups, roles, or individuals after a specified number of consecutive failed authentication attempts within a pre-defined time period.
f. Voting systems **shall** allow the administrator group or role to configure the account lock out policy, including the time period within which failed attempts must occur, the number of consecutive failed access attempts allowed before lock out, and the length of time the account is locked out.
g. If the voting system uses a user name and password authentication method, the voting system **shall** allow the administrator to enforce password strength, histories, and expiration.
h. The voting system **shall** allow the administrator group or role to specify password strength for all accounts, including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters.
i. The voting system **shall** enforce password histories, and allow the administrator to configure the history length.
j. Voting system equipment **shall** ensure that the username is not used in the password.
k. Voting systems **shall** provide a means to automatically expire passwords in accordance with the voting jurisdiction's policies.

7.2.4 Access Control Authorization

Authorization is the process of determining access rights based on authentication of a user, application, or process within a voting system. Authorization permits or denies access to an object by a subject. Subjects may be users, applications, or processes that interact with the voting system. Objects may be files or programs within the voting system.

a. Voting systems **shall** ensure that only authorized roles, groups, or individuals have access to election data.
b. Voting systems **shall** explicitly authorize subject's access based on access control lists or policies.
c. Voting systems **shall** explicitly deny subject's access based on access control lists or policies.

7.3 Physical Security Measures

A voting system's sensitivity to disruption or corruption of data depends, in part, on the physical location of equipment and data media, and on the establishment of secure telecommunications among various locations. Most often, the disruption of voting and vote counting results from a physical violation of one or more areas of the system thought to be protected. Therefore, security procedures **shall** address physical threats and the corresponding means to defeat them.

a. Any unauthorized physical access **shall** leave physical evidence that an unauthorized event has taken place.
b. Voting systems **shall** only have physical ports and access points that are essential to voting operations and to voting system testing and auditing.
c. An event log entry that identifies the name of the affected device **shall** be generated if a component connected to a piece of voting system equipment is disconnected while polls are open.
d. Ports disabled while polls are open **shall** only be re-enabled by authorized administrators.
e. Access points, such as covers and panels, **shall** be secured by locks or tamper-evident seals or tamper resistant countermeasures **shall** be implemented so that system owners can monitor access to voting system components through these points.
f. Ballot boxes **shall** be designed such that any unauthorized physical access results in physical evidence that an unauthorized event has taken place.

7.3.1 Polling Place Security

For polling place operations, manufacturers **shall** develop and provide detailed documentation of measures to enable poll workers to physically protect and perform orderly shutdown of voting equipment to counteract vandalism, civil disobedience, and similar occurrences.

The measures **shall** allow the immediate detection of tampering with vote casting devices and precinct ballot counters. They also **shall** control physical access to a telecommunications link if such a link is used

7.3.2 Central Count Location Security

Manufacturers **shall** develop and document in detail the measures to be taken in a central counting environment. These measures **shall** include physical and procedural controls related to the handling of ballot boxes, preparing of ballots for counting, counting operations and reporting data.

7.4 Software Security

Voting systems **shall** meet specific security requirements for the installation of software and for protection against malicious software.

7.4.1 Software and Firmware Installation

The system **shall** meet the following requirements for installation of software, including hardware with embedded firmware.

a. If software is resident in the system as firmware, the manufacturer **shall** require and state in the system documentation that every device is to be retested to validate each ROM prior to the start of elections operations.
b. To prevent alteration of executable code, no software **shall** be permanently installed or resident in the voting system unless the system documentation states that the jurisdiction must provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of the system hardware.
c. The voting system bootstrap, monitor, and device-controller software may be resident permanently as firmware, provided that this firmware has been shown to be inaccessible to activation or control by any means other than by the authorized initiation and execution of the vote counting program, and its associated exception handlers.
d. The election-specific programming may be installed and resident as firmware, provided that such firmware is installed on a component (such as a computer chip) other than the component on which the operating system resides.
e. After initiation of election day testing, no source code or compilers or assemblers **shall** be resident or accessible.

7.4.2 Protection Against Malicious Software

Voting systems **shall** deploy protection against the many forms of threats to which they may be exposed such as file and macro viruses, worms, Trojan horses, and logic bombs.

Manufacturers **shall** develop and document the procedures to be followed to ensure that such protection is maintained in a current status.

7.4.3 Software Distribution and Setup Validation

Subsections 7.4.4, 7.4.5 and 7.4.6 specify requirements for the distribution of voting system software and the setup validation performed on voting system equipment. These requirements are applicable to voting systems that have completed certification testing. The goal of the software distribution requirements is to ensure that the correct voting system software has been distributed without modification. The goal of setup validation requirements, including requirements for verifying the presence of certified software and the absence of other software, is to ensure that voting system equipment is in a proper initial state before being used.

In general, a voting system can be considered to be composed of multiple associated systems including polling place systems, central counting/aggregation systems, and election management systems. These other systems may reside on different computer platforms at different locations and run different software. Voting system software is considered to be all executable code and associated configuration files critical for the proper operation of the voting system regardless of the location of installation and functionality provided. This includes third party software such as operating systems, drivers, and database management systems.

7.4.4 Software Distribution

a. The manufacturer **shall** document all software including voting system software, third party software (such as operating systems and drivers) to be installed on the certified voting system, and installation programs.
    i. The documentation **shall** have a unique identifier (such as a serial number or part number) for the following set of information: documentation, software manufacturer name, product name, version, the certification application number of the voting system, file names and paths or other location information (such as storage addresses) of the software.
    ii. The documentation **shall** designate all software files as static, semi-static or dynamic.

Discussion: Static voting system software such as executable code does not change based on the election being conducted or the voting equipment upon which it is installed. Semi-static voting system software contains configuration information for the voting system based on the voting equipment that is installed and the election being conducted. Semi-static software is only modified during the installation of (a) the voting system software on voting equipment or (b) the election-specific software such as ballot formats. Dynamic voting system software changes over time once installed on voting equipment. However, the specific time or value of the change in the dynamic software is usually unknown in advance, making it impossible to create reference information to verify the software.

7.4.5 Software Reference Information

a. The manufacturer **shall** provide the NSRL and any repository designated by a state with a copy of the software installation disk, which the manufacturer will distribute to purchasers--including the executable binary images of all third party software.
    i. All voting system software, installation programs and third party software (such as operating systems and drivers) used to install or to be installed on voting system equipment **shall** be distributed using unalterable storage media.
    ii. The manufacturer **shall** document that the process used to verify the software distributed on unalterable storage media is the certified software by using the reference information provided by the NSRL or other designated repository before installing the software.
b. The voting system equipment **shall** be designed to allow the voting system administrator to verify that the software is the certified software by comparing it to reference information produced by the NSRL or other designated repository.
c. The manufacturers **shall** document to whom they provide voting system software.

7.4.6 Software Setup Validation

The following requirements support the security of voting systems by providing methods to verify that only authorized software is present on voting systems. It includes requirements for two software verification techniques. One method verifies digital signatures on software prior to installation on pieces of voting system equipment. This is a useful mechanism that helps prevent accidental or malicious software from being installed and could be employed by any voting system to protect against unauthorized software. The second method provides an external interface to voting system software. A separate piece of equipment could use this interface to verify the software on the voting system. However, this method merely provides a mechanism for detecting unauthorized software and, by itself, does not help prevent the installation of accidental or malicious software.

a. Setup validation methods **shall** verify that only authorized software is present on the voting equipment. Authorized software is COTS software components needed to run the voting system and voting software components identified by the manufacturer as authorized.
b. The manufacturer **shall** provide a method to comprehensively list all software files that are installed on voting systems.
    i. This method **shall** list version names and numbers for all application software on the voting system.
    ii. This method should list of the date of installation for all application software on the voting system.
c. Setup validation methods **shall** include a software verification method that ensures that the voting system software has not been modified illegitimately.
    i. The voting systems **shall** include any supporting software and hardware necessary to conduct the software verification method.
    ii. The manufacturer **shall** document the process used to conduct the software verification method.
    iii. The software verification method **shall** not modify the voting system software on the voting system.
d. Voting systems **shall** include a software verification method that either verifies software prior to installation or a method that verifies software using an external interface. Voting systems may include both software verification methods. Voting systems may provide ancillary setup validation methods, including methods for verifying or identifying installed software, other than those described in this section. There are no specific requirements for ancillary setup validation methods. However, any method intended to serve as the voting system software verification method must meet the requirements outlined in this section.
e. Voting systems which implement a software verification method that verifies software prior to installation **shall** meet the following requirements.
    i. The voting system **shall** contain no more than one method for installing, updating, or removing software on a system.
        - Voting system equipment **shall** prevent processes from installing software except for the one specific software installation process identified by the manufacturer.
        - The voting system manufacturer **shall** document the procedures for installing, updating, and removing voting system software, configuration files, and data files.
        - Voting system equipment **shall** prevent processes from installing, updating or removing software while the polls are open.
        - Voting system equipment **shall** prevent the execution of software not installed using the specified software installation process.
    ii. The voting system **shall** only allow authenticated administrators to install software on voting equipment. The voting system **shall** present the administrator with a description of the software change being performed, including:
        - A list of all applications and/or file names being updated.
        - The type of action performed on each application and/or file (e.g., new application/file, deletion or overwriting of existing file)
    iii. Voting system equipment **shall** store the current version identification of all software installed on the voting system equipment.

- The current version identification **shall** be included as part of reports created by the voting system equipment.
- The current version identification **shall** be displayed as part of the voting system equipment start up process.

iv. The process for installing, updating and removing software **shall** make software changes based on information contained in software update packages. Software update packages **shall** minimally contain the following information:
- A unique identifier for the software update package.
- Names of the applications or files modified during the update process.
- Version numbers of the applications or files modified during the update process.
- Any software prerequisites or dependencies for the software involved in the update.
- A description of the type of action performed on each application and/or file (e.g., new application/file, deletion or overwriting of existing file).
- The binary data of any new or updated files involved in the update process.

v. The software update package **shall** be formatted in a non-restrictive, publicly-available format. Manufacturers **shall** provide a specification describing how they have implemented the format with respect to the manufacturer's specific voting devices and data, including such items as descriptions of elements, attributes, constraints, extensions, syntax and semantics of the format, and definitions for data fields and schemas.

vi. Software update packages **shall** be digitally signed by using a NIST approved algorithm with a security strength of at least 112 bits.

vii. The software installation process **shall** verify digital signatures, software version identification, software prerequisites and dependencies, and manufacturer specific authorization information associated with the software before the software is installed. The software installation process **shall** not install software with invalid digital signatures, version numbers, or manufacturer specific authorization information, and **shall** not install software on systems that do not meet the update requisites.

viii. The voting system **shall** have the capability to prevent the installation of previous versions of applications or files.

ix. The software installation process **shall** result in information being stored in the voting system equipment's log such that altering or deleting log entries or the log will be detected.

x. The minimum information to be included in the voting system equipment log **shall** be:
- Success or failure of the software installation process;
- Cause of a failed software installation (such as invalid version identification, digital signature, etc.);
- Application or file name(s), and version number(s);
- A description of the type of action performed on each application and/or file (e.g., new application/file, deletion or overwriting of existing file);

- A cryptographic hash of the software update package using FIPS 140-2 level 1 or higher validated cryptographic module.

f. If software is verified after being installed on the voting system equipment, the voting system equipment **shall** provide an external interface to the location of the voting system software for software verification purposes.
   i. The external interface:
      - **Shall** be protected using tamper evident techniques,
      - **Shall** have a physical indicator showing when the interface is enabled and disabled
      - **Shall** be disabled during voting
      - Should provide a direct read-only access to the location of the voting system software without the use of installed software
   ii. The verification process should be able to be performed using COTS software and hardware available from sources other than the voting system manufacturer.
      - If the process uses hashes or digital signatures, then the verification software **shall** use a FIPS 140-2 level 1 or higher validated cryptographic module.
      - The verification process **shall** either (a) use reference information on unalterable storage media received from the repository or (b) verify the digital signature of the reference information on any other media.

g. Setup validation methods **shall** verify the contents of all system storage locations (e.g., system registers, variables, files, etc.) containing election specific information (e.g., ballot style, candidate registers, measure registers, etc.).
   i. The manufacturer should provide a method to query the voting system to determine the value contained in all system storage locations containing election specific information.
   ii. The manufacturer **shall** document the default values of all system storage locations that hold election specific information.

7.5 Telecommunications and Data Transmission

There are four areas that must be addressed by telecommunications and data transmission security capabilities: access control, data integrity, detection and prevention of data interception, and protection against external threats.

7.5.1 Maintaining Data Integrity

Voting systems that use telecommunications to communicate between system components and locations are subject to the same security requirements governing access to any other system hardware, software, and data function.

a. Voting systems that use electrical or optical transmission of data **shall** ensure the receipt of valid vote records is verified at the receiving station. This should include standard transmission error detection and correction methods such as checksums or message digest hashes. Verification of correct transmission **shall**

occur at the voting system application level and ensure that the correct data is recorded on all relevant components consolidated within the polling place prior to the voter completing casting of his or her ballot.

i. Cryptography used to verify the receipt of vote records **shall** use NIST approved algorithms with security strength of at least 112 bits. Message Authentication Code (MAC) keys **shall** have a security strength of at least 112 bits.

b. Voting systems that use telecommunications to communicate between system components and locations **shall**:
   i. Implement encryption using NIST approved algorithms with a security strength of at least 112 bits within a FIPS 140-2 level 1 or higher validated cryptographic module operating in FIPS mode
   ii. Provide a means to detect the presence of an intrusive process, such as an Intrusion Detection System

7.5.2 Protection Against External Threats

a. Voting systems that use public telecommunications networks **shall** implement protections against external threats to which commercial products used in the system may be susceptible.
b. Voting systems that use public telecommunications networks **shall** provide system documentation that clearly identifies all COTS hardware and software products and communications services used in the development and/or operation of the voting system, including operating systems, communications routers, modem drivers and dial-up networking software.
   i. Such documentation **shall** identify the name, manufacturer, and version used for each such component.
c. Voting systems that use public telecommunications networks **shall** use protective software at the receiving-end of all communications paths to:
   i. Detect the presence of a threat in a transmission
   ii. Remove the threat from infected files/data
   iii. Prevent against storage of the threat anywhere on the receiving device
   iv. Provide the capability to confirm that no threats are stored in system memory and in connected storage media
   v. Provide data to the system audit log indicating the detection of a threat and the processing performed
d. Manufacturers **shall** use multiple forms of protective software as needed to provide capabilities for the full range of products used by the voting system.

7.5.3 Monitoring and Responding to External Threats

Voting systems that use public telecommunications networks may become vulnerable, by virtue of their system components, to external threats to the accuracy and integrity of vote recording, vote counting, and vote consolidation and reporting processes. Therefore,

manufacturers of such systems **shall** document how they plan to monitor and respond to known threats to which their voting systems are vulnerable. This documentation **shall** provide a detailed description, including scheduling information, of the procedures the manufacturer will use to:

a. Monitor threats, such as through the review of assessments, advisories, and alerts for COTS components issued by the Computer Emergency Response Team (CERT), for which a current listing can be found at http://www.cert.org, the National Infrastructure Protection Center (NIPC), and the Federal Computer Incident Response Capability (FedCIRC), for which additional information can be found at www.us-cert.gov
b. Evaluate the threats and, if any, proposed responses
c. Develop responsive updates to the system and/or corrective procedures
d. Submit the proposed response to the VSTLs and appropriate states for approval, identifying the exact changes and whether or not they are temporary or permanent
e. After implementation of the proposed response is approved, assist clients, either directly or through detailed written procedures, how to update their systems and/or to implement the corrective procedures within the timeframe established
f. Address threats emerging too late to correct the system by:
    i. Providing prompt, emergency notification to the EAC, VSTLs and the affected states and user jurisdictions
    ii. Assisting client jurisdictions directly or advising them through detailed written procedures to disable the public telecommunications mode of the system
    iii. Modifying the system after the election to address the threat, submitting the modified system to a VSTL and the EAC for approval, and assisting client jurisdictions directly or advising them through detailed written procedures, to update their systems and/or to implement the corrective procedures after approval

7.5.4 Shared Operating Environment

Ballot recording and vote counting can be performed in either a dedicated or non-dedicated environment. If ballot recording and vote counting operations are performed in an environment that is shared with other data processing functions, both hardware and software features **shall** be present to protect the integrity of vote counting and of vote data.

Systems that use a shared operating environment shall:

a. Use security procedures and logging records to control access to system functions
b. Partition or compartmentalize voting system functions from other concurrent functions at least logically, and preferably physically as well
c. Control system access by means of passwords, and restrict account access to necessary functions only
d. Have capabilities in place to control the flow of information, precluding data leakage through shared system resources

7.5.5 Election Returns

If the voting system provides access to election returns or interactive inquiries, the system **shall**:

a. Allow authorized administrators the ability to disable or restrict access to election returns (for equipment that operates in a central counting environment). This requirement applies as well to polling place equipment that contains a removable memory module or that may be removed in its entirety to a central place for the consolidation of polling place returns
b. Design voting system software and its security environment such that data accessible to interactive queries resides in an external file or database created and maintained by the elections software under the restrictions applying to any other output report:
    i. The output file or database has no provision for write access back to the system
    ii. Persons whose only authorized access is to the file or database are denied write access, both to the file or database, and to the system

7.6 Use of Public Communications Networks

Voting systems that transmit data over public telecommunications networks face security risks that are not present in other voting systems. This section describes standards applicable to voting systems that use public telecommunications networks.

7.6.1 Data Transmission

All systems that transmit data over public telecommunications networks **shall**:

a. Preserve the secrecy of voter ballot selections and prevent anyone from violating ballot privacy
b. Employ digital signatures for all communications between the vote server and other devices that communicate with the server over the network
c. Require that at least two authorized election officials activate any critical operation regarding the processing of ballots transmitted over a public communications network, i.e. the passwords or cryptographic keys of at least two employees are required to perform processing of votes

Cryptography used to provide protection of data transmitted over public telecommunications networks **shall** use NIST approved algorithms with security strength of at least 112 bits. Message Authentication Code (MAC) keys **shall** have a security strength of at least 112 bits. The security strengths of cryptographic algorithms can be found in NIST Special Publication 800-57: Recommendation for Key Management – Part 1 General.

7.6.2 Casting Individual Ballots

Systems designed for transmission of data over public networks **shall** meet security standards that address the security risks attendant with the casting of ballots from polling places controlled by election officials using voting devices configured and installed by election officials and/or their manufacturer or contractor, and using in-person authentication of individual voters.

7.6.2.1 Documentation of Mandatory Security Activities

Manufacturers of voting systems that cast individual ballots over a public telecommunications network **shall** provide detailed descriptions of:

a. All activities mandatory to ensuring effective voting system security to be performed in setting up the system for operation, including testing of security before an election
b. All activities that should be prohibited during voting equipment setup and during the timeframe for voting operations, including both the hours when polls are open and when polls are closed

7.6.2.2 Ability to Operate During Interruption of Service

These systems **shall** provide the following capabilities to provide resistance to interruptions of telecommunications service that prevent voting devices at the polling place from communicating with external components via telecommunications:

a. Detect the occurrence of a telecommunications interruption at the polling place and switch to an alternative mode of operation that is not dependent on the connection between polling place voting devices and external system components
b. Provide an alternate mode of operation that includes the functionality of a conventional electronic voting system without losing any votes
c. Create and preserve an audit trail of every vote cast during the period of interrupted communication and system operation in conventional electronic voting system mode
d. Upon reestablishment of communications, transmit and process votes accumulated while operating in conventional electronic voting system mode with all security safeguards in effect
e. Ensure that all safeguards related to voter identification and authentication are not affected by the procedures employed by the system to counteract potential interruptions of telecommunications capabilities

7.7 Wireless Communications

This section provides requirements for implementing and using wireless communications within a voting system. These requirements reduce, but do not eliminate, the risk of using wireless communications for voting systems.

Wireless is defined as any means of communications that occurs without wires. This normally covers the entire electromagnetic spectrum. For the purposes of this section, wireless includes radio frequency, infrared, and microwave. This section provides requirements and considerations that apply to external wireless communications capabilities existing on voting equipment or as a component within a voting system. These requirements may be applied to internal wireless communications, but this is not required when the physical container that houses the voting equipment or voting system is considered adequate to protect the internal wireless between or among voting system components.

Since the wireless communications path on which the signals travel is via the air and not a wire or cable, devices other than those intended to receive the wireless signal (e.g. voting data) can receive (intentionally and unintentionally) the wireless signals. Some of the wireless communications paths (i.e. signals) are weakened by walls and distance, but are not stopped. This makes it possible to eavesdrop from a distance as well as transmit wireless signals (e.g., interference or intrusive data) from a distance. In many cases, the wireless signals cannot be seen, heard, or felt, thus making the presence of wireless communication hard to determine by the human senses. The requirements in this section mitigate the risks associated with wireless by controlling and identifying usage, and protecting the transmitted data and path.

There are other concerns when evaluating wireless usage; specifically radio frequency (RF). A device's radio frequencies usage and the power output are governed by Federal Communications Commission (FCC) regulations and therefore all RF wireless communications devices are subject to the applicable FCC requirements. However, these FCC regulations do not fully address RF wireless interference caused by multiple FCC compliant devices. That is, the RF wireless used in a voting system may be using the same radio frequency as another non-voting wireless system and which may potentially cause a degradation of the wireless performance or a complete wireless failure for the voting system.

Sometimes a particular wireless technology permits a power output range, which may be used to overcome interference received from another device. A radio emissions site test can determine the extent of potential existing interference at the location where the wireless voting system is to be used. A radio emission site test can also determine the extent that the RF wireless transmission of the voting system escapes the building in which the RF wireless voting system is used.

7.7.1 Controlling Usage

a. If wireless communications are used in a voting system, then the manufacturer **shall** supply documentation describing how to use all aspects of wireless communications in a secure manner. This documentation **shall** include:
   i. A complete description of the uses of wireless in the voting system including descriptions of the data elements and signals that are to be carried by the wireless mechanism
   ii. A complete description of the vulnerabilities associated with this proposed use of wireless, including vulnerabilities deriving from the insertion, deletion, modification, capture or suppression of wireless messages
   iii. A complete description of the techniques used to mitigate the risks associated with the described vulnerabilities including techniques used by the manufacturer to ensure that wireless cannot send or receive messages other than those situations specified in the documentation. Cryptographic techniques **shall** be carefully and fully described, including a description of cryptographic key generation, management, use, certification, and destruction
   iv. A rationale for the inclusion of wireless in the proposed voting system, based on a careful and complete description of the perceived advantages and disadvantages of using wireless for the documented uses compared to using non-wireless approaches

> Discussion: In general, convenience is not a sufficiently compelling reason, on its own, to justify the inclusion of wireless communications in a voting system. Convenience must be balanced against the difficulty of working with cryptographic keys.

b. The details of all cryptographic protocols used for wireless communications, including the specific features and data, **shall** be documented.
c. The wireless documentation **shall** be closely reviewed for accuracy, completeness, and correctness.
d. There **shall** be no undocumented use of the wireless capability, nor any use of the wireless capability that is not entirely controlled by an election official.

> Discussion: This can be tested by reviewing all of the software, hardware, and documentation, and by testing the status of wireless activity during all phases of testing.

e. If a voting system includes wireless capabilities, then the voting system **shall** be able to accomplish the same function if wireless capabilities are not available due to an error or no service.
   i. The manufacturer **shall** provide documentation how to accomplish these functions when wireless is not available.
f. The system **shall** be designed and configured so it is not vulnerable to a single point of failure using wireless communications that causes a total loss of any voting capabilities.

g. If a voting system includes wireless capabilities, then the system **shall** have the ability to turn on the wireless capability when it is to be used and to turn off the wireless capability when the wireless capability is not in use.
h. If a voting system includes wireless capabilities, then the system **shall** not activate the wireless capabilities without confirmation from an elections official.

7.7.2 Identifying Usage

Since there are a wide variety of wireless technologies (both standard and proprietary) and differing physical properties of wireless signals, it is important to identify some of the characteristics of the wireless technologies used in the voting system.

a. If a voting system provides wireless communications capabilities, then there **shall** be a method for determining the existence of the wireless communications capabilities.
b. If a voting system provides wireless communications capabilities, then there **shall** be an indication that allows one to determine when the wireless communications (such as radio frequencies) capability is active.
c. The indication **shall** be visual.
d. If a voting system provides wireless communications capabilities, then the type of wireless communications used (such as radio frequencies) **shall** be identified either via a label or via the voting system documentation.

7.7.3 Protecting Transmitted Data

The transmitted data, especially via wireless communications, needs to be protected to ensure confidentiality and integrity. Examples of election information that needs to be protected include: ballot definitions, voting device counts, precinct counts, opening of poll signal, and closing of poll signal. Examples of other information that needs to be protected include: protocol messages, address or device identification information, and passwords.

Since radio frequency wireless signals radiate in all directions and pass through most construction material, anyone may easily receive the wireless signals. In contrast, infrared signals are line of sight and do not pass through most construction material. However, infrared signals can still be received by other devices that are in the line of sight. Similarly, wireless signals can be transmitted by others to create unwanted signals. Thus, encryption is required to protect the privacy and confidentiality of the voting information.

a. All information transmitted via wireless communications **shall** be encrypted and authenticated--with the exception of wireless T-coil coupling--to protect against eavesdropping and data manipulation including modification, insertion, and deletion.
    i. Cryptography used for encryption and authentication **shall** use NIST approved algorithms with security strength of at least 112 bits. Message

Authentication Code (MAC) keys **shall** have a security strength of at least 112 bits.

ii. The cryptographic modules used **shall** comply with FIPS 140-2, Security Requirements for Cryptographic Modules.

b. The capability to transmit non-encrypted and non-authenticated information via wireless communications **shall** not exist.
c. If audible wireless communication is used, and the receiver of the wireless transmission is the human ear, then the information **shall** not be encrypted.

Discussion: This specifically covers wireless T-Coil coupling for assistive devices used by people who are hard of hearing.

7.7.4 Protecting the Wireless Path

If wireless communications are used, then the following capabilities **shall** exist in order to mitigate the effects of a denial of service (DoS) attack:

a. The voting system **shall** be able to function properly throughout a DoS attack, since the DoS attack may continue throughout the voting period.
b. The voting system **shall** function properly as if the wireless capability were never available for use.
c. Alternative procedures or capabilities **shall** exist to accomplish the same functions that the wireless communications capability would have done.
d. If infrared is being used, the shielding **shall** be strong enough to prevent escape of the voting system signal, as well as strong enough to prevent infrared saturation jamming.

Discussion: Since infrared has the line-of-sight property, securing the wireless path can be accomplished by shielding the path between the communicating devices with an opaque enclosure. However, this is only practical for short distances. This shielding would also help prevent accidental eye damage from the infrared signal.

7.7.5 Protecting the Voting System

Physical security measures to prevent access to a voting system are not possible when using a wireless communications interface because there is no discrete physical communications path that can be secured.

a. The security requirements in Subsection 2.1.1 **shall** be applicable to systems with wireless communications.
b. The accuracy requirements in Subsection 2.1.2 **shall** be applicable to systems with wireless communications.

c. The use of wireless communications that may cause impact to the system accuracy through electromagnetic stresses is prohibited.
d. The error recovery requirements in Subsection 2.1.3 **shall** be applicable to systems with wireless communications.
e. All wireless communications actions **shall** be logged.
    i. The log **shall** contain at least the following entries: times when the wireless is activated and deactivated, services accessed, identification of device to which data was transmitted to or received from, identification of authorized user, and successful and unsuccessful attempts to access wireless communications or service.

Discussion: Other information such as the number of frames or packets transmitted or received at various logical layers may be useful, but is dependent on the wireless technology used.

f. Device authentication **shall** occur before any access to, or services from, the voting system are granted through wireless communications.

Discussion: Authentication is an important element to protect the security of wireless communications. Authentication verifies the identity and legitimacy of users, devices, and services.

    i. User authentication **shall** be at least level 2 as per NIST Special Publication 800-63 Version 1.0.1, Electronic Authentication Guideline.

7.8 Voter Verifiable Paper Audit Trail Requirements

This section contains requirements for DREs with a Voter Verifiable Paper Audit Trail (VVPAT) component, henceforth referred to as VVPAT voting systems. A VVPAT voting system **shall** consist minimally of the following fundamental components:

- A voting device, on which a voter makes selections and prepares to cast a ballot;
- A printer that prints a paper record summary of the voter's ballot selections, and that allows the voter to compare it with the electronic ballot selections;
- A mechanism by which the voter may indicate acceptance or rejection of the paper record;
- Ballot box/cartridge to contain accepted and voided paper records; and
- A paper record for each electronic ballot image. The paper record may be printed on a separate sheet for each record ("cut-sheet VVPAT") or on a continuous paper roll ("paper-roll VVPAT").

VVPAT capability is not required for national certification. However, these requirements will be applied for certification testing of DRE systems that are intended for use in states that require DREs to provide this capability. The manufacturer's certification testing application to the EAC must indicate whether the system being presented for testing includes this capability, as provided under Subsection 1.6.2.5 extensions.

7.8.1 Display and Print a Paper Record

a. VVPAT voting systems **shall** provide capabilities for the voter to review a paper record of ballot selections and a summary of the voter's electronic ballot selections prior to casting a ballot.
b. VVPAT voting systems **shall** create a paper record that election officials can use to reconstruct the full set of totals from the election.
c. Each paper record **shall** contain a human-readable summary of the electronic ballot image record. In addition, all paper records **shall** contain audit-related information including:
    i. Machine ID;
    ii. Reporting context, such as precinct or election district;
    iii. Ballot style;
    iv. Date of election or date record printed; and
    v. Complete summary of voter's choices.

7.8.2 Approve or Void the Paper Record

a. The VVPAT voting system format and presentation of the paper record and electronic summaries of ballot selections **shall** be designed to facilitate the voter's comparison between the electronic summaries of ballot selections displayed on the screen and the paper record.
b. When a voter indicates that the paper record is to be accepted, the VVPAT voting system **shall**:
    i. Immediately print an indication that the vote has been accepted, in view of the voter;
    ii. Electronically store the electronic ballot image record as a cast vote; and
    iii. Deposit the paper record into a secure receptacle.
c. When a voter indicates that the paper record is to be rejected, the VVPAT voting system **shall**:
    i. Immediately print an unambiguous indication that the vote has been rejected, in view of the voter;
    ii. Electronically store a record that the paper record was rejected; and
    iii. Deposit the rejected paper record into the secure receptacle.
d. The VVPAT voting system **shall** have the capacity to be configured to limit the number of times a single voter may reject a paper record without election official intervention. The VVPAT voting system **shall** support limits between zero (any rejected paper record requires election official intervention) to five times, and may support an unlimited number of rejections without election official intervention.
e. The VVPAT voting system **shall** have the capacity to limit the total number of paper records that a machine may reject before election official intervention is required. The VVPAT voting system **shall** have a default limit of three rejected paper records before election official intervention is required. The VVPAT voting system **shall** permit the setting of no limit, so that no number of total rejected paper records requires immediate election official intervention.

f. The VVPAT voting system **shall** have the capacity to be configured to remove any indication of the voter's choices from the screen when the configured limit of rejected paper records per voter or per machine is reached.
g. When a VVPAT voting system reaches a configured limit of rejected paper records per voter or per machine, it **shall** do the following:
    i. Place the paper record that has been rejected into the ballot box or other receptacle;
    ii. Clearly display that a paper record has been rejected and indicate the need for election official intervention; and
    iii. Suspend normal operations until re-enabled by an authorized election official.

7.8.3 Electronic and Paper Record Structure

a. Electronic ballot images **shall** be recorded in a randomized order by the voting system for the election. NIST Special Publication 800-90: Recommendation for Random Number Generation Using Deterministic Random Bit Generators specifies techniques for the generation of random numbers that can be used to randomize the order of ballot images in a cryptographically sound way. For each voted ballot, this includes:
    i. Ballot style and reporting context such as precinct or election district;
    ii. For each contest:
        - The choice recorded, including undervotes and write-ins; and
        - Any information collected by the vote-capture device electronically about each write-in;
    iii. Information specifying whether the ballot is provisional, early voting or election day voting. Types of provisional ballots (such as "regular provisional", "extended hours provisional", and "regular extended hours") are jurisdiction-dependent.
    iv. Information linking the electronic ballot image to a paper record, if such functionality is enabled in the voting system.
b. The voting system **shall** provide the capability to export the collection of electronic ballot images in a publicly documented format, such as XML, or include a utility to export the records into a publicly documented format for offline viewing.
c. Electronic ballot images **shall** be digitally signed by the voting system. The digital signature **shall** be generated using a NIST-approved digital signature algorithm with a security strength of at least 112 bits implemented within a FIPS 140-2 validated cryptographic module operating in FIPS mode.
d. The human-readable contents of the paper record should be created in a manner that is machine-readable by optical character recognition.
e. Paper-roll VVPAT voting systems **shall** mark paper rolls with the following:
    i. Machine ID;
    ii. Reporting context, such as precinct or election district;
    iii. Date of election or date record printed;
    iv. If multiple paper rolls were produced during this election on this device, the number of the paper roll (e.g., Roll #2); and

f. Paper-roll VVPAT voting systems **shall** include the following on each paper record:
    i. Ballot style;
    ii. Type of voting (e.g., provisional, early, etc.);
    iii. Complete summary of voter's choices;
    iv. For each ballot contest:
        - Contest name (e.g., "Governor");
        - Any additional information needed for unambiguous interpretation of the paper record;
        - An indication, if the contest was undervoted; and
        - An indication, if the choice is a write-in vote.
    v. An indication of whether the paper record has been accepted or rejected by the voter.
g. Paper-roll VVPAT voting systems **shall** not split paper records across rolls; each paper record must be contained in its entirety by the paper roll.
h. Cut-sheet VVPAT voting systems **shall** include the following on each paper record:
    i. Machine ID;
    ii. Reporting context, such as precinct or election district;
    iii. Date of election or date record printed;
    iv. Ballot style
    v. Type of voting (e.g., provisional, early, etc.);
    vi. Complete summary of voter's choices;
    vii. For each ballot contest:
        - Contest name (e.g., "Governor");
        - Any additional information needed for unambiguous interpretation of the paper record;
        - An indication, if the contest was undervoted; and
        - An indication, if the choice is a write-in vote.
    viii. An indication of whether each sheet has been accepted or rejected by the voter.
i. If a cut-sheet VVPAT voting system splits paper records across multiple sheets of paper, each sheet **shall** include:
    i. Page number of this sheet and total number of sheets (e.g., page 1 of 4);
    ii. Ballot style
    iii. Reporting context, such as precinct or election district
    iv. An indication that the sheet's contents have been accepted or rejected by the voter; and
    v. Any correspondence information included to link the paper record to its corresponding electronic ballot image record.
j. If a cut-sheet VVPAT voting system splits paper record across multiple sheets of paper, it **shall** not split ballot contests across sheets.
k. If a cut-sheet VVPAT voting system splits paper records across multiple sheets of paper, the ballot choices on each sheet **shall** be submitted to the voter for verification separately according to the following:
    i. The voter **shall** be presented a verification screen for the contents of each sheet separately at the same time as the voter is able to verify the contents of the part of the paper record on the sheet;

ii. When a voter accepts or rejects the contents of a sheet, the votes contained on that sheet and verification screen **shall** be committed to memory, regardless of the verification of any other sheet by the same voter;
iii. Configurable limits on rejected paper records per voter **shall** count each rejected sheet as a rejected paper record;
iv. Configurable limits on rejected paper records per machine **shall** not count more than one rejected paper record per voter; and
v. When a rejected paper record requires election official intervention, the VVPAT voting system **shall** indicate which sheets have been accepted and which rejected.

l. The VVPAT voting system **shall** provide a capability to print information on each paper record sufficient for auditors to identify from an electronic ballot image record its corresponding paper record and from a paper records its corresponding electronic ballot image. This capability **shall** be possible for election officials to enable or disable.
m. Any information on the paper record that identifies the corresponding electronic ballot image should not be practical for the voter to read or copy by hand.
n. The VVPAT voting system manufacturer **shall** include a capability for auditors to verify the correspondence between the electronic ballot image and paper record pairs, if the correspondence information is printed on the paper record.

7.8.4 Equipment Security and Reliability

a. The VVPAT printer **shall** be physically connected via a standard, publicly documented printer port using a standard communications protocol.
b. Tamper-evident seals or physical security measures **shall** protect the connection between the printer and the voting machine.
c. If the connection between the voting machine and the printer has been broken, the voting machine **shall** detect this event and record it in the system event log.
d. The VVPAT voting system **shall** detect printer errors that may prevent paper records from being correctly displayed, printed or stored, such as lack of consumables such as paper, ink, or toner, paper jams/misfeeds, and memory errors.
e. If a printer error or malfunction is detected, the VVPAT voting system **shall**:
    i. Present a clear indication to the voter and election officials of the malfunction. This must indicate clearly whether the current voter's vote has been cast, discarded, or is waiting to be completed;
    ii. Suspend voting operations until the problem is resolved;
    iii. Allow canceling of the current voter's electronic ballot image by election officials in the case of an unrecoverable error; and
    iv. Protect the privacy of the voter while the error is being resolved.
f. Procedures for recovery from printer errors on paper-roll VVPAT voting systems **shall** not expose the contents of previously cast paper records.
g. Paper-roll VVPAT voting systems **shall** be designed so that when the rolls are removed from the voting device according to the following:
    i. All paper records are contained inside the secure container;
    ii. The container supports being tamper-sealed and locked; and

iii. The container supports being labeled with the device serial number, precinct, and other identifying information to support audits and recounts.

h. If a continuous paper spool is used to store paper records, the manufacturer **shall** provide a mechanism for an auditor to unspool the paper, view each paper record in its entirety, and then respool the paper, without modifying the paper in any way.
i. The printer **shall** not be permitted to communicate with any system or machine other than the voting machine to which it is connected.
j. The printer **shall** only be able to function as a printer; it **shall** not contain any other services (e.g., provide copier or fax functions) or network capability.
k. Protective coverings intended to be transparent on voting equipment **shall** be maintainable via a predefined cleaning process. If the coverings become damaged such that they obscure the paper record, they **shall** be replaceable.
l. The paper record **shall** be of sufficient durability to remain unchanged for minimally 22 months to be used for verifications, reconciliations, and recounts conducted manually or by automated processing.

7.8.5 Preserving Voter Privacy

VVPAT records can be printed and stored by two different methods:

- Printed and stored on a continuous spool-to-spool paper roll where the voter views the paper record in a window
- Printed on separate pieces of paper, which are deposited in a secure receptacle.

If a requirement applies to only one method, that will be specified. Otherwise, the requirement applies to both.

a. Voter privacy **shall** be preserved during the process of recording, verifying and auditing his or her ballot selections.

> Discussion: The privacy requirements from Section 3 also apply to voting equipment with VVPAT.

b. When a VVPAT with a spool-to-spool continuous paper record is used, a means **shall** be provided to preserve the secrecy of the paper record of voter selections.
c. When a VVPAT with a spool-to-spool continuous paper record is used, no record **shall** be maintained of which voters used which voting machine or the order in which they voted.
d. The electronic and paper records **shall** be created and stored in ways that preserve the privacy of the voter.

> Discussion: For VVPAT systems that use separate pieces of paper for the record, this can be accomplished in various ways including shuffling the order of the records or other methods to separate the order of stored records.

e. The privacy of voters whose paper records contain an alternative language **shall** be maintained.
f. Unique identifiers **shall** not be displayed in a way that is easily memorable by the voter.

> Discussion: Unique identifiers on the paper record are displayed or formatted in such a way that they are not memorable to voters, such as by obscuring them in other characters.

g. Both paper rolls and paper record secure receptacles **shall** be controlled, protected, and preserved with the same security as a ballot box.

7.8.6 VVPAT Usability

a. All usability requirements from Subsection 3.1 **shall** apply to voting machines with VVPAT.

> Discussion: The requirements in this section are in addition to those in Subsection 3.1.

b. The voting equipment **shall** be capable of showing the information on the paper in a font size of at least 3.0 mm and should be capable of showing the information in at least two font ranges; 3.0–4.0 mm, and 6.3–9.0 mm, under control of the voter or poll worker.

> Discussion: In keeping with requirements in Subsection 3.1, the paper record should use the same font sizes as displayed by the voting machine, but at least be capable of 3.0 mm. While larger font sizes may assist voters with poor vision, certain disabilities such as tunnel vision are best addressed by smaller font sizes.

c. The voting equipment **shall** display, print and store the paper record in any of the written alternative languages chosen for the ballot.
    i. To assist with manual auditing, candidate names on the paper record **shall** be presented in the same language as used on the DRE summary screen.
    ii. Information on the paper record not needed by the voter to perform verification **shall** be in English.

> Discussion: In addition to the voter ballot selections, the marking of the paper record as accepted or void, and the indication of the ballot page number need to be printed in the alternative language. Other information, such as precinct and election identifiers, **shall** be in English to facilitate use of the paper record for auditing.

d. The paper and electronic records **shall** be presented to allow the voter to read and compare the records without the voter having to shift his or her position.
e. If the paper record cannot be displayed in its entirety on a single page, a means **shall** be provided to allow the voter to view the entire record.

> Discussion: Possible solutions include scrolling the paper or printing a new sheet of paper. The voter should be notified if it is not possible to scroll in reverse, so they will know to complete verification in one pass.

f. If the paper record cannot be displayed in its entirety on a single page, each page of the record **shall** be numbered and **shall** include the total count of pages for the record.

> Discussion: Possible numbering schemes include "Page X of Y."

g. The instructions for performing the verification process **shall** be made available to the voter in a location on the voting machine.

> Discussion: All instructions must meet the usability requirements contained in Subsection 3.1.

7.8.7 VVPAT Accessibility

a. All accessibility requirements from Subsection 3.2 **shall** apply to voting machines with VVPAT.
b. If the normal voting procedure includes VVPAT, the accessible voting equipment should provide features that enable voters who are visually impaired and voters with an unwritten language to perform this verification. If state statute designates the paper record produced by the VVPAT to be the official ballot or the determinative record on a recount, the accessible voting equipment **shall** provide features that enable visually impaired voters and voters with an unwritten language to review the paper record.

> Discussion: For example, the accessible voting equipment might provide an automated reader that converts the paper record contents into audio output. Subsection 3.3.1.e also applies.

8 Quality Assurance and Configuration Management

Table of Contents

---

8 Quality Assurance and Configuration Management

The quality assurance and configuration management requirements discussed in this section help assure that voting systems conform to the requirements of the VVSG. Quality Assurance is a manufacturer function with associated practices that is initiated prior to system development and continues throughout the maintenance life cycle of the voting system. Quality Assurance focuses on building quality into a system and reducing dependence on system tests at the end of the life cycle to detect deficiencies, thus helping ensure that the system:

- Meets stated requirements and objectives;
- Adheres to established standards and conventions;
- Functions consistent with related components and meets dependencies for use within the jurisdiction; and
- Reflects all changes approved during its initial development, internal testing, qualification, and, if applicable, additional certification processes.

Configuration management is a set of activities and associated practices that ensures full knowledge and control of the components of a system, starting with its initial development progressing through its ongoing maintenance and enhancement, and including its operational life cycle.

8.1 Standards based framework for Quality Assurance and Configuration Management

The requirement in this section establishes the quality assurance and configuration standards for voting system to which manufacturers must conform. The requirement to develop a Quality and Configuration Management manual, and the detailed requirements on that manual, are contained in Volume II Section 2.11.

a. Voting system manufacturers **shall** implement a quality assurance and configuration management program that is conformant with the recognized ISO standards in these areas:
   i. ISO 9000:2005;
   ii. ISO 9001:2000; and
   iii. ISO 10007:2003.

8.2 Configuration Management Requirements

This section specifies the key configuration management requirements for voting system manufacturers. The requirements include those of equipment tags and configuration logs. Continuation of the program, in the form of usage logs, is the responsibility of State and local officials.

a. Each voting system **shall** have an identification tag that is attached to the main body. The tag **shall** be tamper-resistant and difficult to remove. The tag **shall** contain the following information:
    i. The voting system model identification in the form of a model number and possibly a model name. The model identification identifies the exact variant or version of the system;
    ii. The serial number that uniquely identifies the system;
    iii. Identification of the manufacturer, including address and contact information for technical service, and manufacturer certification information; and
    iv. Date of manufacture of the voting system.
    v. The system's power requirements, if applicable.
b. For each voting system manufactured, a Voting System Configuration Log **shall** be established. The Log is initialized by the configuration data supplied by the manufacturer. From that point on, it functions like a diary of the system. Entries are made by election officials whenever any change occurs. Every exception, disruption, anomaly, and every failure is recorded. Every time the cover is opened for inspection or a repair or maintenance is performed, an entry details what was done, and what component was changed against what other component, as well as any diagnosis of failures or exceptions. The Log **shall** be kept on a medium that allows the writing, but not the modification or deletion, of records. The Log **shall** contain the following information:
    i. The information on the system tag described in Requirement a;
    ii. The identification of all critical parts, components, and assemblies of the system; and
    iii. The complete historical record, as developed by the manufacturer per Requirement II.2.11.l, of all critical parts, components, and assemblies included in the voting system.

The list of critical parts, components, and assemblies should be consistent with the rules for determining which of these entities is critical, as specified in the Quality and Configuration Manual. See Requirement II.2.11.f.

Appendix A Glossary

Table of Contents

Appendix A: Glossary

This glossary contains terms needed to understand voting systems and related areas such as security, human factors, and testing. Sources consulted in preparing the definitions are listed in section A.2.

A.1 Glossary

A

abandoned ballot: Ballot that the voter did not place in the ballot box or record as cast on DRE before leaving the polling place

absentee ballot: Ballot cast by a voter unable to vote in person at his or her polling place on Election Day

acceptance testing: Examination of a voting system and its components by the purchasing election authority (usually in a simulated-use environment) to validate performance of delivered units in accordance with procurement requirements, and to validate that the delivered system is, in fact, the certified system purchased

Access Board: Independent federal agency whose primary mission is accessibility for people with disabilities and a leading source of information on accessible design

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 and mobility, as well as cognitive disabilities.

Accessible Voting Station (Acc-VS): Voting station specially equipped for individuals with disabilities referred to in HAVA 301 (a)(3)(B).

accreditation: Formal recognition that a laboratory is competent to carry out specific tests or calibrations

accreditation body: (1) Authoritative body that performs accreditation (2) An independent organization responsible for assessing the performance of other organizations against a recognized standard, and for formally confirming the status of those that meet the standard

accuracy: (1) Extent to which a given measurement agrees with an accepted standard for that measurement (2) Closeness of the agreement between the result of a measurement

and a true value of the particular quantity subject to measurement. Accuracy is a qualitative concept and is not interchangeable with precision.

accuracy for voting systems: Ability of the system to capture, record, store, consolidate and report the specific selections and absence of selections, made by the voter for each ballot position without error. Required accuracy is defined in terms of an error rate that for testing purposes represents the maximum number of errors allowed while processing a specified volume of data.

adequate security: Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, unauthorized access to, or modification of, information. This includes ensuring that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

alert time: The amount of time the system will wait for detectible voter activity after issuing an alert before going into an inactive state requiring poll worker intervention.

alternative format: The ballot or accompanying information is said to be in an alternative format if it is in a representation other than the standard ballot language and format. Examples include, but are not limited to languages other than English, Braille, ASCII text, large print, recorded audio.

application logic: Software, firmware, or hardwired logic from any source that is specific to the voting system, with the exception of border logic.

audio ballot: a ballot in which a set of offices is presented to the voter in spoken, rather than written, form

audio-tactile interface (ATI): Voter interface designed to not require visual reading of a ballot. Audio is used to convey information to the voter and sensitive tactile controls allow the voter to convey information to the voting system.

audit: 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

audit trail: Recorded information that allows election officials to review the activities that occurred on the voting equipment to verify or reconstruct the steps followed without compromising the ballot or voter secrecy

audit trail for direct-recording equipment: Paper printout of votes cast, produced by direct-recording electronic (DRE) voting machines, which election officials may use to crosscheck electronically tabulated totals

availability: The percentage of time during which a system is operating properly and available for use

B

ballot: The official presentation of all of the contests to be decided in a particular election. See also**, audio ballot, ballot image, video ballot, electronic ballot interface.**

ballot configuration: Particular set of contests to appear on the ballot for a particular election district, their order, the list of ballot positions for each contest, and the binding of candidate names to ballot positions

ballot counter: Process in a voting device that counts the votes cast in an election

ballot counting logic: The software logic that defines the combinations of voter choices that are valid and invalid on a given ballot and that determines how the vote choices are totaled in a given election

ballot format: The concrete presentation of the contents of a ballot appropriate to the particular voting technology being used. The contents may be rendered using various methods of presentation (visual or audio), language or graphics.

ballot image: Electronically produced record of all votes cast by a single voter. See also **cast vote record**.

ballot instructions: Information provided to the voter during the voting session that describes the procedure for executing a ballot. Such material may (but need not) appear directly on the ballot.

ballot measure: (1) A question that appears on the ballot for approval or rejection. (2) A contest on a ballot where the voter may vote yes or no.

ballot position: A specific place in a ballot where a voter's selection for a particular contest may be indicated. Positions may be connected to row and column numbers on the face of a voting machine or ballot, particular bit positions in a binary record of a ballot (for example, an electronic ballot image), the equivalent in some other form. Ballot positions are bound to specific contests and candidate names by the ballot configuration.

ballot preparation: Selecting the specific contests and questions to be contained in a ballot format and related instructions; preparing and testing election-specific software containing these selections; producing all possible ballot formats; and validating the correctness of ballot materials and software containing these selections for an upcoming election

ballot production: Process of generating ballots for presentation to voters, e.g., printing paper ballots or configuring the ballot presentation on a DRE

ballot rotation: Process of varying the order of the candidate names within a given contest

ballot scanner: Device used to read the voter selection data from a paper ballot or ballot card

ballot style: See **ballot configuration**

border logic: Software, firmware, or hardwired logic that is developed to connect application logic to COTS or third-party logic. Note: 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 must interact. It is not always possible for border logic to achieve its function while conforming to coding standards. 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.

C

callable unit: (Of a software program or analogous 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 choices on the ballot or may be a write-in candidate.

candidate register: Record that reflects the total votes cast for the candidate. This record is augmented as each ballot is cast on a DRE or as digital signals from the conversion of voted paper ballots are logically interpreted and recorded.

canvass: Compilation of election returns and validation of the outcome that forms the basis of the official results by political subdivision

cast ballot: Ballot that has been deposited by the voter in the ballot box or electronically submitted for tabulation

Cast Vote Record (CVR): Permanent record of all votes produced by a single voter whether in electronic, paper or other form. Also referred to as ballot image when used to refer to electronic ballots.

catastrophic system failure: Total loss of function or functions, such as the loss or unrecoverable corruption of voting data or the failure of an on board battery of volatile memory

central count voting system: A voting system that tabulates ballots from multiple precincts at a central location. Voted ballots are placed into secure storage at the polling place. Stored ballots are transported or transmitted to a central counting place which produces the vote count report.

certification: Procedure by which a third party gives written assurance that a product, process or service conforms to specified requirements. See also **state certification** and **national certification.**

certification testing: Testing performed under either national or state certification processes to verify voting system conformance to requirements

challenged ballot: Ballot provided to an individual who claim they are registered and eligible to vote but whose eligibility or registration status cannot be confirmed when they present themselves to vote. Once voted, such ballots must be kept separate from other ballots and are not included in the tabulation until after the voter's eligibility is confirmed. Michigan is an exception in that they determine voter eligibility before a ballot is issued. See also **provisional ballot**

checksum: Value computed from the content of a document or data record. Typically this is the sum of the numeric representations of all the characters in the text. Checksums are used to aid in detecting errors or alterations during transmission or storage.

claim of conformance: Statement by a manufacturer declaring that a specific product conforms to a particular standard or set of standard profiles; for voting systems, NASED qualification or EAC certification provides independent verification of a claim

closed primary: Primary election in which voters receive a ballot listing only those candidates running for office in the political party with which the voters are affiliated. In some states, non-partisan contests and ballot issues may be included. In some cases, political parties may allow unaffiliated voters to vote in their party's primary

Common Industry Format (CIF): Format to be used for summative usability test reporting, described in ISO/IEC 25062:2006 "Common Industry Format (CIF) for Usability Test Reports"

completed system response time: The time taken from when the voter performs some detectible action to when the voting system completes its response and settles into a stable state (e.g., finishes "painting" the screen with a new page).

component: Element within a larger system; a component can be hardware or software. For hardware, it is a physical part of a subsystem that can be used to compose larger systems (e.g., circuit boards, internal modems, processors, computer memory). For software, it is a module of executable code that performs a well-defined function and interacts with other components.

confidentiality: Prevention of unauthorized disclosure of information

configuration management: Discipline applying technical and administrative direction and surveillance to identify and document functional and physical characteristics of a configuration item, control changes to these characteristics, record and report change processing and implementation status, and verify compliance with specified requirements

configuration management plan: Document detailing the process for identifying, controlling and managing various released items (such as code, hardware and documentation)

configuration status accounting: An element of configuration management, consisting of the recording and reporting of information needed to manage a configuration effectively. This includes a listing of the approved configuration identification, the status of proposed changes to the configuration, and the implementation status of approved changes.

conformance: Fulfillment of specified requirements by a product, process or service

conformance testing: Process of testing an implementation 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. Also known as certification testing.

contest: Decision to be made within an election, which may be a contest for office or a referendum, proposition and/or question. A single ballot may contain one or more contests.

COTS: Software, firmware, device or component that is used in the United States by many different people or organizations for many different applications and that is incorporated into the voting system with no manufacturer- or application-specific modification. Note: (1) The expansion of COTS as Commercial Off-The-Shelf is no longer helpful, since much of what satisfies the requirements is non-commercial software that is not available in stores. The acronym COTS is used here only because it is familiar to the audience. (2) By requiring "many different applications," this definition deliberately prevents any application logic from receiving a COTS designation.

count: Process of totaling votes. See **tabulation.**

counted ballot: Ballot that has been processed and whose votes are included in the candidates and measures vote totals

corrective action: Action taken to eliminate the causes of an existing deficiency or other undesirable situation in order to prevent recurrence

critical failure: Functional failure the occurrence of which jeopardizes the validity of the election or casts doubt on the credibility of the election result.

cross filing: 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. Also referred to as cross-party endorsement.

cryptographic key: Value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification

cryptography: Discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, prevent their undetected modification and establish their authenticity

cumulative voting: A method of voting exclusive to multi-member district election (e.g. county board) in which each voter may cast as many votes as there are seats to be filled and may cast two or more of those votes for a single candidate

D

decertification: Revocation of national or state certification of voting system hardware and software

decryption: Process of changing encrypted text into plain text

device: Functional unit that performs its assigned tasks as an integrated whole

digital signature: An asymmetric key operation where the private key is used to digitally sign an electronic document and the public key is used to verify the signature. Digital signatures provide data authentication and integrity protection

direct-recording electronic (DRE) voting system: Combination Accessible Voting Station and tabulator that gathers votes via an electronic ballot interface, records voting data and ballot images in memory components, and produces a tabulation of the voting data. Note: A typical DRE presents contest choices to the voter on an electronic monitor, and after the voter finishes the ballot the voter's votes are stored locally on the computer.

directly verifiable: Voting system feature that allows the voter to verify at least one representation of his or her ballot with his/her own senses, not using any software or hardware intermediary. Examples include a marksense paper ballot and a DRE with a voter verifiable paper record feature.

disability: With respect to an individual; (1) a physical or mental impairment that substantially limits one or more of the major life activities of such individual; (2) a record of such an impairment; (3) being regarded as having such an impairment (definition from the Americans with Disabilities Act).

dynamic voting system software: Software that changes over time once it is installed on the voting equipment. See also voting system software.

E

EAC: Election Assistance Commission (www.eac.gov)

early voting: Broadly, voting conducted before Election Day where the voter completes the ballot in person at a county office or other designated polling place or ballot drop site prior to Election Day

election: A formal process of selecting a person for public office or of accepting or rejecting a political proposition by voting

election databases: Data file or set of files that contain geographic information about political subdivisions and boundaries, all contests and questions to be included in an election, and the candidates for each contest

election definition: Definition of the contests and questions that will appear on the ballot for a specific election

election district: Contiguous geographic area represented by a public official who is elected by voters residing within the district boundaries. The district may cover an entire state or political subdivision, may be a portion of the state or political subdivision, or may include portions of more than one political subdivision.

election management system: Set of processing functions and databases within a voting system that defines, develops and maintains election databases, performs election definitions and setup functions, format ballots, count votes, consolidates and report results, and maintains audit trails

election officials: The people associated with administering and conducting elections, including government personnel and poll workers

election programming: Process by which election officials or their designees use voting system software to logically define the ballot for a specific election

electronic ballot interface: Subsystem within a voting system which communicates ballot information to a voter in video, audio or other alternative format which allows the voter to select candidates and issues by means of vocalization or physical actions

electronic cast vote record: An electronic version of the cast vote record

electronic voting machine: Any system that utilizes an electronic component. Term is generally used to refer to DREs. See also voting equipment, voting system.

electronic voting system: An electronic voting system is one or more integrated devices that utilize an electronic component for one or more of the following functions: ballot presentation, vote capture, vote recording, and tabulation. A DRE is a functionally and physically integrated electronic voting system which provides all four functions electronically in a single device. An optical scan (also known as marksense) system where the voter marks a paper ballot with a marking instrument and then deposits the ballot in a tabulation device is partially electronic in that the paper ballot provides the presentation, vote capture and vote recording functions. An optical scan system employing a ballot marking device adds a second electronic component for ballot presentation and vote capture functions.

Electronically-assisted Ballot Marker (EBM): Accessible Voting Station that produces an executed, human-readable paper ballot as a result, and that does not make any other lasting record of the voter's votes. Note: One kind of EBM presents contest choices to the voter on an electronic monitor; after the voter finishes the ballot, the voter's choices are printed on a paper ballot that is the only record of the voter's choices. However, vote-by-telephone systems that are in use at the time of this writing are also EBMs. The voter uses an audio interface (remotely) and a paper ballot is produced (centrally). An EBM may mark ballot positions on a pre-printed ballot or it may print an entire ballot; however, in any event, the ballot produced is assumed to be human-readable and comparable to a manually-marked paper ballot.

encryption: Process of obscuring information by changing plain text into ciphertext for the purpose of security or privacy. See also **cryptography** and **decryption**.

error correcting code: coding system that allows data being read or transmitted to be checked for errors and, when detected, corrects those errors

F

failure: (Voting system reliability) Event that results in (a) loss of one or more functions, (b) degradation of performance such that the device is unable to perform its intended function for longer than 10 seconds, (c) automatic reset, restart or reboot of the voting device, operating system or application software, (d) a requirement for an unanticipated intervention by a person in the role of poll worker or technician before normal operation can continue, or (e) error messages and/or audit log entries indicating that a failure has occurred. Discussion: In plain language, failures are equipment breakdowns, including software crashes, such that continued use without service or replacement is worrisome to impossible. Normal, routine occurrences like running out of paper are not considered failures. Misfeeds of ballots into optical scanners are handled by a separate benchmark (Requirement 4.1.5.1.f), so these are not included as failures for the general reliability benchmark.

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.

firmware: Computer programming stored in programmable read-only memory thus becoming a permanent part of the computing device. It is created and tested like software.

Functional Configuration Audit (FCA): Exhaustive verification of every system function and combination of functions cited in the manufacturer’s documentation. The FCA verifies the accuracy and completeness of the system’s Voter Manual, Operations Procedures, Maintenance Procedures, and Diagnostic Testing Procedures.

functional test: Test performed to verify or validate the accomplishment of a function or a series of functions

G

general election: Election in which voters, regardless of party affiliation, are permitted to select candidates to fill public office and vote on ballot issues

guidelines: See **product standard**

H

hash: Algorithm that maps a bit string of arbitrary length to a fixed-length bit string.

hash function: A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties: 1. (One-way) It is computationally infeasible to find any input that maps to any pre-specified output, and 2. (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output.

hardwired logic: Logic implemented through the design of an integrated circuit; the programming of a Programmable Logic Device (PLD), Field-Programmable Gate Array (FPGA), Peripheral Interface Controller (PIC), or similar; the integration of smaller hardware components; or mechanical design (e.g., as in lever machines).

I

indirectly verifiable: Voting system feature that allows a voter to verify his or her selections via a hardware or software intermediary. An example is a touch screen DRE where the voter verifies the ballot selections through the assistance of audio stimuli.

implementation statement: Statement by a manufacturer indicating the capabilities, features, and optional functions as well as extensions that have been implemented. Also known as implementation conformance statement.

Independent Testing Authority (ITA): Replaced by “accredited testing laboratories” and “VSTL” (Voting System Test Lab). Prior usage referred to independent testing organizations accredited by the National Association of State Election Directors (NASED) to perform voting system qualification testing.

information security: Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability

initial system response time: The time taken from when the voter performs some detectible action (such as pressing a button) to when the voting system begins responding in some obvious way (such as an audible response or any change on the screen).

inspection: Examination of a product design, product, process or installation and determination of its conformity with specific requirements or, on the basis of professional judgment, with general requirements. Inspection of a process may include inspection of staffing, facilities, technology and methodology.

integrity: Guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity

internal audit log: A human readable record, resident on the voting machine, used to track all activities of that machine. This log records every activity performed on or by the machine indicating the event and when it happened.

K

key management: Activities involving the handling of cryptographic keys and other related security parameters (e.g., passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization.

L

logic and accuracy testing: Testing of the tabulator setups of a new election definition to ensure that the content correctly reflects the election being held (i.e., contests, candidates, number to be elected, ballot styles) and that all voting positions can be voted for the maximum number of eligible candidates and that results are accurately tabulated and reported.

logical correctness: Condition signifying that, for a given input, a computer program will satisfy the program specification and produce the required output

logic defect: Fault in software, firmware, or hardwired logic.

M

marksense: System by which votes are recorded by means of marks made in voting response fields designated on one or both faces of a ballot card or series of cards. Marksense systems may use an optical scanner or similar sensor to read the ballots. Also known as optical scan.

measure register: Record that reflects the total votes cast for and against a specific ballot issue. This record is augmented as each ballot is cast on a DRE or as digital signals from the conversion of voted paper ballots are logically interpreted and recorded.

mechanical lever voting machine: Machine that directly records a voter's choices via mechanical lever-actuated controls into a counting mechanism that tallies the votes without using a physical ballot

module: Structural unit of software or analogous logical design, typically containing several callable units that are tightly coupled. Note: Modular design requires that inter-module coupling be loose and occur over defined interfaces. A module should contain all elements needed to compile or interpret successfully and have limited access to data in other modules. A module should be substitutable with another module whose interfaces match the original module. In software, a module typically corresponds to a single source code file or a source code / header file pair. In object-oriented languages, this typically corresponds to a single class of object.

multi-seat contest: Contest in which multiple candidates can run, up to a specified number of seats. Voters may vote for no more than the specified number of candidates

N

NASED: National Association of State Election Directors**, (**www.nased.org**)**

national certification testing: Examination and testing of a voting system to determine if the system complies with the performance and other requirements of the national certification standards and with its own specifications

national certification test report: Report of results of independent testing of a voting system by a VSTL delivered to the EAC with a recommendation regarding granting a certification number

NIST: National Institute of Standards and Technology

NIST approved: An algorithm or technique that for which at least one of the following is true:

a. is specified in a FIPS or NIST Recommendation,
b. is adopted in a FIPS or NIST Recommendation, or
c. is specified in a list of NIST approved security functions (e.g., specified as approved in the annexes of FIPS 140-2)

non-partisan office: Elected office for which candidates run without political party affiliation

non-user-serviceable failure: Functional failure that requires the manufacturer or highly trained personnel to repair.

nonvolatile memory: Memory in which information can be stored indefinitely with no power applied. ROMs and PROMs are examples of nonvolatile memory.

NVLAP: The National Voluntary Laboratory Accreditation Program operated by NIST

O

open primary: Primary election in which any voters can participate, regardless of their political affiliation. Some states require voters to publicly declare their choice of party ballot at the polling place, after which the poll worker provides or activates the appropriate ballot. Other states allow the voters to make their choice of party ballot within the privacy of the voting booth.

operational environment: All software, hardware (including facilities, furnishings and fixtures), materials, documentation, and the interface used by the election personnel, maintenance operator, poll worker, and voter, required for voting equipment operations.

optical scan, optical scan system: System by which votes are recorded by means of marks made in voting response fields designated on one or both faces of a ballot card or series of cards. An optical scan system reads and tabulates ballots, usually paper ballots, by scanning the ballot and interpreting the contents. Also known as **marksense**.

overvote: Voting for more than the maximum number of selections allowed in a contest

P

paper-based voting system: Voting system that records votes, counts votes, and tabulates the vote count, using one or more ballot cards or paper ballots

paper record: Paper cast vote record that can be directly verified by a voter. See also **ballot image, cast vote record**.

partisan office: An elected office for which candidates run as representatives of a political party

personal assistive device: A device that is carried or worn by an individual with some physical impairment whose primary purpose is to help compensate for that impairment

Physical Configuration Audit (PCA): Inspection by a VSTL that compares the voting system components submitted for certification testing to the manufacturer's technical documentation and confirms that the documentation submitted meets the national certification requirements. Includes witnessing of the build of the executable system to ensure that the certified release is built from the tested components.

political subdivision: Any unit of government, such as counties and cities, school districts, and water and conservation districts having authority to hold elections for public offices or on ballot issues

polling location: Physical address of a polling place

polling place: Facility to which voters are assigned to cast in-person ballots

precinct: Election administration division corresponding to a contiguous geographic area that is the basis for determining which contests and issues the voters legally residing in that area are eligible to vote on

precinct count: Counting of ballots in the same precinct in which those ballots have been cast

Precinct Count Optical Scanner (PCOS): Optical scanner used as a precinct tabulator. Note: A PCOS is a special purpose scanner designed to enable the voter to feed his or her own paper ballot—one ballot at a time.

precinct count voting system: A voting system that tabulates ballots at the polling place. These systems typically tabulate ballots as they are cast and print the results after the close of polling. For DREs, and for some paper-based systems, these systems provide electronic storage of the vote count and may transmit results to a central location over public telecommunication networks.

precinct tabulator: Tabulator that counts votes at the polling place. Note: These devices typically tabulate ballots as they are cast and print the results after the close of polls. For DREs and some paper-based systems, these devices provide electronic storage of the vote count and may transmit results to a central location over public telecommunication networks. A tabulator that may be configured for use either in the precinct or in the central location may satisfy the requirements for both Precinct tabulator and Central tabulator.

precision: (1) Extent to which a given set of measurements of the same sample agree with their mean. Thus, precision is commonly taken to be the standard deviation estimated from sets of duplicate measurements made under conditions of repeatability, that is, independent test results obtained with the same method on identical test material, in the same laboratory or test facility, by the same operator using the same equipment within short intervals of time. (2) Degree of refinement in measurement or specification, especially as represented by the number of digits given.

primary election: Election held to determine which candidate will represent a political party for a given office in the general election. Some states have an open primary, while others have a closed primary. Sometimes elections for nonpartisan offices and ballot issues are held during primary elections.

primary presidential delegation nomination: Primary election in which voters choose the delegates to the presidential nominating conventions allotted to their states by the national party committees

privacy: The ability to prevent others from determining how an individual voted

private key: The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data

product standard: Standard that specifies requirements to be fulfilled by a product or a group of products, to establish its fitness for purpose

provisional ballot: Ballot provided to individuals who claim they are registered and eligible to vote but whose eligibility or registration status cannot be confirmed when they present themselves to vote. Once voted, such ballots must be kept separate from other ballots and are not included in the tabulation until after the voter's eligibility is confirmed. In some jurisdictions called an affidavit ballot. See also **challenged ballot**.

public key: Public part of an asymmetric key pair that is typically used to verify digital signatures or encrypt data

public network direct-recording electronic (DRE) voting system: A DRE that transmits vote counts to a central location over a public telecommunication network

Q

qualification number: A number issued by NASED (National Association of State Election Directors) to a system that has been tested by an accredited Independent Testing Authority for compliance with the voting system standards. Issuance of a qualification number indicates that the system conforms to the national standards.

qualification test report: Report of results of independent testing of a voting system by an Independent Test Authority documenting the specific system configuration tested, the scope of tests conducted and when testing was completed.

qualification testing: Examination and testing of a voting system by a NASED-accredited Independent Test Authority to determine if the system conforms to the performance and other requirements of the national certification standards and the manufacturer's own specifications.

R

ranked order voting: Practice that allows voters to rank candidates in a contest in order of choice: 1, 2, 3 and so on. A candidate receiving a majority of the first choice votes wins that election. If no candidate receives a majority, the last place candidate is deleted, and all ballots are counted again, with each ballot cast for the deleted candidate applied to the next choice candidate listed on the ballot. The process of eliminating the last place candidate and recounting the ballots continues until one candidate receives a majority of the vote. The practice is also known as instant runoff voting, preferences or preferential voting, or choice voting.

recall issue with options: Process that allows voters to remove elected representatives from office prior to the expiration of their terms of office. The recall may involve not only the question of whether a particular officer should be removed, but also the question of naming a successor in the event that there is an affirmative vote for the recall.

recertification: Re-examination, and possibly retesting of a voting system that was modified subsequent to receiving national and/or state certification. The object of is to determine if the system as modified still conforms to the requirements.

recount: Retabulation of the votes cast in an election

referendum: Process whereby a state law or constitutional amendment may be referred to the voters before it goes into effect.

reporting context: Scope within which reported totals or counts are calculated (e.g., precinct or election district).

reproducibility: Ability to obtain the same test results by using the same test method on identical test items in different testing laboratories with different operators using different equipment

requirement: Provision that conveys criteria to be fulfilled

residual vote: Total number of votes that cannot be counted for a specific contest. There may be multiple reasons for residual votes (e.g., declining to vote for the contest, overvoting in a contest).

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

runoff election: Election to select a winner following a primary or a general election, in which no candidate in the contest received the required minimum percentage of the votes cast. The two candidates receiving the most votes for the contest in question proceed to the runoff election.

S

secure receptacle: The container for storing VVPAT paper audit records

security analysis: An inquiry into the potential existence of security flaws in a voting system. Includes an analysis of the system's software, firmware, and hardware, as well as the procedures associated with system development, deployment, operation and management.

security controls: Management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

security strength: A number associated with the amount of work (that is, the number of operations) that is required to break a cryptographic algorithm or system.

semi-static voting system software: Software that may change in response to the voting equipment on which it is installed or to election-specific programming.

split precinct: A precinct that contains an election district subdivision, e.g., a water district or school board district, requiring an additional ballot configuration

spoiled ballot: Ballot that has been voted but will not be cast

state certification: State examination and possibly testing of a voting system to determine its compliance with state requirements for voting systems

static voting system software: Software that does not change based on the election being conducted or the voting equipment upon which it is installed, e.g., executable code

straight party voting: Mechanism that allows voters to cast a single vote to select all candidates on the ballot from a single political party

summative usability testing: Evaluation of a product with representative users and tasks designed to measure the usability (defined as effectiveness, efficiency and satisfaction) of the complete product. The purpose of a summative test is to evaluate a product through defined measures, rather than diagnosis and correction of specific design problems, as in formative testing.

support software: Software that aids in the development, maintenance, or use of other software, for example, compilers, loaders and other utilities

symmetric (secret) encryption algorithm: Encryption algorithms using the same secret key for encryption and decryption

T

tabulation: Process of totaling votes**.** See also **count.**

tabulator: Device that counts votes. Note: Any distinction between processing individual votes and processing vote totals that resulted from a previous step is not relevant; both of these constitute “counting votes”.

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.

technical data package: Manufacturer documentation relating to the voting system required to be submitted with the system as a precondition of certification testing

telecommunications: Transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received

test: Technical operation that consists of the determination of one or more characteristics of a given product, process or service according to a specified procedure

test campaign: Sum of the work by a VSTL on a single product or system from contract through test plan, conduct of testing for each requirement (including hardware, software, and systems), reporting, archiving, and responding to issues afterwards

testing standard: Standard that is concerned with test methods, sometimes supplemented with other provisions related to testing, such as sampling, use of statistical methods or sequence of tests

test method: Specified technical procedure for performing a test

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; e.g., general-purpose software developed by a third party that is either customized (e.g., ported to a new platform, as is Windows CE[40]) or not widely used, or source code generated by a COTS package.

touch screen voting machine: A voting machine that utilizes a computer screen to display the ballot and allows the voter to indicate his or her selections by touching designated locations on the screen

U

undervote: Occurs when the number of choices selected by a voter in a contest is less than the maximum number allowed for that contest or when no selection is made for a single choice contest

40 Specific equipment and materials are identified in order to describe certain procedures. In no case does such identification imply recommendation or endorsement, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

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 ballot choices were recorded correctly. It also refers to the usability of the setup and operation in the polling place of voting equipment.

usability testing: Encompasses a range of methods that examine how users in the target audience actually interact with a system, in contrast to analytic techniques such as usability inspection

user-serviceable failure: Functional failure that can be remedied by a troubleshooter and/or election official using only knowledge found in voting equipment user documentation.

V

valid vote: Vote from a ballot or ballot image that is legally acceptable according to state law

validation: Process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements

verification: Process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions (such as specifications) imposed at the start of the phase

video ballot: Electronic ballot interface which presents ballot information and voting instructions as video images. See also **ballot**.

vote for N of M: A multi-seat contest in which voters are allowed to vote for a specified number ("N") of candidates.

voted ballot: Ballot that contains all of a voter's selections and has been cast

voter inactivity time: The amount of time from when the system completes its response until there is detectible voter activity. In particular, note that audio prompts from the system may take several minutes and that this time does not count as voter inactivity.

voter verifiable: A voting system feature that provides the voter an opportunity to verify that his or her ballot selections are being recorded correctly, before the ballot is cast

voter verifiable audit record: Human-readable printed record of all of a voter's selections presented to the voter to view and check for accuracy

voting device: Device that is part of the voting system. Note: Components and materials that are vital to the function of the voting device within the voting system, such as smart

cards and ballot printers, are considered parts of the device for the purpose of conformity assessment.

voting equipment: All devices, including the voting machine, used to display the ballot, accept voter selections, record voter selections, and tabulate the votes

voting machine: The mechanical, electromechanical and electric components of a voting system that the voter uses to view the ballot, indicate their selections, verify their selections. In some instances, the voting machine also casts and tabulates the votes. See **voting equipment**.

voting officials: Term used to designate the group of people associated with elections, including election personnel, poll workers, ballot designers and those responsible for the installation, operation and maintenance of the voting systems.

voting position: Specific response field on a ballot where the voter indicates the selection of a candidate or ballot proposition response

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 as well as the voting machine. See **voting machine.**

voting system: The total combination of mechanical, electromechanical or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment) that is used to define ballots; to cast and count votes; to report or display election results; and to maintain and produce any audit trail information; and the practices and associated documentation used to identify system components and versions of such components; to test the system during its development and maintenance; to maintain records of system errors and defects; to determine specific system changes to be made to a system after the initial qualification of the system; and to make available any materials to the voter (such as notices, instructions, forms or paper ballots). Note: An Automatic Bar Code Reader is considered part of a voting system based on the definition of a voting system. Specifically, the Automatic Bar Code Reader "supports" the system and is used to produce audit trail information, therefore it must be included as part of the testing of a voting system.[41]

voting system software: All the executable code and associated configuration files needed for the proper operation of the voting system. This includes third party software such as operating systems, drivers, and database management tools. See also **dynamic voting system software, semi-static voting system software**, and **static voting system software**.

voting system testing: Examination and testing of a computerized voting system by using test methods to determine if the system complies with the requirements in the *Voluntary Voting System Guidelines* and with its own specifications.

---

41 The italicized test is based on EAC Decision on Request for Interpretation 2008-08, http://www.eac.gov/assets/1/Page/EAC%20Decision%20on%20Automatic%20Bar%20Code%20Readers.pdf.

Voting System Test Lab (VSTL): Test laboratory accredited by the Election Assistance Commission under the EAC's Voting System Testing and Certification Program.

W

write-in voting: To make a selection of an individual not listed on the ballot. In some jurisdictions, voters may do this by using a marking device to physically write their choice on the ballot or they may use a keypad, touch screen or other electronic means to enter the name.

A.2 Sources

Definitions in this glossary are either extracted from or based on the following sources:

44 U.S.C. 35	United States Code, Title 44, Chapter 35, Information Security, Section 3542, Definitions.
ACM SIGCHI	ACM's Special Interest Group on Computer-Human Interaction, http://www.acm.org/sigchi/ (February 2005).
ADA	Americans with Disabilities Act of 1990.
ANSI Dictionary	American National Dictionary for Information Processing Systems, American National Standards Committee X3, Information Processing Systems, 1982.
ANSI 354	American National Standards Institute, International Committee for Information Technology Standards, Common Industry Format for Usability Test Reports, ANSI/INCITS 354-2001
ANSI C63.19	American National Standards for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, 2001.
electionline	http://electionline.org/, (March 2005).
FIPS 81	Federal Information Processing Standard 81, DES Modes of Operations, December, 1980.
FIPS 140-2	Federal Information Processing Standard 140-2, Security Requirements for Cryptographic Modules, May 2001.
FIPS 199	Federal Information Processing Standard 199, Standards for Security Categorization of Federal Information and Information Systems, December 2003.

FIPS 201	Federal Information Processing Standard 201, Personal Identity Verification for Federal Employees and Contractors, February 2005.
HAVA	Help America Vote Act of 2002 - Public Law 107-252.
IEA	International Ergonomics Association, http://www.iea.cc/, (February 2005).
IEEE 1583	IEEE P1583/D5.3.2 Draft Standard for the Evaluation of Voting Equipment, December 6, 2004.
ISO 5725	ISO/IEC 5725:1994 Accuracy (trueness and precision) of measurement methods and results.
ISO 9241	ISO/IEC 9241:1997 Ergonomic requirements for office work with visual display terminals (VDT).
ISO 17000	ISO/IEC 17000:2004 Conformity assessment -- Vocabulary and general principles.
ISO Guide 2-4	ISO/IEC Guide 2:2004 Standardization and related activities - General vocabulary.
ISO Guide 2-6	ISO/IEC Guide 2:1996 Standardization and related activities - General vocabulary.
NASS	National Association of Secretaries of State Election Reform Key Terms, http://www.nass.org/Election%20Reform%20Key%20Terms.pdf (February 2005).
NIST HB 143	NIST Handbook 143 State Weights and Measures Laboratories Program Handbook.
NIST HB 150	NIST Handbook 150:2001 NVLAP Procedures and General Requirements.
NIST HF Rpt.	NIST Special Publication 500-256 Improving the Usability and Accessibility of Voting Systems and Products, May 2004.
NIST SP 800-30	NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems, July 2002.
NIST SP 800-49	NIST Special Publication 800-49 Federal S/MIME V3 Client Profile, November 2002.

NIST SP 800-53	NIST Special Publication 800-53 Recommended Security Controls for Federal Information Systems, Appendix B, Glossary.
NIST SP 800-59	NIST Special Publication 800-59 Guideline for Identifying an Information System as a National Security System, August 2003.
NIST SP 800-63	NIST Special Publication 800-63 Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology, June 2004.
OMB A130	OMB Circular A-130, Appendix III.
Section 508 of the Rehabilitation Act of 1973, as amended.	Electronic and Information Technology Accessibility Standards (2002) Architectural and Transportation Barriers Compliance Board, 36 CRF Part 1194, http://www.accessboard.gov/sec508/508standards.htm
Usability Glossary	Usability First Usability Glossary, http://www.usabilityfirst.com/glossary/main.cgi, (February 2005).
VIM	The ISO International Vocabulary of Basic and General Terms in Metrology (VIM), 1994.
VSS	2002 Voting Systems Standards, Volumes I and II. Federal Election Commission.
Whatis.com	http://whatis.com, IT Encyclopedia

Appendix B References

Table of Contents

Appendix B: References

B.1 Documents Incorporated in the Guidelines

The following publications have been incorporated into the Guidelines. When specific provisions from these publications have been incorporated, specific references are made in the body of the Guidelines.

Federal Regulations

Code of Federal Regulations, Title 29, Part 1910, Occupational Safety and Health Act

Code of Federal Regulations, Title 36, Part 1194, Architectural and Transportation Barriers Compliance Board, Electronic and Information Technology Standards - Final Rule

Code of Federal Regulations, Title 47, Parts 15 and 18, Rules and Regulations of the Federal Communications Commission

Code of Federal Regulations, Title 47, Part 15, "Radio Frequency Devices", Subpart J, "Computing Devices", Rules and Regulations of the Federal Communications Commission

International Organization for Standardization (ISO)

ISO 9001:2000	Quality Management Systems – Requirements
ISO 10007:2003	Quality Management Systems – Guidelines for Configuration Management
ISO 9000:2005	Quality Management Systems – Fundamentals and Vocabulary

American National Standards Institute (ANSI)

ANSI C63.4	Methods of Measurement of Radio-Noise Emissions from Low-Voltage Electrical and Electronic Equipment in the Range of 9Khz to 40 GHz
ANSI C63.19	American National Standard for Methods of Measurement of Compatibility between Wireless Communication Devices and Hearing Aids

ANSI-NCITS	Industry Usability Reporting and the Common Industry Format 354-2001

International Electrotechnical Commission (IEC)

IEC 61000-4-2 (2008-12) Ed. 2.0	Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques. Section 2 Electrostatic Discharge Immunity Test (Basic EMC publication).
IEC 61000-4-3 (1996)	Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques. Section 3 Radiated Radio-Frequency Electromagnetic Field Immunity Test.
IEC 61000-4-4 (2004-07) Ed. 2.0	Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques. Section 4 Electrical Fast Immunity Test.
IEC 61000-4-5 (1995-02)	Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques. Section 5 Surge Immunity Test.
IEC 61000-4-6 (1996-04)	Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques. Section 6 Immunity to Conducted Disturbances Induced by Radio-Frequency Fields.
IEC 61000-4-8 (1993-06)	Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques. Section 8 Power-Frequency Magnetic Field Immunity Test. (Basic EMC publication).
IEC 61000-4-11 (1994-06)	Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques. Section 11. Voltage Dips, Short Interruptions and Voltage Variations Immunity Tests.
IEC 61000-5-7 Ed. 1.0 b:2001	Electromagnetic compatibility (EMC) Part 5-7: Installation and mitigation guidelines—Degrees of protection provided by enclosures against electromagnetic disturbances

National Institute of Standards and Technology

FIPS 140-2	Security Requirements for Cryptographic Modules
FIPS 180-2	Secure Hash Standard, August 2002
FIPS 186-2	Digital Signature Standard, February 2000
FIPS 188	Standard Security Label for Information Transfer
FIPS 196	Entity Authentication Using Public Key Cryptography

FIPS 197	Advanced Encryption Standard (AES)
SP 800-63	Electronic Authentication Guideline, Version 1.0.1

Military Standards

MIL-STD-498	Software Development and Documentation Standard, 1989
MIL-STD-810D(2)	Environmental Test Methods and Engineering Guidelines, 19 July 1983

B.2 Other Documents Used in Developing the Guidelines

The following publications have been used for guidance in the revision of the *Guidelines*.

American National Standards Institute (ANSI), International Organization for Standardization (ISO), International Electro-technical Commission (IEC)

ANSI/ISO/IEC R 9294.1990	Information Technology Guidelines for the Management of Software Documentation
IEC/UL 60950-1	
ISO/IEC 60950-1	Information technology— Safety—Part 1: General Requirements
ISO/IEC TR 13335-4:2000	Information technology—Guidelines for the management of IT Security—Part 4: Selection of safeguards
ISO/IEC TR 13335-3:1998	Information technology—Guidelines for the management of IT Security—Part 3 Techniques for the management of IT security
ISO/IEC TR 13335-2:1997	Information technology—Guidelines for the management of IT Security—Part 2: Managing and planning IT security
ISO/IEC TR 13335-1:1996	Information technology—Guidelines for the management of IT Security—Part 1: Concepts and models for IT security
ISO/IEC 2506206	ISO/IEC 25062:2006 Common Industry Format (CIF) for Usability Test Reports.

Electronic Industries Alliance Standards

MB2, MB5, MB9	Maintainability Bulletins
EIA 157	Quality Bulletin

EIA QB2-QB5	Quality Bulletins
EIA RB9	Failure Mode and Effect Analysis, Revision 71
EIA SEB1—SEB4	Safety Engineering Bulletins
RS-232-C	Interface Between Data Terminal Equipment and Data Communications Equipment Employing Serial Binary Data Interchange
RS-366-A Calling	Interface Between Data Terminal Equipment and Automatic Equipment for Data Communication
RS-404	Standard for Start-Stop Signal Quality Between Data Terminal Equipment and Non-synchronous Data Communication Equipment

National Institute of Standards and Technology

NIST SP 800-57	NIST Special Publication 800-57: Recommendation for Key Management – Part 1: General
NISTIR 7519	Style Guide for Voting System Documentation, http://www.nist.gov/itl/vote/upload/NISTIR-7519.pdf
NISTIR 7537	Guidelines for Using Color in Voting Systems, http://www.nist.gov/itl/vote/upload/NISTIR-7537.pdf
NISTIR 4909	Software Quality Assurance: Documentation and Reviews

Institute of Electrical and Electronics Engineers

610.12-1990	IEEE Standard Glossary of Software Engineering Terminology
730-1998	IEEE Standard for Software Quality Assurance Plans
828-1998	IEEE Standard for Software Configuration Management Plans
829-1998	IEEE Standard for Software Test Documentation
830-1998	IEEE Recommended Practice for Software Requirements Specifications

Military Standards

MIL-STD-498	Software Development and Documentation, 27 May 1998

B.3 Legislation References

Help America Vote Act, Pub. L. 107-252, 42 USC Sections 15301-15545

Americans With Disabilities Act of 1990, Pub. L. 101-336, 42 USC Sections 12101-12213

42 USC 1974

Occupational Safety and Health Act, Pub. L. 91-596, 29 USC Sections 651-678, 42 USC Section 3142-1

Architectural Barriers Act of 1968, Pub. L. 90-480, 42 USC Sections 4151-4157

Voting Rights Act of 1965, Pub. L. 89-110, 42 USC Sections 1973; 1973a-p; 1973aa; 1973aa-1-6; 1973bb; 1973bb-1

B.4 Additional References

The following publications contain information that is useful in understanding and complying with the *Guidelines*.

American National Standards Institute (ANSI), International Organization for Standardization (ISO), International Electro-technical Commission (IEC)

ANSI/ISO/IEC TR 10176.1998	Information Technology Guidelines for the Preparation of Programming Language Standards
ANSI/ISO/IEC 6592.2000	Information Technology Guidelines for the Documentation of Computer Based Application Systems
ANSI X9.31-1998	Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry, 1998
ANSI X9.62-1998	Public Key Cryptography for Financial Services Industry: The Elliptic Curve Digital Signature Algorithm, 1998
ISO/IEC 9594-8:2001	ITU-T Recommendation X.509 (2000), Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks

National Institute of Standards and Technology

FIPS 102	Guideline for Computer Security Certification and Accreditation

FIPS 112	Password Usage (3)
FIPS 113	Computer Data Authentication

***Institute of Electrical and Electronics* Engineers**

488-1987	IEEE Standard Digital Interface for Programmable Instrumentation
796-1983	IEEE Standard Microcomputer System Bus IEEE/ANSI Software Engineering Standards
750.1-1995	IEEE Guide for Software Quality Assurance Planning
1008-1987	IEEE Standard for Software Unit Testing
1016-1998	IEEE Recommended Practice for Software Design Descriptions
1012-1998	IEEE Guide for Software Verification and Validation Plans

Military *Standards*

MIL-HDBK-454	Standard General Requirements for Electronic Equipment
MIL-HDBK-470	Maintainability Program for Systems & Equipment
MIL-HDBK-781A for	Handbook for Reliability Test Methods, Plans, and Environments Engineering, Development Qualification, and Production
MIL-STD-882	Systems Safety Program Requirements
MIL-STD-1472	Human Engineering Design Criteria for Military Systems, Equipment and Facilities
MIL-STD-973	Configuration Management, 30 September 2000

Other References

Designing for the Color-Challenged: A Challenge, by Thomas G. Wolfmaier (March 1999); http://www.sandia.gov/itg/newsletter/mar99/accessibility_color_challenged.html;

Effective Color Contrast: Designing for People with Partial Sight and Color Deficiencies, by Aries Arditi, Ph.D; http://www.lighthouse.org/color_contrast.htm

Electronic Markup Language (EML), Version 4.0, (Committee Draft) Organization for the Advancement of Structured Information Standards (OASIS), January 24, 2005

Guidelines for Writing Clear Instructions and Messages for Voters and Poll Workers, http://vote.nist.gov/032906PlainLanguageRpt.pdf

NIST Special Publication 500-256, Improving the Usability and Accessibility of Voting Systems and Products, http://vote.nist.gov

RSA Laboratories Technical Note, Public Key Cryptographic Standard (PKCS) #7: Cryptographic Message Syntax Standard, November 1, 1993

RSA Laboratories Technical Note, Extensions and Revisions to PKCS #7, May 13, 1997

The Americans with Disabilities Act Accessibility Guidelines (ADAAG 2202), Access Board; http://www.access-board.gov/adaag/html/adaag.htm