Federal Register

Wednesday,

April 12, 2006

Part II

Election Assistance Commission

2005 Voluntary Voting System Guidelines; Notice

ELECTION ASSISTANCE COMMISSION 2005

2005 Voluntary Voting System Guidelines

AGENCY: United States Election Assistance Commission.

ACTION: Notice; publication of final 2005 Voluntary Voting System Guidelines.

SUMMARY: The Help America Vote Act of 2002 (HAVA) Section 231 directs the U.S. Election Assistance Commission (EAC) to provide for the testing, certification, decertification and recertification of voting systems. HAVA Section 221 mandates the development of voluntary voting system guidelines to support this process. In 2004, the EAC formed the Technical Guidelines Development Committee (TGDC) to create an initial set of recommendations for the guidelines. The Director of the National Institute of Standards and Technology (NIST) chairs the TGDC and NIST staff provides technical support for the TGDC's work. This committee of fifteen experts began their work in July 2004 and submitted their recommendations to the EAC in May 2005. EAC reviewed and revised these recommendations and published its proposed Voluntary Voting System Guidelines in June 2005, 70 FR 37378 (June 29, 2005), beginning the ninety-day public comment period. The Commission adopted the 2005 Voluntary Voting System Guidelines on December 13, 2005. The Guidelines published here will be used to test voting systems for national certification.

FOR FURTHER INFORMATION CONTACT: Brian Hancock (Election Research Specialist), Washington, DC, (202) 566–3100, Fax: (202) 566–3127.

SUPPLEMENTARY INFORMATION:

Public Comment Process

HAVA requires publication of the proposed guidelines for public comment. HAVA further mandates a public hearing about the proposed guidelines. In addition, the guidelines must be reviewed by the EAC Board of Advisors and the EAC Standards Board.

EAC posted the proposed guidelines on its Web site and made the document available to the public in hardcopy and CD–ROM. Notice of the public comment period was published in the **Federal Register**. Both the **Federal Register** notice and the Web site provided instructions for submitting comments on-line, as well as by e-mail, postal mail and facsimile. EAC conducted three public hearings in the following locations: New York City; Pasadena, California: and Denver, Colorado. At these hearings, testimony was received from state and local election officials, the vendor community, the testing laboratories, public interest groups, academics, voting system experts, and members of the general public. All comments received were posted on the EAC Web site. The document was distributed to the Board of Advisors and the Standards Board. Each board conducted a two-day meeting to formulate recommendations.

Discussion of Comments

The EAC received 6,576 comments on the guidelines. Of this number, 4,300 were emails requesting that EAC to require voter verifiable audit trail capability for all electronic voting systems. The remaining 2,276 comments covered various sections of the document. Of this set, the majority were submitted by individuals—776 comments. The next largest number of comments (684) came from system vendors, testing laboratories, and other corporate entities. Public interest groups submitted 436 comments. Election and other government officials submitted 218 comments, and 162 comments were submitted by academics.

Some comments were of a general nature that did not specifically relate to the Guidelines document. The comments from the testing laboratories, system vendors and other corporate entities addressed voting system functional requirements and independent dual verification systems. Public interest groups focused their attention predominantly on usability and accessibility requirements for voting systems and for voter verifiable paper audit trails. Election officials commented on a variety of topics including accessibility, security, wireless communications, and voter verifiable paper trails. The academic community commented principally on security.

Volume 1, Voting System Performance Guidelines, received a total of 1,660 comments. The subject area that received the most comments was security (471), followed by the glossary (367), usability and accessibility (361), and voting system functional requirements (267). Volume 2, National Certification Testing Guidelines, received a total of 167 comments on a variety of topics: software testing (31), documentation (24), and hardware testing (11).

Consideration of Comments

The EAC reviewed and considered each comment. In some instances, EAC also gathered more information and performed additional research regarding the suggestions. There were 404 comments requiring extensive research that were forwarded to the TGDC for future consideration.

Similarly, many comments (73) dealt with election administration and procedural matters, which fall outside the scope of the VVSG. These comments were forwarded to EAC's Management Guidelines Working Group, which is developing a companion document covering these topics.

Changes to VVSG

The VVSG have been enhanced in response to comments received. The document has been reorganized and reformatted. Usability and accessibility requirements were removed from the functional requirements section and placed in a separate section. The glossary was revised to clarify definitions. Information about independent verification systems was incorporated into the security section to provide context for the voter verifiable paper audit trail requirements. Best Practices for Election Officials (Appendix C in the proposed guidelines) was removed and forwarded to the Management Guidelines Working Group for consideration.

The substantive changes made to the functional requirements section brought the language into conformance with HAVA requirements and clarified the technical specifications regarding environmental standards. Many comments about this section were carried over for future TGDC consideration because they related to complex topics such as specific testing protocols and software coding standards.

The principal substantive changes to security requirements were as follows: clarification of language regarding software distribution and generation of reference information; clarification of wireless communication discussion and requirements language; revision to VVPAT requirements related to the topics of ''Approve or Spoil the Paper Record,'' ''Equipment Security and Reliability,'' ''Preserve Voter Privacy,'' and ''Electronic and Paper Record Structure.''

The most significant changes overall were on the topics of usability and accessibility. These requirements were placed in their own section to reflect their importance and in anticipation that they will continue to expand over time. Usability requirements were placed first in the new section because these requirements apply to all voting systems. Alternative language requirements were placed under the usability heading because these apply to all voting systems.

Several requirements regarding system navigation and controls were made mandatory for usability, as well as the requirement for vendors to conduct and document summative usability testing during system development. Requirements for accessible voting systems, including the use of personal assistive devices, buttons and controls, speech quality for audio ballots, limited dexterity accessibility, and voter verifiable paper audit trail accessibility were changed from permissive to mandatory. In addition, summative accessibility testing and documentation by vendors was made mandatory. A complete discussion of how comments to the VVSG were handled can be found on the EAC Web site at *www.eac.gov.*

Effective Date

The guidelines will take effect in December 2007 (24 months), at which time voting systems will no longer be tested against the 2002 Voting System Standards (VSS) developed by the Federal Election Commission (FEC). However, states may decide to adopt these guidelines before the effective date and EAC anticipates being prepared to certify voting systems before the effective date. The effective date was adopted to provide testing laboratories time to prepare to test to the VVSG, give states time to change their respective laws and statutes reflecting EAC's role in the certification process and in recognition of efforts to develop voting systems that will meet the requirements of the VVSG.

Thomas R. Wilkey,

Executive Director, U.S. Election Assistance Commission.

Voluntary Voting System Guidelines

Table of Contents

Volume I Voting System Performance Guidelines

Volume II National Certification Testing Guidelines

Voluntary Voting System Guidelines

Volume I

Voting System Performance Guidelines

Voluntary Voting System Guidelines Overview

Table of Contents

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.

As required by HAVA, the EAC formed the Technical Guidelines Development Committee (TGDC) to develop an initial set of recommendations for the Guidelines. This committee of 15 experts began their work in July 2004 and submitted their recommendations to the EAC in the 9-month timeline prescribed by HAVA. The TGDC was provided with technical support by the National Institute for Standards and Technology (NIST), which was given nearly $3 million dollars by the EAC to complete this work.

The EAC reviewed and revised the TGDC recommendations and, as required by HAVA, published the proposed Guidelines for a 90 day public comment period. The document was also provided to both the Board of Advisors and the Standards Board for their review and comment. During the comment period the EAC conducted 3 public hearings on the Guidelines in New York City, Pasadena and Denver. Over 6000 comments were received from the public and the Boards. Each of these comments was reviewed and considered by the EAC in consultation with NIST in the development of this final version.

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 2005 Voluntary Voting System Guidelines will take effect 24 months after their final adoption in December 2005 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 2005 VVSG. All previous versions of national standards will become obsolete at this time. This effective date provision does not have any impact on the mandatory January 1, 2006, deadline for states to comply with the HAVA Section 301 requirements.

Summary of Changes

Volume I of the Guidelines, entitled Voting System Performance Guidelines, includes new requirements for usability, accessibility, voting system software distribution, generation of software reference information, validation of software during voting system setup, and the use of wireless communications. System functional requirements have been revised to comply with HAVA Section 301 requirements. Environmental criteria have been updated. This volume also includes requirements for a voter verifiable paper audit trail component for direct-recording electronic voting systems for use by states that require this feature. In addition, this volume includes an updated glossary and a conformance clause.

Volume II of the Guidelines, entitled National Certification Testing Guidelines, has been revised to reflect the new EAC process for national certification of voting systems. This process was initiated in 2005 and replaces the voting system qualification process conducted by the National Association of State Election Directors (NASED) since 1994. In addition, revisions have been made to the testing procedures to reflect new requirements for the conduct of usability and accessibility testing. Volume II also includes an updated appendix on procedures for testing system error rates. Terminology in both volumes has been revised to reflect new terminology introduced by HAVA.

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; 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.

Sections 8 and 9 describe requirements for vendor 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.

Appendix C presents an introductory discussion of independent verification systems as a potential concept for future voting system security design.

Appendix D contains technical guidance on color, contrast and text size adjustment for individuals with low vision or color blindness.

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 accredited by the EAC. It is intended principally for use by vendors: test labs: and election officials who certify, procure, and accept voting systems. This volume contains the following sections:

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

Section 2 provides a description of the Technical Data Package that vendors 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 vendor quality assurance and configuration management practices.

Appendix A provides the requirements for the National Certification Test Plan that is prepared by the voting system test lab 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 test lab and delivered to the EAC along with a recommendation for certification.

Appendix C describes the guiding principles used to design the voting system certification testing process. It also contains a revised section on testing system error rates.

Volume I: Voting System Performance Guidelines

Guide to Section Locations

1 Introduction

Table of Contents

1 Introduction

1.1 Purpose and Scope of the Voluntary Voting System Guidelines

The purpose of the Voluntary Voting System Guidelines (VVSG or 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. The VVSG specifies 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. The VVSG is composed of two volumes: Volume 1, Voting System Performance Guidelines; and Volume 2, National Certification Testing Guidelines.

The VVSG is one of several inter-related EAC promulgated guidelines and programs concerned with maintaining the reliability and security of voting systems and the integrity of the overall election process. The performance of national certification testing of voting systems is restricted to testing labs that have been formally accredited to be technically competent to evaluate systems for conformance to the Voting System Performance Guidelines. The National Association of State Election Directors (NASED) initiated the independent testing authority accreditation program for test labs in 1994, applying the standards and procedures in NASED Program Handbook 9201 (Revision A). With the passage of the Help America Vote Act (HAVA), this responsibility transitioned to the Election Assistance Commission (EAC) with support from the National Voluntary Laboratory Accreditation Program (NVLAP). This program is operated by the National Institute of Standards and Technology (NIST), applying the standards and procedures in NIST Handbook 150–22, NVLAP Voting System Testing.

The VVSG and the test lab accreditation process are essential components of the EAC National Certification Program for voting systems. This program applies the standards and procedures documented in the EAC voting system certification manual. HAVA Section 231 charges EAC with providing for the certification, decertification and recertification of voting systems. Under this program national certification is just the first step of the life cycle process of maintaining the reliability and security of the voting systems used in the nation's elections. To carry out this mandate, the EAC program will include monitoring of voting system performance through incident reporting by election officials and others. The certification program will maintain information on the quality assurance practices associated with the development and manufacturing of voting systems. When a system has successfully completed the certification process, the EAC program requires a copy of the certified voting system software to be provided to the National Software Reference Library operated by NIST. This will enable election officials to validate that the software received by their jurisdictions is the same as the certified version.

The VVSG notes the need for appropriate procedures to complement and supplement the technical requirements for voting system performance. It is well known that deficiencies in election management and administration procedures can have just as much impact on the enfranchisement of voters and the outcome of elections as the functioning of the voting machines. The overall integrity of the election process depends on both of these elements working together. EAC and NASED have instituted a multi-year effort to develop a comprehensive set of election management guidelines that will complement the technical system guidelines, as well as cover other elements of the election process.

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.

Volume 2 describes the testing process to provide a documented independent verification by an accredited testing laboratory that a voting system has been demonstrated to conform to the Volume 1 requirements and therefore should receive national certification. It provides the specific detail about the testing process and documentation requirements required to support the national certification program.

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. The TGDC delivered their initial set of recommendations to the EAC in May, 2005.

The TGDC built on the foundation of the 2002 Voting Systems Standards and the accessibility provisions of HAVA to expand requirements for voting system usability and accessibility. HAVA mandates that voting systems shall 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. To facilitate the ability of jurisdictions to meet these requirements, HAVA allows for the use of at least one direct-recording electronic or other voting system equipped for individuals with disabilities at each polling place. Implementing this provision, however, will not entirely eliminate the necessity of accommodating the needs of some disabled voters by human assistance, given the limitations of current technology.

The 2005 VVSG is the culmination of sixteen months of effort by the TGDC, NIST and the EAC. There is still much to be done to further develop the technical guidelines for voting system performance, accessibility and usability features, and security. Further work is also needed for the specification of comprehensive standard test suites for certification testing, to include testing for usability and accessibility features and expanded security testing.

1.4 Overview of Voting System Testing

1.4.1 The National Certification Program for Voting Systems

The purpose of the national 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 vendor'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 the time of VVSG 2005 publication, 39 states either require national certification or utilize the national standards when certifying voting systems.

National certification testing can only be performed by testing labs that have been accredited for demonstrated technical competence to test voting systems using these Guidelines. Volume 2 of the VVSG—National Certification Testing 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 vendor'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.

Since 1994, testing of voting systems has been performed by Independent Test Authorities (ITAs) certified by NASED. Upon the successful completion of testing, the ITA issued a Qualification Test Report to the vendor 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 vendor's developmental testing and beta testing. The test lab is expected to evaluate the completeness of the vendor's developmental test program, including the sufficiency of vendor tests conducted to demonstrate compliance with the Guidelines as well as the system's performance specifications. The test lab undertakes sample testing of the vendor's test modules and also designs independent system-level tests to supplement and check those designed by the vendor. 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 an accredited test lab 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. Vendors request review of modifications by the test lab based on the nature and scope of changes made. The test lab 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 vendor.

Generally, a voting system remains certified under the standards against which it was tested as long as no modifications requiring recertification have been made to the system. However, if a new threat to a particular voting system is discovered, it is the prerogative of EAC to determine which certified voting systems are vulnerable, whether those systems need to be retested, and the specific tests to be conducted. In addition, when new requirements supersede the requirements under which the system was certified, it is the prerogative of EAC to determine when systems that were certified under the earlier requirements will need to be re-tested to meet current guidelines.

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

1.4.3 Acceptance Testing

Acceptance tests are performed at the state or local jurisdiction level upon system delivery by the vendor 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.

1.5 Definitions, References, and Types of Voting Systems

1.5.1 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.

1.5.2 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, vendors 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. Vendors shall also submit a proposed test plan to the EAC for use in national certification testing. The Guidelines permit vendors 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 1.5.2.1 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.

1.5.2.2 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.

1.5.2.3 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.

1.5.2.4 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.

1.5.2.5 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.

1.6 Conformance Clause

1.6.1 Scope and Applicability

The Voluntary Voting System Guidelines define requirements for conformance of voting systems that voting system vendors shall meet. The Guidelines also provide the framework, procedures, and requirements that testing labs responsible for the certification testing of voting systems shall follow. The requirements and procedures in the Guidelines may also be used by states to certify voting systems. To ensure that correct voting system software has been distributed without modification, the Guidelines include requirements for certified voting system software to be deposited in a national software repository. This provides an independent means for election officials to verify the software they purchase.

The Guidelines define the minimum requirements for voting systems and the process of testing voting systems. The guidelines are intended for use by:

- Designers and manufacturers of voting systems
- Test labs performing the analysis and testing of voting systems in support of the EAC national certification process
- Software repositories designated by EAC or by a state
- Election officials, including ballot designers and officials responsible for the installation, operation, and maintenance of voting machines
- Test labs and consultants performing the state certification of voting systems Minimum requirements specified in these guidelines include:
- Functional capabilities
- Performance characteristics, including security
- Documentation
- Test evaluation criteria

1.6.2 Conformance Framework

This section provides the framework in which conformance is defined. It identifies the entities to which these guidelines apply, the relationships among the various entities, the structure of the requirements, and the terminology used to indicate conformance.

1.6.2.1 Applicable Entities

The requirements, prohibitions, options, and guidance specified in these guidelines apply to voting systems, voting system vendors, test labs, 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.

Other terms in these guidelines shall be construed as synonymous with ''voting systems.'' They are: ''systems'', ''the system'', ''the voting system'', and ''each voting system.''

The term ''voting system vendor'' imposes documentation or testing requirements for the manufacturer or vendor. Other terms in these guidelines shall be construed as synonymous with ''voting system vendor.'' They are: ''vendors'', ''the vendor'', ''manufacturer or vendor'', ''voting system designers'', and ''implementer''.

The terms used to designate requirements and procedural guidelines for national certification testing laboratories are indicated by referring to ''testing authorities'', ''test labs'', and ''accredited 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.

1.6.2.2 Relationships Among Entities

It is the voting system vendor that needs to implement these requirements and provide the necessary documentation for the system. In order to claim conformance to the Guidelines, the voting system vendor shall satisfy the specified requirements, including implementation of functionality, prescribed software coding and assurance practices, and preparation of the Technical Data Package. The voting system vendor shall successfully complete the prescribed test campaign with an EAC accredited test lab.

The accredited test lab shall satisfy the requirements for conducting certification testing. The test lab may use an operational environment emulating that used by election officials as part of their testing to ensure that the voting system can be configured and operated in a secure and reliable manner according to the vendor's documentation and as specified by the Guidelines. The test lab shall coordinate and deliver the requisite documentation and test report to the EAC for review. Upon issuance of a certification number by the EAC, the test lab shall deposit a copy of the certified voting system software with the National Software Reference Library.

The EAC shall review the test results and associated documentation and make a determination that all requirements have been appropriately tested and the test results are acceptable. The EAC will issue a national certification number that indicates conformance of the specified system with these Guidelines.

The National Software Reference Library (NSRL) shall create a digital signature of the voting system software provided by the test lab. This information will be posted to a website so election officials can compare the digital signature of the software provided to them by the voting system vendor with this certified reference. The NSRL shall maintain this reference information until notified by the EAC that it can be archived.

1.6.3 Structure of Requirements

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.

1.6.3.1 Conformance Language

The following keywords are used to convey conformance requirements:

- Shall—indicates a mandatory requirement in order to conform. Synonymous with ''is required to.''
- Is prohibited—indicates a mandatory requirement that indicates something that is not permitted (allowed) in order to conform. Synonymous with ''shall not.''
- 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.''

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.

1.6.3.2 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 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 vendor 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.

1.6.3.3 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 vendor as providing this feature. The use of extensions shall not contradict nor cause the nonconformance of functionality required by the Guidelines.

1.6.4 Implementation Statement

The voting system implementation statement describes the voting system and documents the VVSG Volume 1 requirements that have been implemented by the voting system. It can also identify optional features and capabilities supported by the voting system, as well as any extensions (i.e., additional functionality beyond what is required in the guidelines). The implementation statement must include a checklist identifying all the requirements for which a claim of conformance is made.

The implementation statement must be submitted with the vendor's application to the EAC for national certification testing. It must provide a concise summary and narrative description of the voting system's capabilities. It shall include identifying information about the voting system, including the hardware and software components, version number and date.

1.7 Effective Date

The Voluntary Voting System Guidelines (VVSG) shall become effective for national certification testing 24 months after their final adoption in December, 2005 by EAC. At that time, all new systems submitted for national certification shall be tested for conformance with these Guidelines. In addition, if a modification to a system certified or qualified to a previous standard is submitted for national certification after this date, every component of the modified system shall be tested using these Guidelines. All previous versions of national voting system standards will become obsolete upon this effective date.

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.

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 Web site at *www.eac.gov.*

1 Functional Requirements

Table of Contents

2 Functional Requirements

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.

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. Record and report the date and time of normal and abnormal events

h. Maintain a permanent record of all original audit data that cannot be modified or overridden but may be augmented by designated authorized officials in order to adjust for errors or omissions (e.g., during the canvassing process)

i. Detect and record every event, including the occurrence of an error condition that the system cannot overcome, and time-dependent or programmed events that occur without the intervention of the voter or a polling place operator

j. 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:

k. 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

l. 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 vendor to describe each system's characteristics in sufficient detail so that test labs 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 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. The timing and sequence of audit record entries is as important as the data contained in the record. All voting systems shall meet the requirements for time, sequence and preservation of audit records outlined below.

i. Except where noted, systems shall provide the capability to create and maintain a real-time audit record. This capability records and provides the operator or precinct official with continuous updates on machine status. This information allows effective operator identification of an error condition requiring intervention, and contributes to the reconstruction of election-related events necessary for recounts or litigation.

ii. All systems shall include a real-time clock as part of the system's hardware. The system shall maintain an absolute record of the time and date or a record relative to some event whose time and data are known and recorded.

iii. All audit record entries shall include the time-and-date stamp.

iv. The audit record shall be active whenever the system is in an operating mode. This record shall be available at all times, though it need not be continually visible.

v. The generation of audit record entries shall not be terminated or altered by program control, or by the intervention of any person. The physical security and integrity of the record shall be maintained at all times.

vi. Once the system has been activated for any function, the system shall preserve the contents of the audit record during any interruption of power to the system until processing and data reporting have been completed.

vii. The system shall be capable of printing a copy of the audit record. A separate printer is not required for the audit record, and the record may be produced on the standard system printer if all the following conditions are met:

- The generation of audit trail records does not interfere with the production of output reports
- The entries can be identified so as to facilitate their recognition, segregation, and retention
- The audit record entries are kept physically secure

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

i. The voting system shall generate, store, and report to the user all error messages as they occur.

ii. 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.

iii. 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.

iv. 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.

v. 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.

vi. Voting system design shall ensure that erroneous responses will not lead to irreversible error.

vii. 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.

c. The Guidelines provide latitude in software design so that vendors 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 Shared Computing Platforms

Further requirements must be applied to Commercial-off-the-Shelf operating systems to ensure completeness and integrity of audit data for election software. These operating systems are capable of executing multiple application programs simultaneously. These systems include both servers and workstations, including the many varieties of UNIX and Linux, and those offered by Microsoft and Apple. Election software 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, 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 such systems on which election software is hosted. First, authentication shall be configured on the local terminal (display screen and keyboard) and on all external connection devices (''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.

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 single vote to the county (or contractor) for consolidation with other county 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 anytime 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 card or sheet, 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 vendor 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 vendor 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.

Vendor 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, 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 vendor 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

The 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 (DRE Systems)

To activate the ballot, all DRE systems 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. Allow each eligible voter to cast a ballot

c. Prevent a voter from voting on a ballot to which he or she is not entitled

d. Prevent a voter from casting more than one ballot in the same election

e. Activate the casting of a ballot in a general election

f. Enable the selection of the ballot that is appropriate to the party affiliation declared by the voter in a primary election

g. Activate all portions of the ballot upon which the voter is entitled to vote

h. Disable all portions of the ballot upon which the voter is not entitled to vote

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 System Requirements

In addition to the above common requirements, DRE 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 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

i. Notify the voter when the selection of candidates and measures is completed

j. Allow the voter, before the ballot is cast, to review his or her choices and, if the voter desires, to delete or change his or her choices before the ballot is cast

k. For electronic image displays, prompt the voter to confirm the voter's choices before casting his or her ballot, signifying to the voter that casting the ballot is irrevocable and directing the voter to confirm the voter's intention to cast the ballot

l. Notify the voter after the vote has been stored successfully that the ballot has been cast

m. 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

n. Provide sufficient computational performance to provide responses back to each voter entry in no more than three seconds

o. Ensure that the votes stored accurately represent the actual votes cast

p. Prevent modification of the voter's vote after the ballot is cast

q. 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)]

r. Increment the proper ballot position registers or counters

s. Protect the secrecy of the vote throughout the voting process

t. Prohibit access to voted ballots until after the close of polls

u. Provide the ability for election officials to submit test ballots for use in verifying the end-to-end integrity of the voting system

v. 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 vendor) 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

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 Broadcasting Results

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 and Accessibility Requirements

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

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:

1. *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.

2. *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.

3. *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.

- Requirements for general usability apply to all voting systems. Requirements for any alternative languages required by state or federal law are included under this heading.
- Requirements to assist voters with physical, sensory, or cognitive disabilities apply, as a minimum, to the accessible voting stations required by HAVA Section 301 (a)(3)(B). They may also assist those not usually described as having a disability, e.g., voters with poor eyesight or limited dexterity.

Several uncommon terms are used in this section. For the convenience of the reader, they are defined below, in addition to being included in the Glossary. Other terms frequently used here and throughout this document are defined in the Glossary. Note in particular the distinctions between these terms: voting system, voting equipment, voting machine and voting station.

- Common Industry Format (CIF)—the format to be used for usability testing reporting, described in ANSI/INCITS 354–2001 ''Common Industry Format (CIF) for Usability Test Reports''
- Accessible Voting Station—the voting station equipped for individuals with disabilities referred to in HAVA 301 (a)(3)(B).
- Audio-Tactile Interface—a voter interface designed not to 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.

3.1 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 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.
>
> 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.

Usability is defined generally as a measure of the effectiveness, efficiency, and satisfaction achieved by a specified set of users with a given product in the performance of specified tasks. In the context of voting, the primary user is the voter, the product is the voting system, and the task is the correct recording of the voter ballot selections. Additional requirements for task performance are independence and privacy: the voter should normally be able to complete the voting task without assistance from others, and the voter selections should be private. Lack of independence or privacy may adversely affect effectiveness (e.g., by possibly inhibiting the voter's free choice) and efficiency (e.g., by slowing down the process).

Among the basic metrics for usability are:

- Low error rate for marking the ballot (the voter selection is correctly conveyed to and represented within the voting system)
- efficient operation (time required to vote is not excessive)
- satisfaction (voter experience is safe, comfortable, free of stress, and instills confidence)

It is the intention of the EAC that in future revisions to the Guidelines, usability will be addressed by high-level performance-based requirements. That is, the requirements will directly address metrics for effectiveness (e.g., correct capture of voter selections), efficiency (e.g., time taken to vote), and satisfaction. Until the supporting research is completed, however, the contents of this subsection are limited to a basic set of widely accepted design requirements and lower-level performance requirements. The reasons for this approach are:

- These are to serve as interim requirements, pending the issuance of high-level performance requirements
- The actual benefit of numerous detailed design guidelines is difficult to prove or measure
- The technical complexity and costs of a large set of detailed requirements may not be justified
- Guidelines that are difficult to test because of insufficient specificity have been omitted

While the scope of usability applies to the entire voting process, the emphasis in these requirements is on the voter interface with the voting machine, which is assumed to be a visual-tactile interface.

The outline for this subsection is:

3.1.1 Usability Testing

The vendor shall conduct summative usability tests on the voting system using individuals representative of the general population. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification.

Discussion: Voting system developers are required to conduct realistic usability tests on the final product. For the present, vendors can define their own testing protocols. Future revisions to the Guidelines will include requirements for usability testing that will provide specific performance benchmarks.

3.1.2 Functional Capabilities

The voting process shall provide certain functional capabilities to support voter usability.

a. The voting system shall provide feedback to the voter that identifies specific contests or ballot issues for which he or she has made no selection or fewer than the allowable number of selections (e.g., undervotes)

b. The voting system shall notify the voter if he or she has made more than the allowable number of selections for any contest (e.g., overvotes)

c. The voting system shall 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

d. 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

e. The voting system shall allow the voter, at his or her choice, to submit an undervoted ballot without correction

f. DRE voting machines 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 a DRE should not have to wait for the final ballot review screen in order to change a vote.

g. DRE voting machines should 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 currently being presented (whether visually or aurally).

Discussion: For example, the voter should not be forced to proceed sequentially through all the contests before going back to check his or her selection for a previous contest.

3.1.3 Alternative Languages

The voting equipment shall be capable of presenting the ballot, ballot selections, review screens and instructions in any language required by state or federal law.

Discussion: 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. The audio interface provided for blind voters may also assist voters who speak English, but who are unable to read it (See Subsection 3.2.2.2).

3.1.4 Cognitive Issues

The voting process shall be designed to minimize cognitive difficulties for the voter.

a. Consistent with election law, the voting system should support a process that does not introduce any bias for or against any of the selections to be made by the voter. In both visual and aural formats, contest 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. But comparable characteristics such as font size or voice volume and speed must be the same for all choices.

b. The voting machine or related materials shall provide clear instructions and assistance to allow voters to successfully execute and cast their ballots independently.

Discussion: Voters should not routinely need to ask for human assistance.

i. Voting machines or related materials shall provide a means for the voter to get help at any time during the voting session.

Discussion: The voter should always be able to get help if needed. DRE voting machines may provide this with a distinctive ‘‘help’’ button. Any type of voting equipment may provide written instructions that are separate from the ballot.

ii. The voting machine 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, and how to cast a write-in vote.

c. The voting system shall provide the capability to design a ballot for maximum clarity and comprehension.

i. The voting equipment 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. 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. There shall be a consistent relationship between the name of a candidate and the mechanism used to vote for that candidate.

Discussion: For example, if the response field where voters indicate their selections is located to the left of a candidate's name, then each response field shall be located to the left of the associated candidates' names.

d. Warnings and alerts issued by the voting system should clearly state the nature of the problem and the set of responses available to the voter. The warning should clearly state whether the voter has performed or attempted an invalid operation or whether the voting equipment itself has malfunctioned in some way.

Discussion: In case of an equipment failure, the only action available to the voter might be to get assistance from a poll worker.

e. The use of color by the voting system should 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.

3.1.5 Perceptual Issues

The voting process shall be designed to minimize perceptual difficulties for the voter.

a. No voting machine display screen shall flicker with a frequency between 2 Hz and 55 Hz.

Discussion: Aside from usability concerns, this requirement protects voters with epilepsy.

b. Any aspect of the voting machine that is adjustable by the voter or poll worker, including font size, color, contrast, and audio volume, shall automatically reset to a standard default value upon completion of that voter's session.

Discussion: The voting machine must present the same initial appearance to every voter.

c. If any aspect of a voting machine is adjustable by the voter or poll worker, there shall be a mechanism to reset all such aspects to their default values.

Discussion: The purpose is to allow a voter who has adjusted the machine into an undesirable state to reset all the aspects to begin again.

d. All electronic voting machines shall provide a minimum font size of 3.0 mm (measured as the height of a capital letter) for all text.

e. All voting machines using paper ballots should make provisions for voters with poor reading vision.

Discussion: Possible solutions include: (a) providing paper ballots in at least two font sizes, 3.0–4.0mm and 6.3–9.0mm and (b) providing a magnifying device.

f. The default color coding shall maximize correct perception by voters with color blindness.

Discussion: There are many types of 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.

g. 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 to convey the information, such as a shape or text style. For example, red can be enclosed in an octagon shape.

h. All text intended for the voter should be presented in a sans serif font.

Discussion: Experimentation has shown that users prefer such a font and the legibility of serif and sans serif fonts is equivalent.

i. The minimum figure-to-ground ambient contrast ratio for all text and informational graphics (including icons) intended for the voter shall be 3:1.

3.1.6 Interaction Issues

The voting process shall be designed to minimize interaction difficulties for the voter.

a. Voting machines with electronic image displays shall not require page scrolling by the voter.

Discussion: This 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 machine shall provide unambiguous feedback regarding the voter's selection, such as displaying a checkmark beside the selected option or conspicuously changing its appearance.

c. If the voting machine requires a response by a voter within a specific period of time, it shall issue an alert at least 20 seconds before this time period has expired and provide a means by which the voter may receive additional time.

d. Input mechanisms shall be designed to minimize accidental activation.

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.

ii. No key or control on a voting machine 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.

3.1.7 Privacy

The voting process shall preclude anyone else from determining the content of a voter's ballot, without the voter's cooperation.

Discussion: Privacy ensures that the voter can make selections based solely on his or her own preferences without intimidation or inhibition. Among other practices, this forbids the issuance of a receipt to the voter that would provide proof of how he or she voted.

3.1.7.1 Privacy at the Polls

When deployed according to the installation instructions provided by the vendor, the voting station shall prevent others from observing the contents of a voter's ballot.

a. The ballot and any input controls shall be visible only to the voter during the voting session and ballot submission.

b. The audio interface 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.

c. As mandated by HAVA 301 (a)(1)(C), the voting system shall notify the voter of an attempted overvote in a way that preserves the privacy of the voter and the confidentiality of the ballot.

3.1.7.2 No Recording of Alternate Format Usage

Voter anonymity shall be maintained for alternative format ballot presentation.

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

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

3.2 Accessibility Requirements

The voting process shall be accessible to voters with disabilities. As a minimum, every polling place shall have at least one voting station equipped for individuals with disabilities, as provided in HAVA 301 (a)(3)(B). A machine so equipped is referred to herein as an accessible voting station.

HAVA Section 301 (a) (3) 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 requirements in Subsection 3.2 are intended to address this mandate. Ideally, every voter would be able to vote independently and privately. As a practical matter, there may be some number of voters whose disabilities are so severe that they will need personal assistance. Nonetheless, these requirements are meant to make the voting system independently accessible to as many voters as possible. These requirements are in addition to those described in Subsection 3.1 Usability Requirements.

The outline for this subsection is:

3.2.1 General
3.2.2 Vision
3.2.3 Dexterity
3.2.4 Mobility
3.2.5 Hearing
3.2.6 Speech
3.2.7 English Proficiency
3.2.8 Cognition

3.2.1 General

The voting process shall incorporate the following features that are applicable to all types of disabilities:

a. When the provision of accessibility involves an alternative format for ballot presentation, then all information presented to voters including instructions, warnings, error and other messages, and ballot choices shall be presented in that alternative format.

b. The support provided to voters with disabilities shall be intrinsic to the accessible voting station. It shall not be necessary for the accessible voting station to be connected to any personal assistive device of the voter in order for the voter to operate it correctly.

Discussion: This requirement does not preclude the accessible voting station from providing interfaces to assistive technology. [See definition of ''personal assistive devices'' in the Glossary.] 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 accessible voting station will obviate the need for a voter's ordinary non-interfacing devices, such as eyeglasses or canes. Jurisdictions should ensure that an accessible voting station provides clean and sanitary devices for voters with dexterity disabilities.

c. When the primary means of voter identification or authentication uses biometric measures that require a voter to possess particular biological characteristics, the voting process shall provide a secondary means that does not depend on those characteristics.

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

3.2.2 Vision

The voting process shall be accessible to voters with visual disabilities.

Discussion: Note that all aspects of the voting process are to be accessible, not just the voting machine.

3.2.2.1 Partial Vision

The accessible voting station shall be accessible to voters with partial vision.

a. The vendor shall conduct summative usability tests on the voting system using partially sighted individuals. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification.

Discussion: Voting system developers are required to conduct realistic usability tests on the final product. For the present, vendors can define their own testing protocols. Future revisions to the Guidelines will include requirements for usability testing that will provide specific performance benchmarks.

b. The accessible voting station with an electronic image display shall be capable of showing all information in at least two font sizes, (a) 3.0–4.0 mm and (b) 6.3–9.0 mm, under control of the voter.

Discussion: All millimeters will be calculated using Hard Metric Conversion. [See Glossary for definition.] While larger font sizes may assist most voters with poor vision, certain disabilities such as tunnel vision are best addressed by smaller font sizes.

c. An accessible voting station with a monochrome-only electronic image display shall be capable of showing all information in high contrast either by default or under the control of the voter or poll worker. High contrast is a figure-to-ground ambient contrast ratio for text and informational graphics of at least 6:1.

d. An accessible voting station with a color electronic image display shall allow the voter to adjust the color or the figure-to-ground ambient contrast ratio.

Discussion: See Technical Guide for Color, Contrast and Text Size in Appendix D for examples of how a voting station may meet this requirement by offering a limited number of discrete choices. In particular, it is not required that the station offer a continuous range of color or contrast values.

e. Buttons and controls on accessible voting stations shall be distinguishable by both shape and color.

Discussion: The redundant cues are helpful to those with low vision. They are also helpful to individuals who may have difficulty reading the text on the screen. f. An accessible voting station using an electronic image display shall provide synchronized audio output to convey the same information as that which is displayed on the screen.

3.2.2.2 Blindness

The accessible voting station shall be accessible to voters who are blind.

a. The vendor shall conduct summative usability tests on the voting system using individuals who are blind. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification.

Discussion: Voting system developers are required to conduct realistic usability tests on the final product. For the present, vendors can define their own testing protocols. Future revisions to the Guidelines will include requirements for usability testing that will provide specific performance benchmarks.

b. The accessible voting station shall provide an audio-tactile interface (ATI) that supports the full functionality of the visual ballot interface, as specified in Subsection 2.3.3.

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 this is normally performed by the voter on comparable voting stations
- Instructions and feedback to the voter on how to operate the accessible voting station, including settings and options (e.g., volume control, repetition)
- 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 selections
- Instructions and feedback on final submission of ballot

i. The ATI of the accessible voting station shall provide the same capabilities to vote and cast a ballot as are provided by other voting machines or by the visual interface of the standard voting machine.

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

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

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

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. All voting stations that provide audio presentation of the ballot shall conform to the following requirements:

Discussion: These requirements apply to all voting machine audio output, not just to the ATI of an accessible voting station.

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. When a voting machine utilizes a telephone style handset or headphone to provide audio information, it shall provide a wireless T-Coil 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 American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19.

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

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

iv. 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.

v. The voting machine shall set the initial volume for each voter between 40 and 50 dB SPL.

Discussion: A voter does not ''inherit'' the volume as set by the previous user of the voting station.

vi. The voting machine shall provide a volume control with an adjustable volume from a minimum of 20dB SPL up to a maximum of 100 dB SPL, in increments no greater than 10 dB.

vii. The audio system shall be able to reproduce frequencies over the audible speech range of 315 Hz to 10 KHz.

viii. 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.

ix. The audio system shall allow voters to control the rate of speech. The range of speeds supported should be at least 75% to 200% of the nominal rate.

Discussion: Many blind voters are accustomed to interacting with accelerated speech.

d. If the normal procedure is to have voters initialize the activation of the ballot, the accessible voting station shall 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 normal procedure is for voters to submit their own ballots, then the accessible voting station shall provide features that enable voters who are blind to perform this submission.

Discussion: For example, if voters normally feed their own optical scan ballots into a reader, blind voters should also be able to do so.

f. All mechanically operated controls or keys on an accessible voting station shall be tactilely discernible without activating those controls or keys.

g. On an accessible voting station, the status of all locking or toggle controls or keys (such as the ''shift'' key) shall be visually discernible, and discernible either through touch or sound.

3.2.3 Dexterity

The voting process shall be accessible to voters who lack fine motor control or use of their hands.

a. The vendor shall conduct summative usability tests on the voting system using individuals lacking fine motor control. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification.

Discussion: Voting system developers are required to conduct realistic usability tests on the final product. For the present, vendors can define their own testing protocols. Future revisions to the Guidelines will include requirements for usability testing that will provide specific performance benchmarks.

b. All keys and controls on the accessible voting station 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.

c. The accessible voting station 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.

d. The accessible voting station shall provide a mechanism to enable non-manual input that is functionally equivalent to tactile input.

Discussion: This requirement ensures that the accessible voting station is operable by individuals who do not have the use of their hands. All the functionality of the accessible voting station (e.g., straight party voting, write-in candidates) that is available through the other forms of input, such as tactile, must also be available through a non-manual input mechanism if it is provided by the accessible voting station.

e. If the normal procedure is for voters to submit their own ballots, then the accessible voting station shall provide features that enable voters who lack fine motor control or the use of their hands to perform this submission.

3.2.4 Mobility

The voting process shall be accessible to voters who use mobility aids, including wheelchairs.

a. The accessible voting station shall provide a clear floor space of 30 inches (760 mm) minimum by 48 inches (1220 mm) minimum for a stationary mobility aid. The clear floor space shall be level with no slope exceeding 1:48 and positioned for a forward approach or a parallel approach.

b. All controls, keys, audio jacks and any other part of the accessible voting station necessary for the voter to operate the voting machine shall be within reach as specified under the following sub-requirements:

Discussion: 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.

i. If the accessible voting station 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 Figure 1.

ii. If the accessible voting station has a forward approach with a forward reach obstruction, the following requirements apply (See Figure 2):

- The forward obstruction 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.
- If the obstruction 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 (230 mm) above the finish floor or ground shall be considered toe clearance and shall comply with the following provisions:

- Toe clearance shall extend 25 inches (635 mm) maximum under the obstruction
- The minimum toe clearance under the obstruction shall be either 17 inches (430 mm) or the depth required to reach over the obstruction to operate the accessible voting station, whichever is greater
- Toe clearance shall be 30 inches (760 mm) wide minimum

iv. Space under the obstruction between 9 inches (230 mm) and 27 inches (685 mm) above the finish floor or ground shall be considered knee clearance and shall comply with the following provisions:

- Knee clearance shall extend 25 inches (635 mm) maximum under the obstruction at 9 inches (230 mm) above the finish floor or ground.
- The minimum knee clearance at 9 inches (230 mm) above the finish floor or ground shall be either 11 inches (280 mm) or 6 inches less than the toe clearance, whichever is greater.
- Between 9 inches (230 mm) and 27 inches (685 mm) above the finish floor or ground, the knee clearance shall be permitted to reduce at a rate of 1 inch

(25 mm) in depth for each 6 inches (150 mm) in height.

Discussion: 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.

- Knee clearance shall be 30 inches (760 mm) wide minimum.

v. If the accessible voting station 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 Figure 3.

vi. If the accessible voting station has a parallel approach with a side reach obstruction, the following sub-requirements apply. See Figure 4.

- The side obstruction shall be no greater than 24 inches in depth and its top no higher than 34 inches.
- 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.

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

c. All labels, displays, controls, keys, audio jacks, and any other part of the accessible voting station necessary for the voter to operate the voting machine shall be easily 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 accessible voting station

Discussion: There are a number of factors that could make relevant parts of the accessible voting station 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.

Version 1.0

Volume I: *Voting System Performance Guidelines*
3 Usability and Accessibility Requirements

Figures 1-4

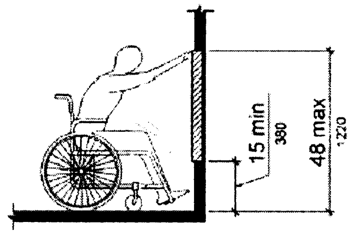


Figure 1
Unobstructed forward reach

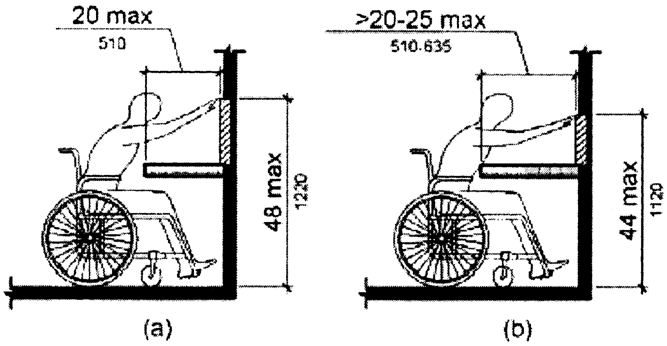


Figure 2
Obstructed forward reach
(a) for an obstruction depth of up to 20 inches (508 mm)
(b) for an obstruction depth of up to 25 inches (635 mm)

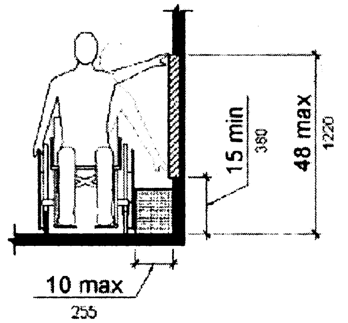


Figure 3
Unobstructed side reach with an allowable obstruction less than 10 inches (254 mm) deep.

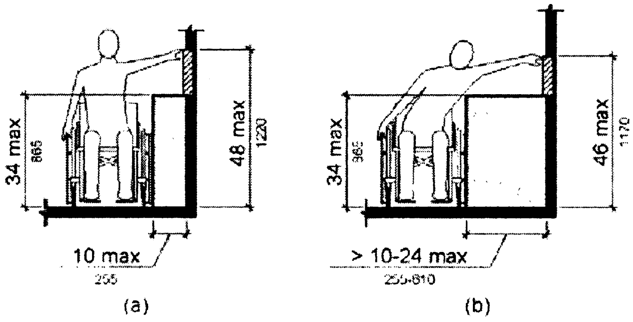


Figure 4
Obstructed side reach
(a) for an obstruction depth of up to 10 inches (254 mm)
(b) for an obstruction depth of up to 24 inches (610 mm)

3.2.5 Hearing

The voting process shall be accessible to voters with hearing disabilities. a. The accessible voting station shall incorporate the features listed under requirement 3.2.2.2 (c) for voting equipment that provides audio presentation of the ballot to provide accessibility to voters with hearing disabilities.

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

b. If voting equipment 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. Some voting equipment may have an audio-only mode, in which case, there would be no visual cue.

3.2.6 Speech

The voting process shall be accessible to voters with speech disabilities. a. No voting equipment shall require voter speech for its operation.

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

3.2.7 English Proficiency

For voters who lack proficiency in reading English, or whose primary language is unwritten, the voting equipment shall provide spoken instructions and ballots in the preferred language of the voter, consistent with state and federal law. The requirements of 3.2.2.2 (c) shall apply to this mode of interaction.

3.2.8 Cognition

The voting process should be accessible to voters with cognitive disabilities.

Discussion: At present there are no design features specifically aimed at helping those with cognitive disabilities. Requirements 3.2.2.1 (f), the synchronization of audio with the screen in a DRE, is helpful for some cognitive disabilities such as dyslexia. Requirements in Subsection 3.1.4 also address cognitive issues relative to voting system usability.

4 Hardware Requirements

Table of Contents

4 Hardware Requirement

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
- Ballot cards and sheets
- 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 vendor 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

Voting system accuracy addresses the accuracy of data for each of the individual ballot positions that could be selected by a voter, including the positions that are not selected. For a voting system, accuracy is defined as the 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. This rate is set at a sufficiently stringent level that the likelihood of voting system errors affecting the outcome of an election is exceptionally remote even in the closest of elections.

The error rate is defined using a convention that recognizes differences in how vote data is processed by different types of voting systems. Paper-based and DRE systems have different processing steps. Some differences also exist between precinct count and central count systems. Therefore, the acceptable error rate applies separately and distinctly to each of the following functions:

a. For all paper-based voting systems:

i. Scanning ballot positions on paper ballots to detect selections for individual candidates and contests

ii. Conversion of selections detected on paper ballots into digital data

b. For all DRE voting systems:

i. Recording the voter selections of candidates and contests into voting data storage

ii. Recording voter selections of candidates and contests into ballot image storage independently from voting data storage

c. For precinct-count voting systems (paper-based and DRE):

i. Consolidation of vote selection data from multiple precinct-based voting machines to generate jurisdiction-wide vote counts, including storage and reporting of the consolidated vote data

d. For central-count voting systems (paper-based and DRE):

i. Consolidation of vote selection data from multiple counting devices to generate jurisdiction-wide vote counts, including storage and reporting of the consolidated vote data

For testing purposes, the acceptable error rate is defined using two parameters: the desired error rate to be achieved, and the maximum error rate that should be accepted by the test process.

For each processing function indicated above, the voting system shall achieve a target error rate of no more than one in 10,000,000 ballot positions, with a maximum acceptable error rate in the test process of one in 500,000 ballot positions.

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

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.

The Technical Data Package supplied by the vendor shall include a statement of all requirements and restrictions regarding environmental protection, electrical service, recommended auxiliary power, telecommunications service, and 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 vendor 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. All 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

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

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

Vote scanning and counting equipment for paper-based systems, and all DRE 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

Equipment used for election management activities or vote counting (including both precinct and central count systems) shall be capable of operation in temperatures ranging from 50 to 95 degrees Fahrenheit.

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:

- Ballot cards or 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 ballot cards 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 card 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. Achieve an error rate not to exceed the requirement indicated in Subsection 4.1.1

v. 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

vi. Maintain a log of corrected data Recording reliability refers to the ability of the DRE system to record votes accurately at its maximum rated processing volume for a specified period of time. The DRE system shall record votes reliably in accordance with the requirements of Subsection 4.3.3.

4.1.5 Paper-Based Conversion Requirements

The paper-based conversion requirements address the ability of the system to read the ballot card 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 card 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 card'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 vendor. 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 cards 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 cards 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 card reader shall halt in a manner that permits the operator to remove the unread cards causing the error, and reinsert them in the card input hopper

ii. The frequency of multiple feeds with ballots intended for use with the system shall not exceed l in 10,000

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 punches or marks that conform to vendor specifications with an error rate not exceeding the requirement indicated in Subsection 4.1.1

e. Ignore, and not record, extraneous perforations, smudges, and folds

f. Reject ballots that meet all vendor specifications at a rate not to exceed 2 percent

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. Processing accuracy refers to the ability of the system to receive electronic signals produced by punches for punchcard systems and vote marks and timing information for marksense systems; perform logical and numerical operations upon these data; and reproduce the contents of memory when required, without error. Specific requirements are detailed below:

i. Processing accuracy shall be measured by vote selection error rate, the ratio of uncorrected vote selection errors to the total number of ballot positions that could be recorded across all ballots when the system is operated at its nominal or design rate of processing

ii. The vote selection error rate shall include data that denotes ballot style or precinct as well as data denoting a vote in a specific contest or ballot proposition

iii. The vote selection error rate shall include all errors from any source

iv. The vote selection error rate shall not exceed the 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 and voter input without perceptible delay (no more than three seconds)

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 reduced to the lowest level 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

The reliability of voting system devices shall be measured as Mean Time Between Failure (MTBF) for the system submitted for testing. MBTF is defined as the value of the ratio of operating time to the number of failures which have occurred in the specified time interval. A typical system operations scenario consists of approximately 45 hours of equipment operation, consisting of 30 hours of equipment set-up and readiness testing and 15 hours of elections operations. For the purpose of demonstrating compliance with this requirement, a failure is defined as any event which results in either the:

- Loss of one or more functions
- Degradation of performance such that the device is unable to perform its intended function for longer than 10 seconds

The MTBF demonstrated during certification testing shall be at least 163 hours.

4.3.4 Maintainability

Maintainability represents the ease with which maintenance actions can be performed based on the design characteristics of equipment and software and the processes the vendor and election officials have in place for preventing failures and for reacting to failures. Maintainability includes the ability of equipment and software to self-diagnose problems and make non-technical election workers aware of a problem. Maintainability addresses all scheduled and unscheduled events, which are performed to:

- Determine the operational status of the system or a component
- Adjust, align, tune or service components
- Repair or replace a component having a specified operating life or replacement interval
- Repair or replace a component that exhibits an undesirable predetermined physical condition or performance degradation
- Repair or replace a component that has failed
- Verify the restoration of a component or the system to operational status

Maintainability shall be determined based on the presence of specific physical attributes that aid system maintenance activities, and the ease with which system maintenance tasks can be performed by the test lab. Although a more quantitative basis for assessing maintainability, such as the Mean Time to Repair the system is desirable, the certification of a system is conducted before it is approved for sale and thus before a broader base of maintenance experience can be obtained.

4.3.4.1 Physical Attributes

The following physical attributes will be examined to assess reliability:

a. Presence of labels and the identification of test points

b. Provision of built-in test and diagnostic circuitry or physical indicators of condition pc. Presence of labels and alarms related to failures

d. Presence of features that allow non-technicians to perform routine maintenance tasks (such as update of the system database)

4.3.4.2 Additional Attributes

The following additional attributes will be considered to assess system maintainability:

a. Ease of detecting that equipment has failed by a non-technician pb. Ease of diagnosing problems by a trained technician

c. Low false alarm rates (i.e., indications of problems that do not exist)

d. Ease of access to components for replacement

e. Ease with which adjustment and alignment can be performed

f. Ease with which database updates can be performed by a non-technician

g. Adjust, align, tune or service components

4.3.5 Availability

The availability of a voting system is defined as the probability that the equipment (and supporting software) needed to perform designated voting functions will respond to operational commands and accomplish the function. The voting system shall meet the availability standard for each of the following voting functions:

a. For all paper-based systems:

i. Recording voter selections (such as by ballot marking or punch)

ii. Scanning the punches or marks on paper ballots and converting them into digital data

b. For all DRE systems, recording and storing voter ballot selections

c. For precinct count systems (paper-based and DRE), consolidation of vote selection data from multiple precinct based systems to generate jurisdiction-wide vote counts, including storage and reporting of the consolidated vote data

d. For central-count systems (paper-based and DRE), consolidation of vote selection data from multiple counting devices to generate jurisdiction-wide vote counts, including storage and reporting of the consolidated vote data

System availability is measured as the ratio of the time during which the system is operational (up time) to the total time period of operation (up time plus down time). Inherent availability (Ai) is the fraction of time a system is functional, based upon Mean Time Between Failure (MTBF) and Mean Time To Repair (MTTR), that is:

Ai = (MTBF)/(MTBF + MTTR)

MTTR is the average time required to perform a corrective maintenance task during periods of system operation. Corrective maintenance task time is active repair time, plus the time attributable to other factors that could lead to logistic or administrative delays, such as travel notification of qualified maintenance personnel and travel time for such personnel to arrive at the appropriate site.

Corrective maintenance may consist of substitution of the complete device or one of its components, as in the case of precinct count and some central count systems, or it may consist of on-site repair.

The voting system shall achieve at least 99 percent availability during normal operation for the functions indicated above. This standard encompasses for each function the combination of all devices and components that support the function, including their MTTR and MTBF attributes.

Vendors shall specify the typical system configuration that is to be used to assess availability, and any assumptions made with regard to any parameters that impact the MTTR. These factors shall include at a minimum:

e. Recommended number and locations of spare devices or components to be kept on hand for repair purposes during periods of system operation

f. Recommended number and locations of qualified maintenance personnel who need to be available to support repair calls during system operation

g. Organizational affiliation (i.e., jurisdiction, vendor) of qualified maintenance personnel

4.3.6 Product Marking

All voting systems shall:

a. Identify all devices by means of a permanently affixed nameplate or label containing the name of the manufacturer or vendor, the name of the device, its part or model number, its revision letter, its serial number, and if applicable, its power requirements

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

c. 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

4.3.7 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

4.3.8 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

5 Software Requirements

Table of Contents

5 Software Requirements

5 Software Requirements

5.1 Scope

This section describes essential design and performance characteristics of the software used in voting systems, addressing both system level software, such as operating systems, and voting system application software, including firmware. The requirements of this section are intended to ensure that voting system software is reliable, robust, testable, and maintainable. The requirements in this section also support system accuracy, logical correctness, privacy, security and integrity.

The general requirements of this section apply to software used to support the entire range of voting system activities described in Section 2. More specific requirements are defined for ballot counting, vote processing, creating an audit trail, and generating output reports and files. Although this section emphasizes software, the guidelines described also influence hardware design considerations.

This section recognizes that there is no best way to design software. Many programming languages are available for which modern programming practices are applicable, such as the use of rigorous program and data structures, data typing, and naming conventions. Other programming languages exist for which such practices are not easily applied.

The Guidelines are intended to guide the design of software written in any of the programming languages commonly used for mainframe, mini-computer, and microprocessor systems. They are not intended to preclude the use of other languages or environments, such as those that exhibit declarative structure, object-oriented languages, functional programming languages, or any other combination of language and implementation that provides appropriate levels of performance, testability, reliability, and security. The vendor makes specific software selections. However, the use of widely recognized and proven software design methods will facilitate the analysis and testing of voting system software in the certification process.

5.1.1 Software Sources

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

- Software provided by the voting system vendor and its component suppliers
- Software furnished by an external provider (for example, providers of COTS operating systems and web browsers) where the software may be used in any way during voting system operation
- Software developed by the voting jurisdiction

Compliance with the software requirements is assessed by several formal tests, including code examination. Unmodified software is not subject to code examination; however, source code provided by third parties and embedded in software modules for compilation or interpretation shall be provided in human readable form to the accredited test lab. The accredited test lab may inspect source code units to determine testing requirements or to verify that the code is unmodified and that the default configuration options have not been changed.

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 vendors shall submit a record of all user selections made during software installation as part of the Technical Data Package. The vendor shall also submit a record of all configuration changes made to the software following its installation. The accredited test lab shall confirm the propriety and correctness of these user selections and configuration changes.

5.1.2 Management of Software and Hardware

The requirements of this section apply to all software used in any manner to support any voting-related activities, regardless of the ownership of the software or the ownership and location of the hardware on which the software is installed or operates. These requirements apply to:

- Software that operates on voting devices and vote counting devices installed at polling places under the control of the voting jurisdiction
- Software that operates on ballot printers, vote counting devices, and other hardware typically installed at central or precinct locations (including contractor facilities)
- Election management software

However, some requirements apply only in specific situations indicated in this section. In addition to the requirements of this section, all software used in any manner to support any voting-related activities shall meet the requirements for security described in Section 7.

5.1.3 Exclusions

Some voting systems use computers that also may be used for other purposes. General purpose software such as operating systems, programming language compilers, database management systems, and Web browsers may be installed on these computers. Such software is governed by the Guidelines unless:

a. The software provides no support of voting system capabilities

b. The software is removable, disconnectable or switchable such that it cannot function while voting system functions are enabled

c. Procedures are provided that confirm that the software has been removed, disconnected or switched

5.2 Software Design and Coding Standards

The software used by voting systems is selected by the vendor and not prescribed by the Guidelines. This section provides requirements for voting system software with regard to:

- Selection of programming languages
- Software integrity
- Software modularity and programming
- Control constructs
- Naming conventions
- Coding conventions
- Comment conventions

5.2.1 Selection of Programming Languages

Software associated with the logical and numerical operations of vote data shall use a high-level programming language, such as: Pascal, Visual Basic, Java, C and C++. The requirement for the use of high-level language for logical operations does not preclude the use of assembly language for hardware-related segments, such as device controllers and handler programs. Also, operating system software may be designed in assembly language.

5.2.2 Software Integrity

Self-modifying, dynamically loaded or interpreted code is prohibited, except under the security provisions outlined in Subsection 7.4. This prohibition is to ensure that the software tested and approved during the certification process remains unchanged and retains its integrity. External modification of code during execution shall be prohibited. Where the development environment (programming language and development tools) includes the following features, the software shall provide controls to prevent accidental or deliberate attempts to replace executable code:

a. Unbounded arrays or strings (includes buffers used to move data)

b. Pointer variables

c. Dynamic memory allocation and management

5.2.3 Software Modularity and Programming

Voting system application software, including commercial off-the-shelf (COTS) software, shall be designed in a modular fashion. However, COTS software is not required to be inspected for compliance with this requirement. For the purpose of this requirement [1], ''modules'' may be compiled or interpreted independently. Modules may also be nested. The modularity rules described here apply to the component sub-modules of a library. The principle to be followed is that the module contains all the elements to compile or interpret successfully and has limited access to data in other modules. The design concept is simple replacement with another module whose interfaces match the original module. A module is designed in accordance with the rules below.

a. 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. Each module shall be uniquely and mnemonically named, using names that differ by more than a single character. In addition to the unique name, the modules shall include a set of header comments identifying the module's purpose, design, conditions, and version history, followed by the operational code. Headers are optional for modules of fewer than ten executable lines where the subject module is embedded in a larger module that has a header containing the header information. Library modules shall also have a header comment describing the purpose of the library and version information.

c. All required resources, such as data accessed by the module, should either be contained within the module or explicitly identified as input or output to the module. Within the constraints of the programming language, such resources shall be placed at the lowest level where shared access is needed. If that shared access level is across multiple modules, the definitions should be defined in a single file (called header files in some languages, such as C) where any changes can be applied once and the change automatically applies to all modules upon compilation or activation.

d. A module is small enough to be easy to follow and understand. Program logic visible on a single page is easy to follow and correct. Volume II, Section 5 provides testing guidelines for the accredited test lab to identify large modules subject to review under this requirement.

e. Each module shall have a single entry point, and a single exit point, for normal process flow. For library modules or languages such as the object-oriented languages, the entry point is to the individual contained module or method invoked. The single exit point is the point where control is returned. At that point, the data that is expected as output must be appropriately set. The exception for the exit point is where a problem is so severe that execution cannot be resumed. In this case, the design must explicitly protect all recorded votes and audit log information and must implement formal exception handlers provided by the language.

f. Process flow within the modules shall be restricted to combinations of the control structures defined in Volume II, Section 5. These structures support the modular concept, especially the single entry and exit rule above. They apply to any language feature where program control passes from one activity to the next, such as control scripts, object methods or sets of executable statements, even though the language itself is not procedural

5.2.4 Control Constructs

Voting system software shall use the control constructs identified in Volume II, Section 5:

a. Acceptable constructs are Sequence, If-Then-Else, Do-While, Do-Until, Case, and the General Loop (including the special case for loop).

i. If the programming language used does not provide these control constructs, the vendor shall provide comparable control structure logic. The constructs shall be used consistently throughout the code. No other constructs shall be used to control program logic and execution.

ii. While some programming languages do not create programs as linear processes, stepping from an initial condition through changes to a conclusion, the program components nonetheless contain procedures (such as ''methods'' in object-oriented languages). Even in these programming languages, the procedures must execute through these control constructs or their equivalents, as defined and provided by the vendor.

iii. Operator intervention or logic that evaluates received or stored data shall

Some software languages and develpment environments use a different definition of module but this principle still applies.

not re-direct program control within a program routine. Program control may be re-directed within a routine by calling subroutines, procedures, and functions, and by interrupt service routines and exception handlers (due to abnormal error conditions). Do-While (False) constructs and intentional exceptions (used as GoTos) are prohibited.

5.2.5 Naming Conventions

Voting system software shall use the naming conventions below.

a. Object, function, procedure, and variable names shall be chosen to enhance the readability and intelligibility of the program. Insofar as possible, names shall be selected so that their parts of speech represent their use, such as nouns to represent objects and verbs to represent functions.

b. Names used in code and in documentation shall be consistent.

c. Names shall be unique within an application. Names shall differ by more than a single character. All single-character names are forbidden except those for variables used as loop indexes. In large systems where subsystems tend to be developed independently, duplicate names may be used where the scope of the name is unique within the application. Names should always be unique where modules are shared.

d. Language keywords shall not be used as names of objects, functions, procedures, variables or in any manner not consistent with the design of the language.

5.2.6 Coding Conventions

Voting system software shall adhere to basic coding conventions. The coding conventions used shall meet one of the following conditions:

a. The vendors shall identify the published, reviewed, and industry-accepted coding conventions used and the accredited test lab shall test for compliance

b. The accredited test lab shall evaluate the code using the coding convention requirements specified in Volume II, Section 5

These guidelines reference conventions that protect the integrity and security of the code, which may be language-specific and language-independent conventions that significantly contribute to readability and maintainability. Specific style conventions that support economical testing are not binding unless adopted by the vendor.

5.2.7 Comment Conventions

Voting system software shall use the following comment conventions:

a. All modules shall contain headers. For small modules of 10 lines or less, the header may be limited to identification of unit and revision information. Other header information should be included in the small unit headers if not clear from the actual lines of code. Header comments shall provide the following information:

i. The purpose of the unit and how it works

ii. Other units called and the calling sequence

iii. A description of input parameters and outputs

iv. File references by name and method of access (i.e., read, write, modify or append)

v. Global variables used

vi. Date of creation and a revision record

b. Descriptive comments shall be provided to identify objects and data types. All variables shall have comments at the point of declaration clearly explaining their use. Where multiple variables that share the same meaning are required, the variables may share the same comment

c. In-line comments shall be provided to facilitate interpretation of functional operations, tests, and branching

d. Assembly code shall contain descriptive and informative comments , such that its executable lines can be clearly understood

e. All comments shall be formatted in a uniform manner that makes it easy to distinguish them from executable code

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 2.5.1.1. 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, vendors 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 card reader 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 Systems

All DRE systems shall ensure vote secrecy by:

a. Immediately after the voter chooses to cast his or her ballot, record the voter's selections in the memory to be used for vote counting and audit data (including ballot images), and erase the selections from the display, memory, and all other storage, including all forms of temporary storage

b. Immediately after the voter chooses to cancel his or her ballot, erase 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 vendors 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 vendor but that the vendor permits to be acquired from third party sources not under the vendor'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: For systems that transmit votes individually over a public network, the transmission of a single vote within a network at a polling place and to the county (or contractor) for consolidation with other county 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 Maintainability

The telecommunications components of all voting systems shall meet the maintainability requirements of Subsection 4.3.4.

6.2.5 Availability

The telecommunications components of all voting systems shall meet the availability requirements of Subsection 4.3.5.

6.2.6 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.

6.2.7 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 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

This section describes specific capabilities that vendors shall integrate into a voting system to address the risks above. Several new elements have been added since the 2002 Voting Systems Standards:

- Requirements for software distribution to purchasing jurisdictions.
- Generation of reference information to validate software
- Validation of software using the reference information
- Requirements regarding the use of wireless communications
- Requirements for DREs with voter verifiable paper trail components

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 vendor and the vendor'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 Vendor Control

The requirements of this section apply to the capabilities of a voting system that must be provided by the vendor. 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 vendor, they will be addressed in the forthcoming Management Guidelines that will address the procedural aspects of conducting elections and managing the operation of voting systems. However, vendors 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 vendors.

7.2.1 General Access Control Policy

The vendor shall specify the general features and capabilities of the access control policy recommended to provide effective voting system security.

Although the jurisdiction in which the voting system is operated is responsible for determining the access policies for each election, the vendor shall provide a description of recommended policies for:

a. Software access controls
b. Hardware access controls
c. Communications
d. Effective password management
e. Protection abilities of a particular operating system
f. General characteristics of supervisory access privileges
g. Segregation of duties
h. Any additional relevant characteristics

7.2.1.1 Individual Access Privileges

Voting system vendors shall:

a. Identify each person to whom access is granted, and the specific functions and data to which each person holds authorized access

b. Specify whether an individual's authorization is limited to a specific time, time interval or phase of the voting or counting operations

c. Permit the voter to cast a ballot expeditiously, but preclude voter access to all aspects of the vote counting processes

7.2.1.2 Access Control Measures

Vendors shall provide a detailed description of all system access control measures designed to permit authorized access to the system and prevent unauthorized access. Examples of such measures include:

a. Use of data and user authorization
b. Program unit ownership and other regional boundaries
c. One-end or two-end port protection devices
d. Security kernels
e. Computer-generated password keys
f. Special protocols
g. Message encryption
h. Controlled access security

Vendors also shall define and provide a detailed description of the methods used to prevent unauthorized access to the access control capabilities of the system itself.

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.

7.3.1 Polling Place Security

For polling place operations, vendors 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

Vendors 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 vendor 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. Vendors 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 vendor 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 vendor 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.

b. The EAC accredited testing lab shall witness the final build of the executable version of the certified voting system software performed by the vendor.

i. The testing lab shall create a complete record of the build that includes: a unique identifier (such as a serial number) for the complete record; a list of unique identifiers of unalterable storage media associated with the record; the time, date, location, names and signatures of all people present; the source code and resulting executable file names; the version of voting system software; the certification application number of the voting system; the name and versions of all (including third party) libraries; and the name, version, and configuration files of the development environment used for the build.

ii. The record of the source code and executable files shall be made on unalterable storage media. Each piece of media shall have a unique identifier.

Discussion: Unalterable storage media includes technology such as a CD–R, but not CD–RW. The unique identifiers appear on indelibly printed labels and in a digitally signed file on the unalterable storage media.

iii. The testing lab shall retain this record until notified by the EAC that it can be archived.

c. After EAC certification has been granted, the testing lab shall create a subset of the complete record of the build that includes a unique identifier (such as a serial number) of the subset, the unique identifier of the complete record, a list of unique identifiers of unalterable storage media associated with the subset, the vendor and product name, the version of voting system software, the certification number of the voting system, and all the files that resulted from the build and binary images of all installation programs.

iii. The record of the software shall be made on unalterable storage media. Each piece of media shall have a unique identifier.

iv. The testing lab shall retain a copy, send a copy to the vendor, and send a copy to the NIST National Software Reference Library (NSRL)[2] and/or to any repository designated by a State.

[2] The National Software Reference Library (NSRL) is a repository of software maintained by the National Institute of Standards and Technology. It was designed to meet the need for court admissible evidence in the identification of software files. The EAC has designated the NSRL as a repository for voting system software. Information is available at *www.nsrl.nist.gov.*

v. The NSRL shall retain this software until notified by the EAC that it can be archived.

d. The vendor shall provide the NSRL and any repository designated by a state with a copy of the software installation disk, which the vendor 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 vendor 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.

e. 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.

f. The vendors and testing labs shall document to whom they provide voting system software.

7.4.5 Software Reference Information

The NSRL or other repository designated by a state election office shall generate reference information using the binary images of the (a) certified voting system software received on unalterable storage media from testing labs and (b) election-specific software received on unalterable storage media from jurisdictions.

a. The NSRL or other designated repository shall generate reference information in at least one of the following forms: (a) complete binary images, (b) cryptographic hash values or (c) digital signatures of the software.

Discussion: Although binary images, cryptographic hashes, and digital signatures can detect a modification or alteration in the software, they cannot determine if the change to the software was accidental or intentional.

b. The NSRL or other designated repository shall create a record of the creation of reference information that includes: a unique identifier (such as a serial number) for the record; the file names of software and associated unique identifier(s) of the unalterable storage media from which reference information is generated; the time, date and name of people who generated reference information; the type of reference information created; the certification number of the voting system; the voting system software version; the product name; and the vendor name.

c. The NSRL or other designated repository shall retain the unalterable storage media used to generate the reference information until notified by the EAC that it can be archived.

7.4.5.1 Hashes and Digital Signatures

a. The NSRL or other designated repository that generates hash value and/or digital signature reference information shall use FIPS-approved algorithms for hashing and signing.

i. The NSRL or other designated repository that generates hash values, digital signatures reference information or cryptographic keys shall use a FIPS 140–2 level 1 or higher validated cryptographic module.

Discussion: See *http://www.csrc.nist.gov/cryptval/* for information on FIPS 140–2.

ii. The NSRL or other designated repository that generates sets of hash values and digital signatures for reference information shall include a hash value or digital signature covering the set of reference information.

b. If the NSRL or other designated repository uses public key technology, the following requirements shall be met:

i. Public and private key pairs used by the repository to generate digital signatures shall be 2048-bits or greater in length

ii. The repository's private keys used to generate digital signature reference information shall be used for no more than three years

iii. Public keys used to verify digital signature reference information shall be placed on unalterable storage media if not contained in a signed non-proprietary format for distribution.

Discussion: Examples of non-proprietary standard formats include X.509 or PKCS#7.

iv. All copies of public key unalterable storage media made by the repository shall be labeled so that they are uniquely identifiable, including at a minimum: a unique identifier (such as a serial number) for the unalterable storage media; the time, date, location and name(s) of the repository owning the associated private keys; documentation about its creation; and an indication that the contents are public keys.

v. The NSRL or other designated repository shall document to whom they provide unalterable storage media containing their public keys used to verify digital signature reference information including at a minimum: the uniquely identified public keys, the time and date provided, the name of the organization, and the name and contact information (phone, address, email address) of the recipient.

vi. When a private key used to generate digital signature reference information becomes compromised, the NSRL or other designated repository shall provide notification to recipients of the associated public key that the private key has been compromised and the date on which it was compromised.

c. The NSRL or other designated repository shall make both the reference information available on unalterable storage media and its associated documentation that is labeled by the repository that created it uniquely identifiable by including at a minimum: a unique identifier (such as a serial number) for the storage media; the time, date, location and name of the creating repository; and an indication that the contents are reference information.

7.4.6 Software Setup Validation

a. Setup validation methods shall verify that no unauthorized software is present on the voting equipment.

b. The vendor shall have a process to verify that the correct software is loaded, that there is no unauthorized software, and that voting system software on voting equipment has not been modified, using the reference information from the NSRL or from a State designated repository.

i. The process used to verify software should be possible to perform without using software installed on the voting system.

ii. The vendor shall document the process used to verify software on voting equipment.

iii. The process shall not modify the voting system software on the voting system during the verification process.

c. The vendor shall provide a method to comprehensively list all software files that are installed on voting systems.

d. The verification process should be able to be performed using COTS software and hardware available from sources other than the voting system vendor.

i. 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.

ii. 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.

e. Voting system equipment shall provide a means to ensure that the system software can be verified through a trusted external interface, such as a read-only external interface, or by other means.

i. The external interface shall be protected using tamper evident techniques

ii. The external interface shall have a physical indicator showing when the interface is enabled and disabled

iii. The external interface shall be disabled during voting

iv. The external interface should provide a direct read-only access to the location of the voting system software without the use of installed software

f. Setup validation methods shall verify that registers and variables of the voting system equipment contain the proper static and initial values.

i. The vendor should provide a method to query the voting system to determine the values of all static and dynamic registers and variables including the values that jurisdictions are required to modify to conduct a specific election.

ii. The vendor shall document the values of all static registers and variables, and the initial starting values of all dynamic registers and variables listed for voting system software, except for the values set to conduct a specific election.

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.

b. Voting systems that use telecommunications to communicate between system components and locations before the polling place is officially closed shall:

i. Implement an encryption standard currently documented and validated for use by an agency of the U.S. government

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, vendor, 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. Vendors 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, vendors 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 vendor 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 test labs 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 by the state, 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 by the state

f. Address threats emerging too late to correct the system by:

i. Providing prompt, emergency notification to the accredited test labs 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 an accredited test lab and the EAC or state certification authority 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 Incomplete Election Returns

If the voting system provides access to incomplete election returns and interactive inquiries before the completion of the official count, the system shall:

a. Be designed to provide external access to incomplete election returns (for equipment that operates in a central counting environment), only if that access for these purposes is authorized by the statutes and regulations of the using agency. 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

7.6.2 Casting Individual Ballots

Systems designed for transmission of telecommunications 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 vendor or contractor, and using in-person authentication of individual voters.

7.6.2.1 Documentation of Mandatory Security Activities

Vendors 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 single vote

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 vendor 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 vendor 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 vendor 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. The encryption shall be as defined in Federal Information Processing Standards (FIPS) 197, ‘‘Advanced Encryption Standard (AES).’’

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 Independent Verification Systems

7.8.1 Overview

Independent verification (IV) systems are electronic voting systems that produce multiple independent cast vote records of voter ballot selections, which can be audited to a high level of precision. For this to happen, the cast vote records must be handled according to the following protocol:

- At least two cast vote records of the voter's selections are produced and one of the records is then stored in a manner that it cannot be modified by the voting system. For example, the voting system creates a record of the voter's selections and then copies it to unalterable storage media.
- The voter must be able to verify that both cast vote records are correct and match before leaving the polling place, *e.g.*, verify his or her selections on the voting machine summary screen and also verify the second record on the unalterable storage media.
- The verification processes for the two cast vote records must be independent of each other, and at least one of the records must be verified directly by the voter.
- The contents of the two cast vote records also can be checked later for consistency through the use of unique identifiers that allow the records to be linked.

The cast vote records would be formatted so that at least one set is usable in an efficient counting process by the electronic voting system and the other set is usable in an efficient process of auditing or verifying the agreement between the two sets.

Given these conditions, the multiple cast vote records are considered to be distinct and independently verifiable, that is, both records are not under the control of the same system processes. As a result of this independence, the audit records can be used to check the accuracy of the counted records. Because the records are separately stored, an attacker who can compromise one will also have to compromise the other.

The voter verifiable paper audit trail (VVPAT) methodology is one of several classes of IV systems. In this approach, the voter can directly compare the electronic summary screen of the voting machine with the printed paper audit record. (This is not to be confused with the paper ballot that is produced by optical scan voting systems that the voter visually verifies before placing it in the ballot box or tabulator.) Requirements for DREs with a VVPAT feature are provided below to reflect the fact that a number of States currently require this feature.

There are a variety of other IV approaches for the voter to verify his or her selections with systems that produce an electronic record for verification. Appendix C describes the characteristics of these systems in more detail. They include:

- Split process systems, which use separate devices for the voters to record and verify their ballot selections
- Cryptographic systems, which provide voters with coded receipts that can be used to verify their ballot selections
- Witness systems, which use an independent module to create the second record

7.8.2 Basic Characteristics of IV Systems

This section describes a preliminary set of basic characteristics that apply to all types of IV systems. This information is provided for the purpose of introducing these concepts for consideration in voting system design. It is anticipated that future voting systems will be required to provide some type of independent verification feature to enable voters to have confidence that their ballot selections are correctly recorded and counted.

An independent verification system produces at least two independent cast vote records of ballot selections via interactions with the voter, such that one record can be compared against the other to check their equality of content.

Discussion: This is the fundamental characteristic of IV systems. The records can be checked against one another to determine whether or not the voter selections are correctly recorded.

The voter verifies the content of each cast vote record and either (a) verifies at least one of the records directly or (b) verifies both records indirectly if the records are each under the control of independent processes.

Discussion: Direct verification involves using human senses; for example, directly reading a paper record via one's eyesight. Indirect verification involves using an intermediary to perform the verification; for example, verifying an electronic ballot image on the voting machine.

The creation, storage and handling of the cast vote records are sufficiently separate that the failure or compromise of one record does not cause the failure or compromise of another.

Discussion: The records must be stored on different media and handled independently of each other so that no one process could compromise all records. If an attack can alter one record, it should still be very difficult to alter the other record.

Both cast vote records are highly resistant to damage or alteration and capable of long-term storage.

Discussion: The records should be difficult to alter or damage so that they could be used in case the counted records are damaged or lost.

The processes of verification for the cast vote records do not all depend on the same device, software module, or system for their integrity, and are sufficiently separate that each record provides evidence of the voter's selections independently of its corresponding record.

Discussion: For example, the verification of the summary screen (electronic record) of a DRE is sufficiently separate from the verification of a paper record printed by a VVPAT component or a copy of the electronic record stored on a separate system.

The multiple cast vote records are linked to their corresponding audit records by including a unique identifier within each record.

Discussion: The identifier serves the purpose of uniquely identifying and linking the records for cross-checking.

Each cast vote record includes information identifying the following:

- An identification of the polling place and precinct
- Whether the balloting is provisional, early, or on election day
- Ballot style
- A timestamp generated when the voting machine is enabled to begin a voting session that can be used to correctly group the cast vote records
- A unique identifier associated with the voting machine

Discussion: The identifier could be a serial number or other unique ID.

The cryptographic software used in IV systems is approved by the U.S. Government's Cryptographic Module Validation Program, as applicable.

Discussion: IV voting systems may use cryptographic software for a number of different purposes, including calculating checksums, encrypting records, authentication, generating random numbers, and for digital signatures. This software should be reviewed and approved by the Cryptographic Module Validation Program (CMVP). There may by cryptographic voting schemes where the cryptographic algorithms used are necessarily different from any algorithms that have approved CMVP implementations, thus CMVP-approved software shall be used where feasible. The CMVP Web site is *http://csrc.nist.gov/cryptval.*

7.9 Voter Verifiable Paper Audit Trail Requirements

This section contains requirements for DREs with a Voter Verifiable Paper Audit Trail (VVPAT) component. 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 vendor'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.

7.9.1 Display and Print a Paper Record

a. The voting system shall print and display a paper record of the voter ballot selections prior to the voter making his or her selections final by casting the ballot.

Discussion: This is the basic requirement for VVPAT capability. It requires the paper record to be created as a distinct representation of the voter ballot selections. It requires the paper record to contain the same information as the electronic record and be suitable for use in verifications of the voting machine's electronic records.

b. The paper record shall constitute a complete record of ballot selections that can be used to assess the accuracy of the voting machine's electronic record, to verify the election results, and, if required by state law, in full recounts.

Discussion: This requirement exists to make clear that it is possible to use the paper record for checks of the voting machine's accuracy in recording voter ballot selections, as well as usable for election audits (such as mandatory 1% recounts). The paper record shall also be suitable for use in full recounts of the election if required by state law.

c. The paper record shall contain all voter selection information stored in the electronic (ballot image) record.

Discussion: The electronic ballot image record cannot hide any information related to ballot selections; all information relating to voter selections must be equally present in both records. The electronic record may contain other items that don't necessarily need to be on the paper record, such as digital signature information.

7.9.2 Approve or Void the Paper Record

a. The voting equipment shall allow the voter to approve or void the paper record.

Discussion: There are three possible scenarios regarding the voter's disposition of the paper record.

- The voter can verify that the ballot selections displayed on the DRE summary screen and those printed on the paper record are the same. If they are, and the voter is satisfied with these selections, the voter can proceed to cast his or her ballot, thereby approving the paper record.
- If the selections match, but the voter wishes to change one or more selections, the paper record must be voided so a new paper record can be created to compare to the new summary screen displayed after the voter changes his or her ballot selections.
- In the event the selections do not match between the summary screen and the paper record, the voter shall immediately request assistance from a poll worker. A non-match could indicate a potential voting machine or printer malfunction.

b. The voting equipment shall, in the presence of the voter, mark the paper record as being approved by the voter if the ballot selections are accepted; or voided or if the voter decides to change one or more selections.

c. If the records do not match, the voting equipment shall mark and preserve the paper record and shall provide a means to preserve the corresponding electronic record so the source of error or malfunction can be analyzed.

Discussion: The voting machine shall be withdrawn from service immediately and its use discontinued in accordance with jurisdiction procedures.

d. The voting machine shall not record the electronic record until the paper record has been approved by the voter.

e. Vendor documentation shall include procedures to enable the election official to return a voting machine to correct operation after a voter has used it incompletely or incorrectly. This procedure shall not cause discrepancies between the tallies of the electronic and paper records.

7.9.3 Electronic and Paper Record Structure

a. All cryptographic software in the voting system shall be approved by the U.S. Government's Cryptographic Module Validation Program, as applicable.

Discussion: Cryptographic software may be used for a number of different purposes, including calculating checksums, encrypting records, authentication, generating random numbers, and digital signatures. This software should be reviewed and approved by the Cryptographic Module Validation Program (CMVP). There may be cryptographic voting schemes where the cryptographic algorithms used are necessarily different from any algorithms that have approved CMVP implementations, thus CMVP approved software should be used where feasible but is not required. The CMVP website is *http://csrc.nist.gov/cryptval.*

b. The electronic ballot image and paper records shall include information about the election.

i. The voting equipment shall be able to include an identification of the particular election, the voting site and precinct, and the voting machine.

Discussion: If the voting site and precinct are different, both should be included.

ii. The records shall include information identifying whether the balloting is provisional, early, or on election day, and information that identifies the ballot style in use.

iii. The records shall include a voting session identifier that is generated when the voting equipment is placed in voting mode, and that can be used to identify the records as being created during that voting session.

Discussion: If there are several voting sessions on the same voting machine on the same day, the voting session identifiers must be different. They should be generated from a random number generator.

c. The electronic ballot image and paper records shall be linked by including a unique identifier within each record that can be used to identify each record uniquely and each record's corresponding record.

Discussion: The identifier serves the purpose of uniquely identifying and linking the records for cross-checking.

d. The voting machine should generate and store a digital signature for each electronic record.

e. The electronic ballot image records shall be able to be exported for auditing or analysis on standards-based and /or COTS information technology computing platforms.

i. The exported electronic ballot image records shall be in a publicly available, non-proprietary format.

Discussion: It is advantageous when all electronic records, regardless of manufacturer, use the same format or can easily be converted to a publicly available, non-proprietary format; for example, the OASIS Election Markup Language (EML) Standard.

ii. The records should be exported with a digital signature, which shall be calculated on the entire set of electronic records and their associated digital signatures.

Discussion: This is necessary to determine if records are missing or substituted.

iii. The voting system vendor shall provide documentation as to the structure of the exported ballot image records and how they shall be read and processed by software.

iv. The voting system vendor shall provide a software program that will display the exported ballot image records and that may include other capabilities such as providing vote tallies and indications of undervotes.

v. The voting system vendor shall provide full documentation of procedures for exporting electronic ballot image records and reconciling those records with the paper audit records.

f. The paper record should be created in a format that may be made available across different manufacturers of electronic voting systems.

Discussion: There may be a future requirement for some commonality in the format of paper records.

g. The paper record shall be created such that its contents are machine readable.

Discussion: This can be done by using specific OCR fonts or barcodes.

i. The paper record shall contain error correcting codes for the purpose of detecting read errors and for preventing other markings on the paper record from being misinterpreted when machine reading the paper record.

Discussion: This requirement is not mandatory if a state prohibits the paper record from containing any information that cannot be read and understood by the voter. This requirement serves the purpose of detecting scanning errors and preventing stray or deliberate markings on the paper from being interpreted as valid data.

h. If barcode is used, the voting equipment shall be able to print a barcode with each paper record that contains the human-readable contents of the paper record.

Discussion: This requirement is not mandatory if a state prohibits the paper record from containing any information that cannot be read and understood by the voter.

i. The barcode shall use an industry standard format and shall be able to be read using readily available commercial technology.

Discussion: Examples of such codes are Maxi Code or PDF417.

ii. If the corresponding electronic record contains a digital signature, the digital signature shall be included in the barcode on the paper record.

iii. The barcode shall not contain any information other than the paper record's human-readable content, error correcting codes, and digital signature information.

7.9.4 Equipment Security and Reliability

a. The voting machine shall provide a standard, publicly documented printer port (or the equivalent) using a standard communication protocol.

Discussion: Using a standard, publicly documented printer protocol assists in security evaluations of system software.

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 DRE internal audit log.

d. The paper path between the printing, viewing and storage of the paper record shall be protected and sealed from access except by authorized election officials.

e. The printer shall not be permitted to communicate with any system or machine other than the voting machine to which it is connected.

f. 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.

g. The voting machine shall detect errors and malfunctions such as paper jams or low supplies of consumables such as paper and ink that may prevent paper records from being correctly displayed, printed or stored.

Discussion: This could be accomplished in a variety of different ways; for example, a printer that is out of paper or jammed could issue a different audible alarm for each condition.

h. If an error or malfunction occurs, the voting machine shall suspend voting operations and should present a clear indication to the voter and election officials of the malfunction.

i. The voting machine shall not record votes if an error or malfunction occurs.

j. Printing devices should contain sufficient supplies of paper and ink to avoid reloading or opening equipment covers or enclosures and thus potential circumvention of security features; or be able to reload paper and ink with minimal disruption to voting and without circumvention of security features such as seals.

k. Vendor documentation shall include procedures for investigating and resolving printer malfunctions including, but not limited to; printer operations, misreporting of votes, unreadable paper records, and power failures.

l. Vendor documentation shall include printer reliability specifications including Mean Time Between Failure estimates, and shall include recommendations for appropriate quantities of backup printers and supplies.

m. 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.

n. The paper record shall be sturdy, clean, and of sufficient durability to be used for verifications, reconciliations, and recounts conducted manually or by automated processing.

7.9.5 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.

7.9.6 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.

7.9.7 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.

8 Quality Assurance Requirements

Table of Contents

8 Quality Assurance Requirements

8 Quality Assurance Requirements

8.1 Scope

Quality assurance provides continuous confirmation that a voting system conforms with the Guidelines and to the requirements of state and local jurisdictions. Quality assurance is a vendor function 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 voting system and reducing dependence on system tests at the end of the life cycle to detect deficiencies, thus helping ensure the system:

- Meets stated requirements and objectives
- Adheres to established standards and conventions
- Functions consistently with related components and meets dependencies for use within the jurisdiction
- Reflects all changes approved during its initial development, internal testing, national certification, and, if applicable, state certification processes

8.2 General Requirements

The voting system vendor is responsible for designing and implementing a quality assurance program to ensure that the design, workmanship, and performance requirements are achieved in all delivered systems and components. At a minimum, this program shall:

a. Include procedures for specifying, procuring, inspecting, accepting, and controlling parts and raw materials of the requisite quality

b. Require the documentation of the hardware and software development process

c. Identify and enforce all requirements for:

i. In-process inspection and testing that the manufacturer deems necessary to ensure proper fabrication and assembly of hardware

ii. Installation and operation of software and firmware

d. Include plans and procedures for post-production environmental screening and acceptance testing

e. Include a procedure for maintaining all data and records required to document and verify the quality inspections and tests

8.3 Components from Third Parties

A vendor who does not manufacture all the components of its voting system, but instead procures components as standard commercial items for assembly and integration into a voting system, shall verify that the supplier vendors follow documented quality assurance procedures that are at least as stringent as those used internally by the voting system vendor.

8.4 Responsibility for Tests

The manufacturer or vendor shall be responsible for performing all quality assurance tests, acquiring and documenting test data, and providing test reports for examination by the test lab as part of the national certification process. These reports shall also be provided to the purchaser upon request.

8.5 Parts and Materials Special Tests and Examinations

In order to ensure that voting system parts and materials function properly, vendors shall:

a. Select parts and materials to be used in voting systems and components according to their suitability for the intended application. Suitability may be determined by similarity of this application to existing standard practice or by means of special tests

b. Design special tests, if needed, to evaluate the part or material under conditions accurately simulating the actual voting system operating environment

c. Maintain the resulting test data as part of the quality assurance program documentation

8.6 Quality Conformance Inspections

The vendor performs conformance inspections to ensure the overall quality of the voting system and components delivered to the test lab for national certification testing and to the jurisdiction for implementation.

To meet the conformance inspection requirements the vendor or manufacturer shall:

a. Inspect and test each voting system or component to verify that it meets all inspection and test requirements for the system

b. Deliver a record of tests or a certificate of satisfactory completion with each system or component

8.7 Documentation

Vendors are required to produce documentation to support the independent testing required for their products to be granted national certification. Volume II, Section 2, Description of the Technical Data Package, identifies the documentation required for the national certification testing process. This documentation shall be sufficient to serve the needs of the test lab, election officials, and maintenance technicians. It shall be prepared and published in accordance with standard commercial practice for information technology and electronic and mechanical equipment. It shall include, at a minimum, the following:

- System overview
- System functionality description
- System hardware specification
- Software design and specifications
- System security specification
- System test and verification specification
- System operations procedures
- System maintenance procedures
- Personnel deployment and training requirements
- Configuration management plan
- Quality assurance program
- System change notes

9 Configuration Management Requirements

Table of Contents

9 Configuration Management Requirements

9 Configuration Management Requirements

9.1 Scope

This section contains specific requirements for configuration management of voting systems. For the purpose of the Guidelines, configuration management is defined as a set of activities and associated practices that ensures full knowledge and control of the components of a system, starting with its initial development and progressing through its ongoing maintenance and enhancement. This section describes activities in terms of their purposes and outcomes. It does not describe specific procedures or steps to be employed to accomplish them. Specific steps and procedures are left to the vendor to select.

Vendors are required to submit these procedures as part of the Technical Data Package for system certification. State or local election legislation, regulations, or contractual agreements may require the vendor to conform to additional requirements for configuration management or to adopt specific required procedures. EAC and state and local election officials reserve the right to inspect vendor facilities and operations to determine conformance with the vendor's reported procedures and with these requirements.

9.1.1 Configuration Management Requirements

Configuration management addresses a broad set of record keeping, auditing, and reporting activities that contribute to full knowledge and control of a system and its components. These activities include:

- Identifying discrete system components
- Creating records of a formal baseline and later versions of components
- Controlling changes made to the system and its components
- Releasing new versions of the system
- Auditing the system, including its documentation, against configuration management records
- Controlling interfaces to other systems
- Identifying tools used to build and maintain the system

9.1.2 Organization of Configuration Management Requirements

The requirements for configuration management include:

- Application of configuration management requirements
- Configuration management policy
- Configuration identification

- Baseline, promotion, and demotion procedures
- Configuration control procedures
- Release process
- Configuration audits
- Configuration management resources

9.1.3 Application of Configuration Management Requirements

Requirements for configuration management apply to all components of voting systems regardless of the specific technologies employed. These components include:

- Software
- Hardware
- Communications
- Documentation
- Identification and naming conventions (including changes to these conventions) for software programs and data files
- Development and testing artifacts such as test data and scripts
- File archiving and data repositories

9.2 Configuration Management Policy

The vendor shall describe its policies for configuration management in the Technical Data Package. This description shall address the following elements:

- Scope and nature of configuration management program activities
- Breadth of application of the vendor's policies and practices to the voting system, i.e., extent to which policies and practices apply to the total system, and extent to which policies and practices of suppliers apply to particular components, subsystems or other defined system elements

9.3 Configuration Identification

Configuration identification is the process of identifying, naming, and acquiring configuration items. Configuration identification encompasses all system components.

9.3.1 Classification and Naming Configuration Items

The vendor shall describe the procedures and conventions used to classify configuration items into categories and subcategories, uniquely number or otherwise identify configuration items and name configuration items.

9.3.2 Versioning Conventions

When a system component is part of a higher level system element such as a subsystem, the vendor shall describe the conventions used to:

a. Identify the specific versions of individual configuration items and sets of items that are incorporated in higher level system elements such as subsystems

b. Uniquely number or otherwise identify versions

c. Name versions

9.4 Baseline and Promotion Procedures

The vendor shall establish formal procedures and conventions for establishing and providing a complete description of the procedures and related conventions used to:

a. Establish a particular instance of a component as the starting baseline

b. Promote subsequent instances of a component to baseline status as development progresses through to completion of the initial completed version released to the accredited test lab for testing

c. Promote subsequent instances of a component to baseline status as the component is maintained throughout its life cycle until system retirement (i.e., the system is no longer sold or maintained by the vendor)

9.5 Configuration Control Procedures

Configuration control is the process of approving and implementing changes to a configuration item to prevent unauthorized additions, changes or deletions. The vendor shall establish such procedures and related conventions, providing a complete description of those procedures used to:

a. Develop and maintain internally developed items

b. Acquire and maintain third-party items

c. Resolve internally identified defects for items regardless of their origin

d. Resolve externally identified and reported defects (i.e., by customers and accredited test labs)

9.6 Release Process

The release process is the means by which the vendor installs, transfers or migrates the system to the accredited test lab and, eventually, to its customers. The vendor shall establish such procedures and related conventions, providing a complete description of those used to:

a. Perform a first release of the system to an accredited test lab

b. Perform a subsequent maintenance or upgrade release of the system or particular components, to an accredited test lab

c. Perform the initial delivery and installation of the system to a customer, including confirmation that the installed version of the system matches exactly the certified system version

d. Perform a subsequent maintenance or upgrade release of the system or a particular component to a customer, including confirmation that the installed version of the system matches exactly the certified system version

9.7 Configuration Audits

The Guidelines require two types of configuration audits: Physical Configuration Audits (PCA) and Functional Configuration Audits (FCA).

9.7.1 Physical Configuration Audit

The Physical Configuration Audit is conducted by the accredited test lab to compare the voting system components submitted for certification to the vendor's technical documentation.

For the PCA, a vendor shall provide:

a. Identification of all items that are to be a part of the software release

b. Specification of compiler (or choice of compilers) to be used to generate executable programs

c. Identification of all hardware that interfaces with the software

d. Configuration baseline data for all hardware that is unique to the system

e. Copies of all software documentation intended for distribution to users, including program listings, specifications, operations manual, voter manual, and maintenance manual

f. User acceptance test procedures and acceptance criteria

g. Identification of any changes between the physical configuration of the system submitted for the PCA and that submitted for the FCA, with a certification that any differences do not degrade the functional characteristics

h. Complete descriptions of its procedures and related conventions used to support this audit by:

i. Establishing a configuration baseline of the software and hardware to be tested

ii. Confirming whether the system documentation matches the corresponding system components

9.7.2 Functional Configuration Audit

The Functional Configuration Audit is conducted by the accredited test lab to verify that the system performs all the functions described in the system documentation. The vendor shall:

a. Completely describe its procedures and related conventions used to support this audit for all system components

b. Provide the following information to support this audit:

i. Copies of all procedures used for module or unit testing, integration testing, and system testing

ii. Copies of all test cases generated for each module and integration test, and sample ballot formats or other test cases used for system tests

iii. Records of all tests performed by the procedures listed above, including error corrections and retests

In addition to such audits performed by the accredited test lab during the national certification process, elements of this audit may also be performed by state election organizations during the system certification process and individual jurisdictions during system acceptance testing.

9.8 Configuration Management Resources

Often, configuration management activities are performed with the aid of automated tools. Assuring that such tools are available throughout the system life cycle—including whether the vendor is acquired by or merged with another organization—is critical to effective configuration management. Vendors may choose the specific tools they use to perform the record keeping, auditing, and reporting activities of the configuration management standards.

The resources documentation requirements focus on assuring that procedures are in place to record information about the tools to help ensure that they, and the data they contain, can be transferred effectively and promptly to a third party should the need arise. Within this context, a vendor is required to develop and provide a complete description of the procedures and related practices for maintaining information about:

a. Specific tools used, current version, and operating environment specifications

b. Physical location of the tools, including designation of computer directories and files

c. Procedures and training materials for using the tools

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: Voting station equipped for individuals with disabilities

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.

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.

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 communicate ballot selections 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 voter 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

C

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: 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 vendor 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

commercial off-the-shelf (COTS): Commercial, readily available hardware devices (such as card readers, printers or personal computers) or software products (such as operating systems, programming language compilers, or database management systems)

Common Industry Format (CIF): Refers to the format described in ANSI/INCITS 354–2001 ''Common Industry Format (CIF) for Usability Test Reports

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.

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

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

data accuracy: (1) Data accuracy is defined in terms of ballot position error rate. This rate applies to the voting functions and supporting equipment that capture, record, store, consolidate and report the specific selections, and absence of selections, made by the voter for each ballot position. (2) The system's ability to process voting data absent internal errors generated by the system. It is distinguished from data integrity, which encompasses errors introduced by an outside source.

data integrity: Invulnerability of the system to accidental intervention or deliberate, fraudulent manipulation that would result in errors in the processing of data. It is distinguished from data accuracy that encompasses internal, system-generated errors.

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: An electronic voting system that utilizes electronic components for the functions of ballot presentation, vote capture, vote recording, and tabulation which are logically and physically integrated into a single unit. A DRE produces a tabulation of the voting data stored in a removable memory component and in printed hardcopy.

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 cast vote record: An electronic version of the cast vote record

electronic voter 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 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.

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

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 vendor'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.

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 vendor 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 ''test labs.'' 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

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

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

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 an accredited test lab delivered to the EAC with a recommendation regarding granting a certification number

NIST: National Institute of Standards and Technology

non-partisan office: Elected office for which candidates run without political party affiliation

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 an accredited test laboratory that compares the voting system components submitted for certification testing to the vendor'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 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.

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 vendor'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

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.

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

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.

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.

tabulator: Device that counts votes

technical data package: Vendor 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 voting system test lab 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

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

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

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 voter interface which presents ballot information and voting instructions as video images. See also ballot.

vote for N of M: A ballot choice in which voters are allowed to vote for a specified number (''N'') of candidates in a multi-seat (''M'') contest

voted ballot: Ballot that contains all of a voter's selections and has been cast

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 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).

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.

voting system test laboratory: Test laboratory accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) to be competent to test voting systems. When NVLAP has completed its evaluation of a test lab, the Director of NIST will forward a recommendation to the EAC for the completion of the accreditation process.

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 and book 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

B References

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

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 (1995–010 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 (1995–01) Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques. Section 4 Electrical Fast Transient/Burst 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 TR 9294.1990 Information Technology Guidelines for the Management of Software Documentation

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 10007:1995 Quality Management Guidelines for Configuration Management

ISO 10005–1995 Quality Managment Guidelines for Quality Plans

ANSI/ISO/ASQC QS9000–3–1997 QM and QA standards Part 3: Guidelines for the application of ANSI/ISO/ASQC Q9000–1994 to the Development, Supply, Installation, and Maintenance of Computer Software

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 Interface Between Data Terminal Equipment and Automatic Calling 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

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 U.S.C. Sections 15301–15545

Americans With Disabilities Act of 1990, Pub. L. 101–336, 42 U.S.C. Sections 12101–12213

42 U.S.C. 1974

Occupational Safety and Health Act, Pub. L. 91–596, 29 U.S.C. Sections 651–678, 42 U.S.C. Section 3142–1

Architectural Barriers Act of 1968, Pub. L. 90–480, 42 U.S.C. Sections 4151–4157

Voting Rights Act of 1965, Pub. L. 89–110, 42 U.S.C. 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 Information Technology Guidelines for the Preparation of 10176.1998 Programming Language Standards

ANSI/ISO/IEC 6592.2000 Information Technology Guidelines for the Documentation of Computer Based Application Systems

ANSI/ISO/ASQC 1997 Quality management and quality assurance standards Part 3: Q9000–3—Guidelines for the application of ANSI/IAO/ASQC Q9001–1994 to the Development, supply, installation and maintenance of computer software

ANSI/ISO/ASQC Q9000–1–1994 Quality Management and Quality Assurance Standards—Guidelines for Selection and Use

ANSI/ISO/ASQC Q10007–1995 Quality Management Guidelines for Configuration Management

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 8:2001 ITU–T Recommendation X.509 (2000), Information technology—9594—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 Handbook for Reliability Test Methods, Plans, and Environments for 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.

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.*

Appendix C: Independent Verification Systems

Table of Contents

Appendix C: Independent Verification Systems

Appendix C is an informative section that describes Independent Verification systems followed by characteristics of the types of Independent Verification systems which will be used as the basis for future requirements. This information is preliminary and will be evolving with further research.

C.1 Independent Verification Systems

A primary objective for using electronic voting systems is the production of voting records that are highly precise, highly reliable, and easily counted—in essence, an accurate representation of ballot selections whose handling requirements are reasonable. To meet this objective, there are many factors to consider in an electronic voting system design, including:

- The environment provided for voting, including the physical and environmental factors
- The ease with which voters can use the voting system, i.e., its usability
- The robustness and reliability of the voting equipment
- The capability of the records to be used in audits

Independent Verification (IV) systems have as their primary objective the production of independent records of voter ballot selections that are capable of being used in audits in which their correctness can be audited to a very high level of precision. The primary voting security and integrity issues addressed by IV systems are:

- Whether electronic voting systems are accurately recording ballot selections
- Whether the ballot record contents can be audited precisely post-election

The threats addressed by IV systems are those that could cause a voting system to inaccurately record the voter's selections or cause damage to the voting system records. These threats could occur via any number of means including human error, accident or fraudulent activity. The threats are addressed mainly by providing, in the voting system design, the capability for ballot record audits to detect precisely whether specific records are correct as recorded or damaged, missing, or fraudulent.

C.1.1 Improved Accuracy in Independent Verification Audits

Independent Verification is the top-level categorization for electronic voting systems that produce multiple records of ballot selections that can be audited to a high level of precision. For this to happen, the records must be produced and made verifiable by the voter, and then subsequently handled according to the following protocol:

- At least two records of voter selections are produced and one of the records is then stored such that it cannot be modified by the voting system, e.g., the voting system creates a record of voter selections and then copies it to some unalterable media
- The voter must be able to verify that both records are correct, e.g., verify his or her selections on the voting system's display and also verify the second record of selections stored on the unalterable storage media
- The verification processes for the two records must be independent of each other and (a) at least one of the records must be verified directly by the voter, or (b) it is acceptable for the voter to indirectly verify both records if they are stored on independent systems
- The content of the two records can be checked later for consistency through the use of identifiers that allow the records to be linked An assumption is made that at least one set of records is usable in an efficient counting process such as an automated tabulator, and the other set of records is usable in an efficient process of verifying its agreement with the other set of records used in the counting process. The sets of records would preferentially be different in form and thus have more resistance to accidental or deliberate damage.

Given these conditions, the multiple records are said to be distinct and independently verifiable; that is, both records are not under the control of the same processes. As a result of this independence, one record can be used to audit or check the accuracy of the other record. Because the storage of the records is separate, an attacker who can compromise one of the records still will face a difficult task in compromising the other.

C.1.2 Example Independent Verification Systems

The following sections present overviews of several types of IV systems. Some of these systems have not been marketed as yet but are included here to help clarify approaches to independent verification systems. The Independent Verification systems discussed are:

- Voting systems with a split process architecture [3]
- End-to-end voting systems that include cryptographic audit schemes
- Witness systems that take a picture of or otherwise capture an indirect verification of ballot selections
- Direct independent verification, including voting systems that produce an optically scanned ballot or that produce a voter verifiable paper audit trail

C.1.2.1 The Split Process Architecture for IV Systems

A voting machine with a split process architecture consists of vote capture and verification stations that are separate, i.e., two physical devices. A voter inserts an object called a token into the capture station to make ballot selections and then takes the token object to the verification station to review and store his or her votes. The token object could be paper or unalterable media. Two records of the vote are created: one on the token object and one by the verification station. Either could be used in the final count.

For any split process voting system, the interaction between the voter and the split process operates as follows:

- A voter is given a token object that has been initialized to be blank
- Supporting information is written to the token object including the ballot and identification information about the election and precinct
- The voter inserts the token object into a capture station such as a DRE, which reads the ballot information from the token and then displays the ballot to the voter by some means such as a touch screen. The voter makes his or her ballot selections, which causes a record of the vote to be recorded on the token object
- The voter takes the token object to a separate verification station, which reads the recorded votes from the token object, makes an electronic copy, and displays it to the voter
- The voter verifies that the information is correct and then deposits the token object in a secure container so it can be archived and used later for recounts or audits against the electronic records

Two sets of records are produced: the electronic records and the token records. Typically, the electronic records recorded by the verification station would be counted in the election. The records should be different in form and be resistant to accidental or deliberate damage to be useful for audits and recounts.

In theory, the physical separation of vote capture from vote verification may make analysis of the capture and verification devices easier or less costly. The rationale is that the user interface software on the capture station is expected to be complex and difficult to verify for correctness. On the other hand, the verification station's software is expected to be less complicated because it need only copy the contents of the token, display it to the voter, and store the ballot selections. In general, segregating functions by placing them on physically different systems is a standard computer security practice for making those functions easier to test for correctness and easier to manage securely.

C.1.2.2 End to End Cryptographic IV Systems

End to end systems use cryptographic techniques to store an encrypted copy of the voter's ballot selections. In this way, ballot selections can be audited and demonstrated to have been included in the election count.

End to end systems in existence today generally operate as follows:

- A voter uses a voting machine such as a DRE to make ballot selections
- The DRE issues a paper receipt to the voter that contains information that permits the voter to verify that the choices were recorded correctly. The information does not permit the voter to reveal his or her selections
- The voter may have the option to check that his or her ballot selections were included in the election count, e.g., by checking a web site of values

[3] The split process architecture is otherwise known as the frog protocol, which was first described in the Caltech—MIT report: Voting: What Is, What Could Be, as part of a modular voting architecture. The frog term, i.e., the token, was chosen specifically to convey no information about the physical form of the object used to carry vote information between two separate modules of the voting station. The report is avaialble for download at *http://www.vote.caltech.edu/.*

that (should) match the information on the voter's paper receipt

End to end systems are sometimes referred to as receipt-based systems. They may provide an assurance not only that the correct set of ballot choices was recorded, but that those selections were included in the election count. Some analyses of auditing and cryptographic systems assert that very small numbers of self-audits are required to verify the correctness of an election.

C.1.2.3 Witness IV Systems

A witness system creates the second record of ballot choices by using a separate module to record or witness the voter's verification of the first record. The primary feature of a witness system is that the creation of the record does not require action by the voter. This may result in quicker voting times or voting systems that are simpler to use than other approaches that involve multiple, direct verifications by the voter.

An example of a witness system is a DRE with a camera mounted above its screen. The camera takes pictures and saves them independently of the DRE. It would operate as follows:

- A voter makes ballot selections at the DRE and then presses a button to record his or her vote
- The DRE records the ballot selections and uses them in the election count
- At the time the button is pressed, the camera takes a picture of the DRE summary screen and saves the image. The voter would not be included in the picture.
- This collection of images constitutes a second ballot record that can be used in audits and recounts

As can be seen by this example, the voter's interactions are reduced to making ballot selections at the DRE and pressing a button to make the selections final. If the DRE were to be compromised such that it secretly recorded the ballot choices incorrectly, the stored photographic images would reflect what the voter had seen and verified at the DRE summary screen.

Because the voter may not be able to verify that the creation of the second record was performed accurately, it is important that the creation process be highly reliable and very resistant to accidental or deliberate damage. Also, the suitability of the records for manual or automated auditing is a factor when considering this approach.

C.1.2.4 Direct IV Systems

Direct Independent Verification systems produce a record that the voter may verify directly with the voter's senses and which is then preserved for auditing or counting. Some optical scan voting systems fit this category, as well as DREs with VVPAT capability.

The optical scan voting systems in this category are those in which two records are created: a paper and an electronic record. This system uses Optical Scan Recognition (OCR) to create an electronic record from the paper record after the paper record has been directly verified by the voter. The general operation of this system is:

- A voter uses a marking device such as a DRE to mark a ballot and then presses a button to print the marked ballot
- The voter directly reviews the printed paper record to ensure its correctness, and if correct, places the paper record into a scanner. A procedure would be needed to handle voided ballots.
- The scanner converts the paper record into an electronic format. To reduce errors that may result from scanning the paper record, the paper records might contain a barcode representation of the human readable portion of the ballot.
- The paper record is deposited in a secure receptacle

No verification of the scanned paper record is performed in the above approach. One may assume that the scanning process is highly accurate and can be trusted to create the electronic record correctly; however it would be preferential for the voter to somehow verify that the record was, in fact, created correctly.

A DRE with VVPAT capability is similar to that of the optical scan above but consists typically of a DRE that both creates and records an electronic record, and a printer that creates a paper record of the voter's selections. Like the optical scan system, it creates two distinct representations of the voter's ballot selections: an electronic record and a paper record.

Typically, a voter would use the voting system as follows:

- A voter makes ballot selections and indicates that his or her selections are complete
- A paper record is printed of the voter's ballot selections as displayed on the summary screen. An alternative approach is to print the voter's ballot selections as they are made.
- The voter inspects and directly verifies that the paper record matches the displayed electronic record
- The paper record is deposited in a secure receptacle

Both approaches described here produce paper records that are verified directly by the voter through visual inspection. Voters with sight impairments would require an accessible device for verification that can produce an audible representation of the paper record.

C.1.3 Handling Multiple Records Produced by IV Systems

There are several fundamental questions that need to be addressed when designing the structure and selecting the physical characteristics of IV system records, including:

- How to tell if the records are authentic and not forged
- How to tell if the integrity of the records has remained intact from the time they were recorded
- The suitability of the records for various types of auditing
- How best to address problems if there are errors in the records

Whenever an electronic voting system produces multiple records of votes, there is some possibility that one or more of the records may not match. Records can be lost, or deliberately or accidentally damaged, or stolen, or fabricated. Keeping the two records in correspondence with each other can be made more or less difficult depending on the technologies used for the records and the procedures used to handle the records.

It is important to structure the records so that errors and other anomalies can be readily detected during audits. There are a number of techniques that can be used:

- Associating unique identifiers with corresponding records, e.g., an individual paper record sharing a unique identifier with its corresponding electronic record
- Including an identification of the specific voting system that produced the records, such as a serial number identifier, or by having the voting system digitally sign the records
- Including other information about the election and the precinct or location where the records were created
- Creating checksums of the electronic records and having the voting system digitally sign the entire sets of records so that missing or inserted records can be detected
- Structuring the records in open, publicly documented formats that can be readily analyzed on different computing platforms

The ease with which records can be handled is a factor in the practical capability to conduct precise audits, given that some types of records are better suited to auditing and different voting environments than others. The factors that make certain types of records more suitable than others could vary greatly depending upon many other criteria, both objective and subjective. For example, paper records may require manual handling by poll workers and thus be more susceptible to accidental or deliberate damage, loss, and theft. At the same time, the extent to which the paper records must be handled will vary depending on the type of voting system in use. Electronic records may by their nature be more suitable for automated audits; however electronic records are still subject to accidental or deliberate damage, loss, and theft.

C.2 Core Characteristics for Independent Verification Systems

This section contains a preliminary set of characteristics for IV systems. These characteristics are fundamental in nature and apply to all categories of IV systems. They will form the basis for future requirements for independent verification systems.

- A voting machine equipped with independent verification produces two independent records of ballot selections via interactions with the voter such that one record can be compared against the other to check their equality of content.

Discussion: This is the fundamental characteristic of IV systems. The records can be checked against one another to determine whether or not the voter's selections were correctly recorded.

- The voter verifies the content of each record and either (a) verifies at least one of the records directly or (b) verifies both records indirectly if the records are each under the control of independent processes.
- The creation, storage, and handling of the records are sufficiently separate such that the failure or compromise of one record does not cause the failure or compromise of another.

Discussion: The records must be stored on different media and handled independently of each other, so that no one process could compromise all records. If an attack can alter one record, it should still be very difficult to alter the other record.

—Both records are highly resistant to damage or alteration and should be capable of long-term storage.

- The records are linked to their corresponding records by including a unique identifier within each record that can be used to identify the corresponding record.
- The processes of verification for the multiple records do not all depend for their integrity on the same device or software module, and are sufficiently separate such that each record provides evidence of the voter's selections independently of the corresponding record.
- The records can be used in checks of one another, such that if one set of records can be used in an efficient counting process, the other set of records can be used for checking its agreement with the first set of records.

Discussion: For example, an electronic record can be used in an efficient counting process. A paper record can be used to verify the accuracy of the electronic record. However, it is less suitable for efficient counting unless it can be corrected by an automated scan process.

- Each record includes an identification of the polling place and precinct.

Discussion: If the voting site and precinct are different, both should be included.

- The records include information identifying whether the balloting is provisional, early, or on election day, and information that identifies the ballot style in use.
- The records include a voting session identifier that is generated when the voting station is placed in voting mode and that can be used to identify the records as being created during that voting session.

Discussion: If there are several voting sessions on the same voting station on the same day, the voting session identifiers must be different. They should be generated from a random number generator.

- The records include a unique identifier associated with the voting station

Discussion: The identifier could be a serial number or other unique ID.

- The cryptographic software in voting systems with independent verification is approved by the U.S. Government's Cryptographic Module Validation Program (CMVP) as applicable.

Discussion: Cryptographic software may be used for a number of different purposes, including calculating checksums, encrypting records, authentication, generating random numbers, and for digital signatures. This software should be reviewed and approved by the Cryptographic Module Validation Program. There may be cryptographic voting schemes where the cryptographic algorithms used are necessarily different from any algorithms that have approved CMVP implementations, thus CMVP approved software shall be used where feasible. The CMVP web site is *http://csrc.nist.gov/cryptval.*

C.3 Split Process Independent Verification Systems

This section contains characteristics specific to split process IV systems. The characteristics build on and are in addition to the core characteristics for IV systems. Split process systems consist of separate vote capture and verification stations, i.e., two physical devices. A voter inserts an object called a token into the capture station to make ballot selections and then takes the token object to the verification station to review and store his or her votes. Two records of the vote are created: one on the token object and one by the verification station.

C.3.1 Capture and Verification Stations

- The verification station is able to add information to the token object but cannot change prior recorded information.
- The capture and verification stations do not permit any communications between them except via the token object.
- The verification station shall log all rejected votes, including the precise contents of the votes and the identifier of the token object.

Discussion: The voter could reject and thereby void his or her ballot. This is to prevent the verification station from recording ballot selections that are different from what was entered at the capture station.

- The capture and verification stations could be purchased from different manufacturers and could use different operating systems.

Discussion: The greater the independence of the capture and verification stations, the less likely they could be compromised by the same threats, e.g., software viruses, or by a single conspiracy.

C.3.2 Data Formats for Token Objects

- The format for data written to the token object is specified and publicly available for use without licensing fees.
- The verification station verifies the correctness of the data on the token object and provides an indication of any errors to the voter.

Discussion: The verification station needs to verify that the data written to the token object was formatted properly according to the format specification and reject improperly formatted data. It also checks that the votes are consistent with the voting instructions, e.g., ''vote for one, vote for two.''

- The record on the token object is digitally signed using a private key known only to the vote capture station and whose public key is distributed in an authenticated way to auditing systems and the verification station.
- The record created by the verification station is digitally signed using a private key known only to the verification station and whose public key is distributed in an authenticated way to auditing systems.
- The capture station associates a unique identifier with each record of

voter selections to identify that record and link it to the corresponding record created by the verification station.

Discussion: The identifier serves the purpose of uniquely identifying the record to identify duplicates and/or for cross-checking two record types.

- The records from the verification station are randomly shuffled in memory when exported, so that the order of the records cannot be used to relate the votes to a specific voter.
- Rejected token objects are stored separately from accepted token objects for later auditing.

C.3.3 Storage and Communications of Records

- The verification station exports its records of voter choices accompanied by a digital signature on the entire set of electronic records and their associated digital signatures.

Discussion: This is necessary to determine if records are missing or substituted.

- The token objects are stored and transported in a physically secure way, using chain-of-custody mechanisms to ensure their integrity.
- The records from each station are randomly shuffled, so that an attacker learning the contents of those records at any point in the voting process can learn nothing about the order of votes cast.

C.4 Witness IV Systems

Witness IV systems are composed of two physically separate devices: the vote capture station that captures and stores records of voter selections, and the witness device that captures voter verifications of the records at the vote capture station. Because there are two devices, a number of the definitions for split verification systems apply equally well to witness systems. Because the vote capture station is in essence a DRE, a number of the definitions for DREs with VVPAT also apply to vote capture stations. A witness system fits somewhat loosely in the independent verification category because the voter performs only an indirect verification of ballot choices at the DRE. It is important that the witness device be tested extensively for accuracy and reliability and that malfunctions of the device be made immediately obvious to the voter and poll workers.

- A witness device records only a voter's verification at the vote capture station and stores the record so that it can be used for audit.
- A witness device acts as a passive device that cannot perform any operation with respect to the voting station other than to capture voter ballot selections as the voter verifies them.

Discussion: The witness device is synchronized with the voter verification of the ballot selections.

- A witness device, if attached to the vote capture station, is attached such that it can capture only the voter's verification of ballot selections.

Discussion: For example, the witness device could be connected only to the display unit and not the vote capture station's memory or disk drive.

- The vote capture station is able to detect whether the witness device is connected or in operation.

Discussion: If the witness device is not in operation, the vote capture station should cease recording voter selections.

- The vote capture station and the witness device are connected using a publicly available, published communications interface, such as RS232 or USB.
- Because voters must trust that the witness device records their verifications accurately, assessments of its software and functionality are straightforward, readily performed, and include extensive evaluation and penetration testing above and beyond what may be performed on voting systems that do not contain witness devices.

Discussion: Witness device manufacturers will be required to fully document their systems and conduct stringent testing.

- A voter should be able to inspect the record of his or her verification upon request.

Discussion: It is desirable that a voter have the ability to verify that the witness device is operating as specified.

- The witness device clearly indicates any malfunction in a way that is obvious to the voter and poll workers.
- The records captured by the witness device are able to be used in highly accurate verifications of the voting records of the voting station.
- The records contain unique identifiers that correspond to records stored by the vote capture station.
- The records are digitally signed by the witness device so that the integrity and authenticity of its records can be verified.
- A witness device is able to export its records in an open, nonproprietary format such that the records can be used in automated audits.
- The records are stored in the witness device and exported such that voter privacy is protected, e.g., by randomizing the order of the records.

C.5 End to End Cryptographic IV Systems

This section contains very preliminary definitions for end to end cryptographic-based IV systems. They are consistent with the characteristics of IV systems and build on the core characteristics of IV systems.

End to end voting systems use cryptographic mechanisms as a substitute for some physical, computer-security, or procedural mechanisms used to secure other types of voting systems. These cryptographic mechanisms can be used by a voter to verify that ballot selections were recorded correctly and counted in the election. Some auditing procedures normally performed by voting officials at the tabulation center can be done by voters or their designated representatives, using receipts issued by the voting system that work in conjunction with the cryptographic mechanisms. Typically, multiple individuals, known as designated trustees, hold key information that is combined to form encryption and decryption keys; thus, no one person is able to encrypt or decrypt. Several types of cryptographic voting approaches have been proposed or implemented, with varying properties. There are many cryptographic techniques (such as secure multiparty computation and homomorphic) that could be applied in novel ways in future voting systems.

- End to end systems record voters ballot selections at electronic voting machines and encrypt the records of votes for later counting by designated trustees.

Discussion: The voting station would operate much as a DRE.

- End to end systems produce a receipt that can be used by the voter in a process defined by voting officials that would enable the voter to verify that the voter's ballot selections were recorded correctly and counted in the election.

Discussion: The receipt could have a variety of different forms but likely would be printed on paper for the voter's ease of handling.

- No one designated trustee is able to decrypt the records; decryption of the records is performed by a process that involves multiple designated trustees.
- The receipt preserves voter privacy by not containing any information that can be used to show the voter's selections.
- The process used to verify that ballot selections were recorded correctly and counted preserves voter privacy by not revealing any information that can be used to identify the voter's selections.

- End to end systems store backup records of voter ballot selections that can be used in contingencies such as damage or loss of its counted records.

Discussion: This is necessary because the handling of the encrypted records requires the same chain of custody procedures as records produced by other voting systems and are thus subject to loss or damage. This could be paper for example.

- The backup records contain unique identifiers that correspond to unique identifiers in its counted records, and the backup records are digitally signed so that they can be verified for their authenticity and integrity in audits.
- Cryptographic software in end to end systems is documented thoroughly and subject to extensive verification testing for correctness. The documentation includes extensive discussion of how cryptographic keys are to be generated, distributed, managed, used, certified, and destroyed.
- Vote capture stations used in end to end systems must meet all the security, usability, and accessibility requirements.
- Reliability, usability, and accessibility requirements for printers in other voting systems apply as well to receipt printers used in end to end systems.
- Trustee systems are subject to the same evaluations and assessments as other voting systems.
- Systems for verifying that voter ballot selections were recorded properly and counted are implemented in a robust secure manner.

Discussion: Many of the cryptographic approaches have a ‘‘public append-only bulletin board’’ as a component; this is an important part of the system and needs to be implemented in a robust secure manner.

Appendix D: Technical Guidance for Color, Contrast, and Text Size

Table of Contents

Appendix D: Technical Guidance for Color, Contrast, and Text Size

Although estimates vary, it is generally agreed that there are approximately 10 million visually impaired people in the United States. This estimate includes the 600,000 people who are legally blind. 8.1 million people were estimated to have a functional limitation in seeing in 1994, including both those with ‘‘non-severe limitation’’ (e.g., difficulty seeing words and letters) and those with ‘‘severe limitation’’ (e.g., unable to see words and letters). Approximately 1.8 million people in the U.S. have severe visual impairments but are not legally blind.[4] Low vision 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. For the purposes of this discussion low vision is defined as having a visual acuity greater than 20/70.

People with low vision or color blindness will benefit from high contrast and selection of color combinations that are 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.

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’’ which makes these users unable to distinguish individual letters. Contrast ratio between 6:1 and 15:1 is optimal.[5]

When color selection is provided the 16-color pallet as used in Microsoft Windows for 16 color displays and recognized by HTML 4.0 provides a sufficient range of both saturated and non-saturated color options. Use of non-saturated color options is an advantage for some people. The use of the 16-color palette or a larger color palette is suggested when voter adjustment of color is provided.

Number	Color name (Color names are per HTML 4.0)	RGB value (Hexadecimal)
1	Black	#000000
2	Blue	#0000FF
3	Lime	#00FF00
4	Red	#FF0000
5	Aqua	#00FFFF
6	Fuchsia	#FF00FF
7	Yellow	#FFFF00
8	White	#FFFFFF
9	Navy	#000080
10	Green	#008000
11	Maroon	#800000
12	Teal	#008080
13	Purple	#800080
14	Olive	#808000
15	Grey	#808080
16	Silver	#C0C0C0

Large fonts provide significant help to users with low or impaired vision. A voting system is required to provide letters of at least 6.3 mm, for capital letters. A capital ‘‘X’’ is often used to make this measurement. It is not the size per se, but visual angle that is of primary importance. Visual angle is a measure, in degrees, of the size of the retinal image subtended by a viewed object. It represents the apparent size of an object based on the relationship between an object’s distance from the viewer and its size (perpendicular to the viewer’s line of sight). An object of constant size will subtend a smaller visual angle as it is moved farther from the viewer. Visual angle is typically defined in terms of minutes of visual arc. For people with normal vision, it is recommended that the height of characters in displayed text or labels be at least 16 minutes of arc (4.6 milliradians), and the preferred character height should be 22 minutes of arc (6.4 milliradians), which is preferred for reading tasks.

[4] See the following sites for futher detail: *http://blue.census.gov/hhes/www/disable, http://www.afb.org/info_document_view.asp?documentid=1367, http://www.brailleinstitute.org.*

[5] Cushman, W.H. and Rosenberg, D.J., *Human Factors in Product Design.* New York: Elsevier, 1991.

The size required for low vision accessibility is somewhat arbitrary, in that the larger the size the greater the number of low vision voters who can be accommodated. The Usability/Accessibility Task Group for IEEE P1583 recommends 30 minutes of arc, depending upon the presumed viewing distance. A table in the usability section of IEEE P1583 provides the following recommendations based on three possible viewing distances:

- For a distance of 51cm (20in): 4.43mm (.17in).
- For a distance of 64cm (25in): 5.54mm (.22in).
- for a distance of 76cm (30in): 6.65mm (.26in).

People with tunnel vision can only see 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 recommended range.

Use of sans serif fonts is also recommended for computer displays. Sans serif fonts have proven to be easier to read on computer screens than stylized fonts.

Voluntary Voting System Guidelines

Volume II

National Certification Testing Guidelines

Voluntary Voting System Guidelines

Table of Contents

Volume I Voting System Performance Guidelines

Volume II National Certification Testing Guidelines

Voluntary Voting System Guidelines Overview

Table of Contents

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 nondiscretionary 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.

As required by HAVA, the EAC formed the Technical Guidelines Development Committee (TGDC) to develop an initial set of recommendations for the Guidelines. This committee of 15 experts began their work in July 2004 and submitted their recommendations to the EAC in the 9-month timeline prescribed by HAVA. The TGDC was provided with technical support by the National Institute for Standards and Technology (NIST), which was given nearly $3 million dollars by the EAC to complete this work.

The EAC reviewed and revised the TGDC recommendations and, as required by HAVA, published the proposed Guidelines for a 90 day public comment period. The document was also provided to both the Board of Advisors and the Standards Board for their review and comment. During the comment period the EAC conducted 3 public hearings on the Guidelines in New York City, Pasadena and Denver. Over 6000 comments were received from the public and the Boards. Each of these comments was reviewed and considered by the EAC in consultation with NIST in the development of this final version.

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 2005 Voluntary Voting System Guidelines will take effect 24 months after their final adoption in December 2005 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 2005 VVSG. All previous versions of national standards will become obsolete at this time. This effective date provision does not have any impact on the mandatory January 1, 2006, deadline for states to comply with the HAVA Section 301 requirements.

Summary of Changes

Volume I of the Guidelines, entitled Voting System Performance Guidelines, includes new requirements for usability, accessibility, voting system software distribution, generation of software reference information, validation of software during voting system setup, and the use of wireless communications. System functional requirements have been revised to comply with HAVA Section 301 requirements. Environmental criteria have been updated. This volume also includes requirements for a voter verifiable paper audit trail component for direct-recording electronic voting systems for use by states that require this feature. In addition, this volume includes an updated glossary and a conformance clause.

Volume II of the Guidelines, entitled National Certification Testing Guidelines, has been revised to reflect the new EAC process for national certification of voting systems. This process was initiated in 2005 and replaces the voting system qualification process conducted by the National Association of State Election Directors (NASED) since 1994. In addition, revisions have been made to the testing procedures to reflect new requirements for the conduct of usability and accessibility testing. Volume II also includes an updated appendix on procedures for testing system error rates. Terminology in both volumes has been revised to reflect new terminology introduced by HAVA.

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; 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.

Sections 8 and 9 describe requirements for vendor 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.

Appendix C presents an introductory discussion of independent verification systems as a potential concept for future voting system security design.

Appendix D contains technical guidance on color, contrast and text size adjustment for individuals with low vision or color blindness.

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 accredited by the EAC. It is intended principally for use by vendors: test labs: and election officials who certify, procure, and accept voting systems. This volume contains the following sections:

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

Section 2 provides a description of the Technical Data Package that vendors 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 vendor quality assurance and configuration management practices.

Appendix A provides the requirements for the National Certification Test Plan that is prepared by the voting system test lab 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 test lab and delivered to the EAC along with a recommendation for certification.

Appendix C describes the guiding principles used to design the voting system certification testing process. It also contains a revised section on testing system error rates.

National Certification Testing Guidelines

Guide to Section Locations

Introduction

Table of Contents

Introduction

1.1 Overview of the National Certification Testing Guidelines

Volume II, National Certification Testing Guidelines, is a complementary document to Volume I, Voting System Performance Guidelines. Volume I specifies the requirements that a voting system must conform to in order to be nationally certified as acceptable for use in federal elections. Volume II describes the testing process that is designed to provide a documented independent verification by an accredited voting system test lab that a voting system has been demonstrated to conform to the Volume I requirements and therefore should receive national certification.

Volume II, National Certification Testing Guidelines, provides the specific detail about the testing process that is needed for the accredited test labs, voting system vendors and election officials participating in the system certification process.

Independent Accredited Test Labs: Test labs that are accredited to perform conformance testing of voting systems will use Volume II to guide the development of test plans, the testing of systems, and the preparation of test reports and recommendations for granting national certification. Organizations wishing to become accredited as voting system test labs can refer to Volume II to understand the requirements and obligations placed on an accredited voting system test lab.

Voting System Vendors: Voting system vendors will use Volume II to guide the design, construction, documentation, internal testing, and maintenance of voting systems. They will also use this document to help define the responsibilities of organizations that support the system, such as suppliers, testers and consultants.

Election Officials: Election officials will use Volume II to guide their state certification, procurement, and acceptance processes and requirements. Certification at the state level may entail system conformance with additional requirements beyond those required for national certification to comply with state election laws or procedures.

1.2 Overview of the National Certification Testing Process

Certification testing encompasses the examination and testing of software; tests of hardware under conditions simulating the intended storage, operation, transportation, and maintenance environments; the inspection and evaluation of system documentation; and operational tests to validate system performance and functioning under normal and abnormal conditions. The testing also evaluates the completeness of the vendor's developmental test program, including the sufficiency of vendor tests conducted to demonstrate compliance with stated system design and performance specifications, and the vendor's documented quality assurance and configuration management practices. The tests address individual system components or elements, as well as the integrated system as a whole.

Beginning in 1994, the National Association of State Election Directors (NASED) began accrediting Independent Test Authorities for the purpose of conducting qualification testing of voting systems. The qualification testing process was originally based on the 1990 voting system standards and evolved to encompass the new requirements contained in the 2002 version of the standards.

The Help America Vote Act (HAVA) directs the U.S. Election Assistance Commission (EAC) to provide for the testing, certification, decertification, and recertification of voting system hardware and software by accredited laboratories. HAVA also introduces different terminology for these functions. Under the EAC process, test labs are ''accredited'' and voting systems are ''certified.'' The term ''standards'' has been replaced with the term ''Guidelines.'' As prescribed by HAVA, the EAC process was initially based on the 2002 Voting Systems Standards and will transition to the revised standards issued through the 2005 Voluntary Voting System Guidelines.

1.3 Testing Scope

The national certification testing process is intended to discover vulnerabilities that, should they appear in actual election use, could result in failure to complete election operations in a satisfactory manner. There are four focuses that guide the overall process:

- Operational accuracy in the recording and processing of voting data, as measured by target error rate, for which the maximum acceptable error rate is no more than one in ten million ballot positions, with a maximum acceptable error rate in the test process of one in 500,000 ballot positions
- Operational failures or the number of unrecoverable failures under conditions simulating the intended storage, operation, transportation, and maintenance environments for voting systems, using an actual time-based period of processing test ballots
- System performance and function under normal and abnormal conditions
- Completeness and accuracy of the system documentation and configuration management records to enable purchasing jurisdictions to effectively install, test, and operate the system 1.3.1 Test Categories The certification test procedure is presented in several parts:
- Functionality testing
- Hardware testing
- Software evaluation
- System level integration tests, including audits
- Examination of documented vendor practices for quality assurance and for configuration management

In practice, there may be concurrent indications of hardware and software function, or failure to function, during certain examinations and tests. Operating tests of hardware partially exercise the software as well and therefore supplement software testing. Security tests exercise hardware, software and communications capabilities. Documentation review conducted during software qualification supplements the review undertaken for system-level testing.

Not all systems being tested are required to complete all categories of testing. For example, if a previously certified system has had hardware modifications, the system may be subject only to non-operating environmental stress testing of the modified component and system level integration testing. If a system consisting of general purpose COTS hardware, or one that was previously certified has had modifications to its software, the system is subject only to software testing and system level integration tests, not hardware testing. However, in all cases the system documentation and configuration management records will be examined to confirm that they completely and accurately reflect the components and component versions that comprise the voting system.

1.3.1.1 Focus of Functionality Tests

Functionality testing is performed to confirm the functional capabilities of a voting system. The accredited test lab designs and performs procedures to test a voting system against the requirements outlined in Volume I, Section 2. In order to best complement the diversity of the voting systems industry, this part of the testing process is not rigidly defined. Although there are basic functionality testing requirements, additions or variations in testing are appropriate depending on the system's use of specific technologies and configurations, the system capabilities, and the outcomes of previous testing.

1.3.1.2 Focus of Hardware Tests

Hardware testing begins with non-operating tests that require the use of an environmental test facility. These are followed by operating tests that are performed partly in an environmental facility and partly in a standard accredited test laboratory or shop environment.

The non-operating tests are intended to evaluate the ability of the system hardware to withstand exposure to the various environmental conditions incidental to voting system storage, maintenance, and transportation. The procedures are based on test methods contained in Military Standards (MIL-STD) 810F, modified where appropriate, and include such tests as: bench handling, vibration, low and high temperature, and humidity.

The operating tests involve running the system for an extended period of time under varying temperatures and voltages. This period of operation ensures with confidence that the hardware meets or exceeds the minimum requirements for reliability, data reading, and processing accuracy contained in Volume I, Section 4. The procedure emphasizes equipment operability and data accuracy; it is not an exhaustive evaluation of all system functions. Moreover, the severity of the test conditions, in most cases, has been reduced from that specified in the Military Standards to reflect commercial and industrial practice.

1.3.1.3 Focus of Software Evaluation

The software tests encompass a number of interrelated examinations, involving assessment of application source code for its compliance with the requirements spelled out in Volume I, Section 5. Essentially, the accredited test lab will look at programming completeness, consistency, correctness, modifiability, structure, and traceability, along with its modularity and construction. The code inspection will be followed by a series of functional tests to verify the proper performance of all system functions controlled by the software.

The accredited test lab may inspect COTS generated software source code in the preparation of test plans and conduct some minimal scanning or sampling to check for embedded code or unauthorized changes. Otherwise, the COTS source code is not subject to the full code review and testing. For purposes of code analysis, the COTS units shall be treated as unexpanded macros.

1.3.1.4 Focus of System Integration Tests

The functionality, hardware, and software certification tests supplement a fuller evaluation performed by the system level integration tests. System level tests focus on these aspects jointly, throughout the full range of system operations. They include tests of fully integrated system components, internal and external system interfaces, usability and accessibility, and security. During this process election management functions, ballot-counting logic, and system capacity are exercised. The process also includes the Physical Configuration Audit (PCA) and the Functional Configuration Audit (FCA).

The accredited test lab tests the interface of all system modules and subsystems with each other against the vendor's specifications. Some systems use telecommunications capabilities as defined in Volume 1, Section 6. For those systems that do use such capabilities, components that are located at the poll site or separate vote counting site are tested for effective interface, accurate vote transmission, failure detection, and failure recovery. For voting systems that use telecommunications lines or networks that are not under the control of the vendor (e.g., public telephone networks), the accredited test lab tests the interface of vendor-supplied components with these external components for effective interface, vote transmission, failure detection, and failure recovery.

The security tests focus on the ability of the system to detect, prevent, log, and recover from a broad range of security risks as identified in Volume 1, Section 7. The range of risks tested is determined by the design of the system and potential exposure to risk. Regardless of system design and risk profile, all systems are tested for effective access control and physical data security. For systems that use public telecommunications networks, to transmit election management data or official election results (such as ballots or tabulated results), security tests are conducted to ensure that the system provides the necessary identity-proofing, confidentiality, and integrity of transmitted data. The tests determine if the system is capable of detecting, logging, preventing, and recovering from types of attacks known at the time the system is submitted for qualification. The accredited test lab may meet these testing requirements by confirming the proper implementation of proven commercial security software.

The interface between the voting system and its users, both voters and election officials, is a key element of effective system operation and confidence in the system. Guidelines for usability by individual voters with disabilities have been defined in Volume 1, Section 3. Voting systems are tested to ensure that an accessible voting station is included in the system configuration and that its design and operation conforms to these guidelines.

The Physical Configuration Audit (PCA) compares the voting system components submitted for qualification to the vendor's technical documentation and confirms that the documentation submitted meets the requirements of the Guidelines. As part of the PCA, the accredited test lab also witnesses the build of the executable system to ensure that the qualified executable release is built from the tested components.

The Functional Configuration Audit (FCA) is an exhaustive verification of every system function and combination of functions cited in the vendor's documentation. Through use, the FCA verifies the accuracy and completeness of the system Technical Data Package (TDP). The various options of software counting logic that are claimed in the vendor's documentation shall be tested during the system-level FCA. Generic test ballots or test entry data for DRE systems, representing particular sequences of ballot-counting events, will test the counting logic during this audit.

1.3.1.5 Focus of Vendor Documentation Examination

The accredited test lab reviews the documentation submitted by the vendor for its completeness and accuracy in describing the system. The accredited test lab also reviews the documentation to evaluate the extent to which it conforms to the requirements outlined in Volume 1, Sections 8 and 9 for vendor configuration and quality assurance practices. The accredited test lab examines the conformance of other documentation and information provided by the vendor with the vendor's documented practices for quality assurance and configuration management.

The Guidelines do not require on-site examination of the vendor's quality assurance and configuration management practices during the system development process. However, the accredited test lab conducts several activities while at the vendor site to witness the system build that enable assessment of the vendor's quality assurance and configuration management practices and conformance with them. These include surveys, interviews with individuals at all levels of the development team, and examination of selected internal work products such as system change requests and problem tracking logs.

1.4 Testing Sequence

The overall testing process progresses through several stages involving pre-testing, testing, and post-testing activities. National certification testing involves a series of physical tests and other examinations that are conducted in a particular sequence. The sequence is intended to maximize overall testing effectiveness, as well as conduct testing in as efficient a manner as possible. The accredited test lab will follow the general sequence outlined below. Test anomalies and errors are communicated to the system vendor throughout the process.

a. Initial examination of the system and the technical documentation provided by the vendor to ensure that all components and documentation needed to conduct testing have been submitted, and to help determine the scope and level of effort of testing needed

b. Examination of the vendor's Quality Assurance Program and Configuration Management Plan

c. Development of a detailed system test plan that reflects the scope and complexity of the system, and the status of system certification (i.e., initial certification or a re-certification to incorporate modifications)

d. Code review for selected software components

e. Witnessing of a system 'build' conducted by the vendor to conclusively establish the system version and components being tested

f. Operational testing of hardware components, including environmental tests, to ensure that operational performance requirements are achieved

g. Functional and performance testing of hardware components

h. System installation testing and testing of related documentation for system installation and diagnostic testing i. Functional and performance testing of software components

j. Functional and performance testing of the integrated system, including testing of the full scope of system functionality, performance tests for telecommunications and security; and examination and testing of the System Operations Manual

k. Examination of the system maintenance manual

l. Preparation of the National Certification Test Report

m. Delivery of the National Certification Test Report to the EAC 1.5

Documentation Submitted by Vendor

The vendor shall submit all the documentation necessary for the identification of the full system configuration submitted for evaluation and for the development of an appropriate test plan by the accredited test lab for conducting system certification testing. This documentation collectively is referred to as the Technical Data Package (TDP). The TDP provides information that defines the voting system design, method of operation, and related resources. It provides a system overview and documents the system's functionality, hardware, software, security, test and verification specifications, operations procedures, maintenance procedures, and personnel deployment and training requirements. It also documents the vendor's configuration management plan and quality assurance program. If another version of the system was previously certified, the TDP would also include appropriate system change notes.

1.6 Voting Equipment Submitted by Vendor

Vendors may seek to market a complete voting system or an interoperable component of a voting system. In all instances, vendors shall submit for testing the specific system configuration that will be offered to jurisdictions or that comprises the component to be marketed plus the other components with which the vendor recommends that the component be used. The system submitted for testing shall meet the following requirements:

a. The hardware submitted for certification testing shall be equivalent, in form and function, to the actual production version of the hardware units or the COTS hardware specified for use in the TDP

b. The software submitted for certification testing shall be the exact software that will be used in production units

c. Engineering or developmental prototypes are not acceptable, unless the vendor can show that the equipment to be tested is equivalent to standard production units both in performance and construction

d. Benchmark directory listings shall be submitted for all software/firmware elements (and associated documentation) included in the vendor's release as they would normally be installed upon setup and installation

1.7 Test Applicability

Certification tests are conducted for new systems seeking initial certification as well as for modified versions of systems that have been certified.

1.7.1 General Applicability

Voting system hardware, software, communications and documentation are examined and tested to determine suitability for elections use. Examination and testing addresses the broad range of system functionality and components, including system functionality for pre-voting, voting, and post-voting functions. All products custom designed for election use shall be tested in accordance with the applicable procedures contained in this section. COTS hardware, system software and communications components with proven performance in commercial applications other than elections, however, are exempted from certain portions of the test as long as such products are not modified for use in a voting system. Compatibility of these products with other components of the voting system shall be determined through functional tests integrating these products with the remainder of the system.

1.7.1.1 Hardware

Specifically, the hardware test requirements shall apply in full to all equipment used in a voting system with the exception of the following:

a. Commercially available models of general purpose information technology equipment that have been designed to an ANSI or IEEE standard, have a documented history of successful performance for relevant requirements of the standards, and have demonstrated compatibility with the voting system components with which they interface

b. Production models of special purpose information technology equipment that have a documented history of successful performance under conditions equivalent to election use for relevant requirements of the standards and that have demonstrated compatibility with the voting system components with which they interface

c. Any ancillary devices that do not perform ballot definition, election database maintenance, ballot reading, ballot data processing, or the production of an official output report; and that do not interact with these system functions (e.g. modems used to broadcast results to the press, printers used to generate unofficial reports, or CRTs used to monitor the vote counting process)

This equipment shall be subject to functional and operating tests performed during software evaluation and system level testing. However, it need not undergo hardware non-operating tests. If the system is composed entirely of off-the-shelf hardware, then the system also shall not be subject to the 48-hour environmental chamber segment of the hardware operating tests.

1.7.1.2 Software

Software certification is applicable to the following:

a. Application programs that control and carry out ballot processing, commencing with the definition of a ballot, and including processing of the ballot image (either from physical ballots or electronically activated images), and ending with the system's access to memory for the generation of output reports

b. Specialized compilers and specialized operating systems associated with ballot processing

c. Standard compilers and operating systems that have been modified for use in the vote counting process

Specialized software for ballot preparation, election programming, vote recording, vote tabulation, vote consolidation and reporting, and audit trail production shall be subjected to code inspection. Functional testing of all these programs during software evaluation and system-level testing shall exercise any specially tailored software off-line from the ballot counting process (e.g. software for preparing ballots and broadcasting results).

1.7.2 Modifications to Certified Systems

Changes introduced after the system has completed certified testing will necessitate further review.

1.7.2.1 General Requirements for Modifications

The accredited test lab will determine tests necessary to certify the modified system based on a review of the nature and scope of changes, and other submitted information including the system documentation, vendor test documentation, configuration management records, and quality assurance information. Based on this review, the accredited test lab may:

a. Determine that a review of all change documentation against the baseline materials is sufficient for recommendation for certification

b. Determine that all changes must be retested against the previously certified version. This will include review of changes to source code, review of all updates to the TDP, and performance of system level and functional tests

c. Determine that the scope of the changes is substantial and will require a complete retest of the hardware, software, and/or telecommunications

1.7.2.2 Basis for Limited Testing Determinations

The accredited test lab may determine that a modified system will be subject only to limited certification testing if the vendor demonstrates that the change does not affect demonstrated compliance with these Guidelines for:

a. Performance of voting system functions

b. Voting system security and privacy

c. Overall flow of system control

d. The manner in which ballots are defined and interpreted, or voting data are processed

Limited testing is intended to facilitate the correction of defects, the incorporation of improvements, the enhancement of portability and flexibility, and the integration of vote-counting software with other systems and election software.

1.8 Certification Test Process

The certification test process may be performed by one or more accredited test labs that together perform the full scope of tests required. Where multiple accredited test labs are involved, testing shall be conducted first for the voting system hardware, firmware, and related documentation; then for the system software and communications; and finally for the integrated system as a whole. Voting system hardware and firmware testing may be performed by one accredited test lab independently of the other testing performed by other accredited test labs. Testing may be coordinated across accredited test labs so that hardware/firmware tested by one accredited test lab can be used in the overall system tests performed by another accredited test lab.

When multiple accredited test labs are being used, the development of the National Certification Test Plan (see Appendix A) and the National Certification Test Report (see Appendix B) shall be coordinated by a lead accredited test lab. The lead lab is responsible for ensuring that all testing has been performed and documented in accordance with the Guidelines.

Whether one or more accredited test labs are used, the testing generally consists of three phases:

- Pre-test Activities
- National Certification Testing
- National Certification Report Issuance and Post-test Activities

1.8.1 Pre-test Activities

Pre-test activities include the request for initiation of testing and the pre-test preparation.

1.8.1.1 Initiation of Testing

Certification testing shall be conducted at the request of the vendor, consistent with the provision of the Guidelines. The vendor shall:

a. Request the performance of certification testing from among the accredited testing laboratories

b. Enter into formal agreement with the accredited test lab for the performance of testing

c. Prepare and submit materials required for testing consistent with the requirements of the Guidelines

Certification testing shall be conducted for the initial version of a voting system as well as for all subsequent changes to the system prior to release for sale or for installation. As described in Subsection 1.6.2, the nature and scope of testing for system changes or new versions shall be determined by the accredited test lab based on the nature and scope of the modifications to the system and on the quality of system documentation and configuration management records submitted by the vendor.

1.8.1.2 Pre-test Preparation

Pre-test preparation encompasses the following activities:

a. The vendor shall prepare and submit a complete TDP to the accredited test lab. The TDP should consist of the materials described in Section 2

b. The accredited test lab shall perform an initial review of the TDP for completeness and clarity and request additional information as required

c. The vendor shall provide additional information, if requested by the accredited test lab

d. The vendor and accredited test lab shall enter into an agreement for the testing to be performed by the accredited test lab in exchange for payment by the vendor

e. The vendor shall deliver to the accredited test lab all hardware and software needed to perform testing

1.8.2 Certification Testing

Certification testing encompasses the preparation of a test plan, the establishment of the appropriate test conditions, the use of appropriate test fixtures, the witness of the system build and installation, the maintenance of certification test data, and the evaluation of the data resulting from tests and examinations.

1.8.2.1 National Certification Test Plan

The accredited test lab shall prepare a National Certification Test Plan to define all tests and procedures required to demonstrate compliance with the Guidelines, including:

Verifying or checking equipment operational status by means of manufacturer operating procedures

a. Establishing the test environment or the special environment required to perform the test

b. Initiating and completing operating modes or conditions necessary to evaluate the specific performance characteristic under test

c. Measuring and recording the value or range of values for the characteristic to be tested, demonstrating expected performance levels

d. Verifying, as above, that the equipment is still in normal condition and status after all required measurements have been obtained

e. Confirming that documentation submitted by the vendor corresponds to the actual configuration and operation of the system

f. Confirming that documented vendor practices for quality assurance and configuration management comply with the Guidelines

A recommended outline for the test plan and the details of required testing are contained in Appendix A.

1.8.2.2 Certification Test Conditions

The accredited test lab may perform the tests in any facility capable of supporting the test environment. The following practices shall be employed:

a. Preparations for testing, arrangement of equipment, verification of equipment status, and the execution of procedures shall be witnessed by at least one independent, qualified observer in the form of an accredited testing laboratory, which shall certify that all test and data acquisition requirements have been satisfied

b. When a test is to be performed at ''standard'' or ''ambient'' conditions, this requirement shall refer to a nominal laboratory or office environment, with a temperature in the range of 68 to 75 degrees Fahrenheit, and prevailing atmospheric pressure and relative humidity

c. Otherwise, all tests shall be performed at the required temperature and electrical supply voltage, regulated within the following tolerances:

i. Temperature—±4 degrees F

ii. Electrical supply voltage—±2 voltage alternating current

1.8.2.3 Certification Test Fixtures

The accredited test lab may use test fixtures or ancillary devices to facilitate testing. These fixtures and devices may include arrangements for automating the operation of voting devices and the acquisition of test data:

a. For systems that use a light source as a means of detecting voter selections, the generation of a suitable optical signal by an external device is acceptable. For systems that rely on the physical activation of a switch, a mechanical fixture with suitable motion generators is acceptable

b. The accredited test lab may use a simulation device, and appropriate software, to speed up the process of testing and eliminate human error in casting test ballots, provided that the simulation covers all voting data detection and control paths that are used in casting an actual ballot. In the event that only partial simulation is achieved, then an independent method and test procedure shall be used to validate the proper operation of those portions of the system not tested by the simulator

c. If the vendor provides a means of simulating the casting of ballots, the simulation device is subject to the same performance, reliability, and quality requirements that apply to the voting device itself

1.8.2.4 Witness of System Build and Installation

Although most testing is conducted at facilities operated by the accredited test lab, a key element of voting system testing shall be conducted at either the vendor site or the accredited test lab site. The accredited test lab responsible for testing voting system software, telecommunications, and integrated system operation (i.e., system level testing) shall witness the final system build, encompassing hardware, software and communications, and the version of associated records and documentation. The system elements witnessed, including their specific versions, shall become the specific system version that is recommended for certification.

1.8.2.5 Certification Test Data Requirements

The following test data practices shall be employed:

a. A test log of the procedure shall be maintained. This log shall identify the system and equipment by model and serial number

b. Test environment conditions shall be noted

c. All operating steps, the identity and quantity of simulated ballots, annotations of output reports, the elapsed time for each procedure step, and observations of equipment performance and, in the case of non-operating hardware tests, the condition of the equipment shall be recorded

1.8.2.6 Certification Test Practices

The accredited test lab shall conduct the examinations and tests defined in the National Certification Test Plan such that all applicable tests identified in Volume II, National Certification Testing Guidelines are executed to determine compliance with the voting system requirements described in Volume I. The accredited testing laboratory shall evaluate data resulting from examinations and tests, employing the following practices:

a. If any malfunction or data error is detected that would be classified as a relevant failure using the criteria in Volume II, National Certification Testing Guidelines, its occurrence, and the duration of operating time preceding it, shall be recorded for inclusion in the analysis of data obtained from the test, and the test shall be interrupted

b. If a malfunction is due to a defect in software, then the test shall be terminated and system returned to the vendor for correction

c. If the malfunction is other than a software defect, and if corrective action is taken to restore the equipment to a fully operational condition within 8 hours, then the test may be resumed at the point of suspension

d. If the test is suspended for an extended period of time, the accredited test lab shall maintain a record of the procedures that have been satisfactorily completed. When testing is resumed at a later date, repetition of the successfully completed procedures may be waived, provided that no design or manufacturing change has been made that would invalidate the earlier test results

e. Any and all failures that occurred as a result of a deficiency shall be classified as purged, and test results shall be evaluated as though the failure or failures had not occurred, if the:

i. Vendor submits a design, manufacturing, or packaging change notice to correct the deficiency, together with test data to verify the adequacy of the change

ii. Examiner of the equipment agrees that the proposed change will correct the deficiency

iii. Vendor certifies that the change will be incorporated into all existing and future production units

f. If corrective action cannot be successfully taken as defined above, then the test shall be terminated, and the equipment shall be rejected

1.8.3 Post-test Activities

Certification report issuance and post-test activities encompass the activities described below.

a. The accredited test lab may issue interim reports to the vendor, informing the vendor of the testing status, findings to date, and other information.

b. The accredited test lab shall prepare a National Certification Test Report that confirms the voting system has passed the required testing. This report shall include the date testing was completed, the specific system version addressed by the report, the version numbers of all system elements separately identified with a version number by the vendor, and the scope of tests conducted. A recommended outline for the test report is contained in Appendix B.

c. Where a system is tested by multiple accredited test labs, the lead accredited test lab shall prepare a consolidated National Certification Test Report.

d. The accredited test lab shall deliver the report to the vendor and to the EAC.

e. Upon review and acceptance of the test report, EAC shall issue a Certification Number for the system to the vendor and to the accredited test lab. The issuance of a Certification Number indicates that the system has been tested by the accredited test lab for compliance with the Guidelines.

f. This number applies to the system as a whole only for the configuration and versions of the system elements tested and identified in the National Certification Test Report. The Certification Number does not apply to individual system components or untested configurations.

g. The EAC Certification Number is intended for use by the states and their jurisdictions to support state and jurisdiction processes concerning voting systems. States and their jurisdictions shall request National Certification Test Reports based on the EAC Certification Number to support their voting system certification and procurement processes.

1.8.4 Resolution of Testing Issues

Prior to the transition of this function to the EAC, the NASED Voting Systems Board (the Board) was responsible for resolving questions about the application of the Guidelines in the testing of voting systems. The EAC will have a process for the accredited test labs, vendors and election officials to request an interpretation of the Guidelines. The interpretation will be publicly documented for reference by interested parties. The EAC will periodically assess the interpretations provided to determine which topics should be reflected in a future version of the Guidelines.

2 Description of the Technical Data Package

Table of Contents

2 Description of the Technical Data Package

2.1 Scope

This subsection contains a description of vendor documentation relating to the voting system that shall be submitted with the system as a precondition of national certification testing. These items are necessary to define the product and its method of operation; to provide technical and test data supporting the vendor's claims of the system's functional capabilities and performance levels; and to document instructions and procedures governing system operation and field maintenance. Any information relevant to the system evaluation shall be submitted to include source code, object code, and sample output report formats.

Both formal documentation and notes of the vendor's system development process shall be submitted for qualification tests. Documentation describing the system development process permits assessment of the vendor's systematic efforts to develop and test the system and correct defects. Inspection of this process also enables the design of a more precise test plan. If the vendor's developmental test data are incomplete, the accredited test lab shall design and conduct the appropriate tests to cover all elements of the system and to ensure conformance with all system requirements.

2.1.1 Content and Format

The content of the Technical Data Package (TDP) is intended to provide clear, complete descriptions of the following information about the system:

Overall system design, including subsystems, modules and the interfaces among them
Specific functional capabilities provided by the system
Performance and design specifications
Design constraints, applicable standards, and compatibility requirements
Personnel, equipment, and facility requirements for system operation, maintenance, and logistical support
Vendor practices for assuring system quality during the system's development and subsequent maintenance
Vendor practices for managing the configuration of the system during development and for modifications to the system throughout its life cycle

The vendor shall provide a list of all documents submitted controlling the design, construction, operation, and maintenance of the system. Documents shall be listed in order of precedence.

2.1.1.1 Required Content for Initial Certification

At minimum, the TDP shall contain the following documentation:

System configuration overview
System functionality description
System hardware specifications
Software design and specifications
System test and verification specifications
System security specifications
User/system operations procedures
System maintenance procedures
Personnel deployment and training requirements
Configuration management plan
Quality assurance program
System change notes

2.1.1.2 Required Content for System Changes and Re-certification

For systems seeking re-certification, vendors shall submit System Change Notes as described in Subsection 2.13, as well as current versions of all documents that have been updated to reflect system changes.

Vendors may also submit other information relevant to the evaluation of the system, such as test documentation, and records of the system's performance history, failure analysis and corrective actions.

2.1.1.3 Format

The requirements for formatting the TDP are general in nature; specific format details are of the vendor's choosing. The TDP shall include a detailed table of contents for the required documents, an abstract of each document and a listing of each of the informational sections and appendices presented. A cross-index shall be provided indicating the portions of the documents that are responsive to documentation requirements for any item presented.

2.1.2 Other Uses for Documentation

Although all of the TDP documentation is required for national certification testing, some of these same items may also be required during the state certification process and local level acceptance testing. Therefore, it is recommended that the technical documentation required for certification and acceptance testing be deposited in escrow.

2.1.3 Protection of Proprietary Information

The vendor shall identify all documents, or portions of documents, containing proprietary information not approved for public release. Any person or accredited test lab receiving proprietary information shall agree to use it solely for the purpose of analyzing and testing the system, and shall agree to refrain from otherwise using the proprietary information or disclosing it to any other person or agency without the prior written consent of the vendor, unless disclosure is legally compelled.

2.2 System Overview

In the system overview, the vendor shall provide information that enables the accredited test lab to identify the functional and physical components of the system, how the components are structured, and the interfaces between them.

2.2.1 System Description

The system description shall include written descriptions, drawings and diagrams that present:

A description of the functional components (or subsystems) as defined by the vendor (e.g., environment, election management and control, vote recording, vote conversion, reporting, and their logical relationships)
A description of the operational environment of the system that provides an overview of the hardware, software, and communications structure
A concept of operations that explains each system function, and how the function is achieved in the design
Descriptions of the functional and physical interfaces between subsystems and components
Identification of all COTS hardware and software products and communications services used in the development and/or operation of the voting system, identifying the name, vendor, and version used for each such component, including:
Operating systems
Database software
Communications routers
Modem drivers
Dial-up networking software
Interfaces among internal components, and interfaces with external systems. For components that interface with other components for which multiple products may be used, the TDP shall provide an identification of:
File specifications, data objects, or other means used for information exchange
The public standard used for such file specifications, data objects, or other means
Benchmark directory listings for all software (including firmware elements) and associated documentation included in the vendor's release in the order in which each piece of software would normally be installed upon system setup and installation

2.2.2 System Performance

The vendor shall provide system performance information including:

The performance characteristics of each operating mode and function in terms of expected and maximum speed, throughput capacity, maximum volume (maximum number of voting positions and maximum number of ballot styles supported), and processing frequency
Quality attributes such as reliability, maintainability, availability, usability, and portability
Provisions for safety, security, privacy, and continuity of operation
Design constraints, applicable standards, and compatibility requirements

2.3 System Functionality Description

The vendor shall declare the scope of the system's functional capabilities, thereby establishing the performance, design, test, manufacture, and acceptance context for the system.

The vendor shall provide a listing of the system's functional processing capabilities, encompassing capabilities required by the Guidelines and any additional capabilities provided by the system. This listing shall provide a simple description of each capability. Detailed specifications shall be provided in other documentation required for the TDP.

The vendor shall organize the presentation of required capabilities in a manner that corresponds to the structure and sequence of functional capabilities indicated in Volume I, Section 2. The contents of Volume I, Section 2 may be used as the basis for a checklist to indicate the specific functions provided and those not provided by the system

Additional capabilities shall be clearly indicated. They may be presented using the same structure as that used for required capabilities (i.e., overall system capabilities, pre-voting functions, voting functions, post-voting functions), or may be presented in another format of the vendor's choosing

Required capabilities that may be bypassed or deactivated during installation or operation by the user shall be clearly indicated

Additional capabilities that function only when activated during installation or operation by the user shall be clearly indicated

Additional capabilities that normally are active but may be bypassed or deactivated during installation or operation by the user shall be clearly indicated

2.4 System Hardware Specification

The vendor shall expand on the system overview by providing detailed specifications of the hardware components of the system, including specifications of hardware used to support the telecommunications capabilities of the system, if applicable.

2.4.1 System Hardware Characteristics

The vendor shall provide a detailed discussion of the characteristics of the system, indicating how the hardware meets individual requirements defined in Volume I, Section 4, including:

Performance characteristics: This discussion addresses basic system performance attributes and operational scenarios that describe the manner in which system functions are invoked, describe environmental capabilities, describe life expectancy, and describe any other essential aspects of system performance

Physical characteristics: This discussion addresses suitability for intended use, requirements for transportation and storage, health and safety criteria, security criteria, and vulnerability to adverse environmental factors

Reliability: This discussion addresses system and component reliability stated in terms of the system's operating functions, and identification of items that require special handling or operation to sustain system reliability

Maintainability: Maintainability represents the ease with which maintenance actions can be performed based on the design characteristics of equipment and software and the processes the vendor and election officials have in place for preventing failures and for reacting to failures. Maintainability includes the ability of equipment and software to self-diagnose problems and make non-technical election workers aware of a problem. Maintainability also addresses a range of scheduled and unscheduled events

Environmental conditions: This discussion addresses the ability of the system to withstand natural environments, and operational constraints in normal and test environments, including all requirements and restrictions regarding electrical service, telecommunications services, environmental protection, and any additional facilities or resources required to install and operate the system

2.4.2 Design and Construction

The vendor shall provide sufficient data, or references to data, to identify unequivocally the details of the system configuration submitted for testing. The vendor shall provide a list of materials and components used in the system and a description of their assembly into major system components and the system as a whole. Paragraphs and diagrams shall be provided that describe:

Materials, processes, and parts used in the system, their assembly, and the configuration control measures to ensure compliance with the system specification

The electromagnetic environment generated by the system

Operator and voter safety considerations, and any constraints on system operations or the use environment

Human factors considerations, including provisions for access by disabled voters

2.5 Software Design and Specification

The vendor shall expand on the system overview by providing detailed specifications of the software components of the system, including software used to support the telecommunications capabilities of the system, if applicable.

2.5.1 Purpose and Scope

The vendor shall describe the function or functions that are performed by the software programs that comprise the system, including software used to support the telecommunications capabilities of the system, if applicable.

2.5.2 Applicable Documents

The vendor shall list all documents controlling the development of the software and its specifications. Documents shall be listed in order of precedence.

2.5.3 Software Overview

The vendor shall provide an overview of the software that includes the following items:

A description of the software system concept, including specific software design objectives, and the logic structure and algorithms used to accomplish these objectives

The general design, operational considerations, and constraints influencing the design of the software

Identification of all software items, indicating items that were:
- Written in-house
- Procured and not modified
- Procured and modified, including descriptions of the modifications to the software and to the default configuration options

Additional information for each item that includes:

Item identification

General description

Software requirements performed by the item
- Identification of interfaces with other items that provide data to, or receive data from, the item
- Concept of execution for the item

The vendor shall also include a certification that procured software items were obtained directly from the manufacturer or a licensed dealer or distributor.

2.5.4 Software Standards and Conventions

The vendor shall provide information that can be used by an accredited test lab or state certification board to support software analysis and test design. The information shall address standards and conventions developed internally by the vendor as well as published industry standards that have been applied by the vendor. The vendor shall provide information that addresses the following standards and conventions:

Software System development methodology

Software design standards, including internal vendor procedures

Software specification standards, including internal vendor procedures

Software coding standards, including internal vendor procedures

Testing and verification standards, including internal vendor procedures, that can assist in determining the program's correctness and ACCEPT/REJECT criteria

Quality assurance standards or other documents that can be used to examine and test the software. These documents include standards for program flow and control charts, program documentation, test planning, and test data acquisition and reporting

2.5.5 Software Operating Environment

This section shall describe or make reference to all operating environment factors that influence the software design.

2.5.5.1 Hardware Environment and Constraints

The vendor shall identify and describe the hardware characteristics that influence the design of the software, such as:

The logic and arithmetic capability of the processor

Memory read-write characteristics

External memory device characteristics

Peripheral device interface hardware

Data input/output device protocols

Operator controls, indicators, and displays

2.5.5.2 Software Environment

The vendor shall identify the compilers or assemblers used in the generation of executable code, and describe the operating system or system monitor.

2.5.6 Software Functional Specification

The vendor shall provide a description of the operating modes of the system and of software capabilities to perform specific functions.

2.5.6.1 Configurations and Operating Modes

The vendor shall describe all software configurations and operating modes of the system, such as ballot preparation, election programming, preparation for opening the polling place, recording votes and/or counting ballots, closing the polling place, and generating reports. For each software function or operating mode, the vendor shall provide:

A definition of the inputs to the function or mode (with characteristics, tolerances or acceptable ranges, as applicable)

An explanation of how the inputs are processed

A definition of the outputs produced (again, with characteristics, tolerances, or acceptable ranges, as applicable)

2.5.6.2 Software Functions

The vendor shall describe the software's capabilities or methods for detecting or handling:

Exception conditions

System failures

Data input/output errors

Error logging for audit record generation

Production of statistical ballot data

Data quality assessment

Security monitoring and control

2.5.7 Programming Specifications

The vendor shall provide in this section an overview of the software design, its structure, and implementation algorithms and detailed specifications for individual software modules.

2.5.7.1 Programming Specifications Overview

This overview shall include such items as flowcharts, data flow diagrams, and other graphical techniques that facilitate understanding of the programming specifications. This section shall be prepared to facilitate understanding of the internal functioning of the individual software modules. Implementation of the functions shall be described in terms of the software architecture, algorithms, and data structures.

2.5.7.2 Programming Specifications Details

The programming specifications shall describe individual software modules and their component units, if applicable. For each module and unit, the vendor shall provide the following information:

Module and unit design decisions, if any, such as algorithms used

Any constraints, limitations, or unusual features in the design of the software module or unit

The programming language used and rationale for its use, if other than the specified module or unit language

If the software module or unit consists of, or contains, procedural commands (such as menu selections in a database management system for defining forms and reports, on-line queries for database access and manipulation, input to a graphical user interface builder for automated code generation, commands to the operating system, or shell scripts), a list of the procedural commands and reference to user manuals or other documents that explain them

If the software module or unit contains, receives, or outputs data, a description of its inputs, outputs, and other data elements as applicable. (Subsection 2.5.9 describes the requirements for documenting system interfaces.) Data local to the software module or unit shall be described separately from data input to, or output from, the software module or unit

If the software module or unit contains logic, the logic to be used by the software unit, including, as applicable:

- Conditions in effect within the software module or unit when its execution is initiated
- Conditions under which control is passed to other software modules or units
- Response and response time to each input, including data conversion, renaming, and data transfer operations
- Sequence of operations and dynamically controlled sequencing during the software module's or unit's operation, including:
- The method for sequence control
- The logic and input conditions of that method, such as timing variations, priority assignments
- Data transfer in and out of memory
- The sensing of discrete input signals, and timing relationships between interrupt operations within the software module or unit

Exception and error handling

If the software module is a database, provide the information described in Subsection 2.5.8

2.5.8 System Database

The vendor shall identify and provide a diagram and narrative description of the system's databases, and any external files used for data input or output. The information provided shall include for each database or external file:

The number of levels of design and the names of those levels (such as conceptual, internal, logical, and physical)
Design conventions and standards (which may be incorporated by reference) needed to understand the design
Identification and description of all database entities and how they are implemented physically (e.g., tables, files)
Entity relationship diagrams and description of relationships
Details of table, record or file contents (as applicable) to include individual data elements and their specifications, including:
- Names/identifiers
- Data type (alphanumeric, integer, etc.)
- Size and format (such as length and punctuation of a character string)
- Units of measurement (such as meters, dollars, nanoseconds)
- Range or enumeration of possible values (such as 0–99)
- Accuracy (how correct) and precision (number of significant digits)
- Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether business rules apply
- Security and privacy constraints
- Sources (setting/sending entities) and recipients (using/receiving entities)

For external files, a description of the procedures for file maintenance, management of access privileges, and security

2.5.9 Interfaces

The vendor shall identify and provide a complete description of all internal and external interfaces, using a combination of text and diagrams.

2.5.9.1 Interface Identification

For each interface identified in the system overview, the vendor shall:
Provide a unique identifier assigned to the interface
Identify the interfacing entities (systems, configuration items, users, etc.) by name, number, version, and documentation references, as applicable
Identify which entities have fixed interface characteristics (and therefore impose interface requirements on interfacing entities) and which are being developed or modified (thus having interface requirements imposed on them)

2.5.9.2 Interface Description

For each interface identified in the system overview, the vendor shall provide information that describes:
The type of interface (such as real-time data transfer, storage-and-retrieval of data) to be implemented
Characteristics of individual data elements that the interfacing entity(ies) will provide, store, send, access, receive, etc., such as:
- Names/identifiers
- Data type (alphanumeric, integer, etc.)
- Size and format (such as length and punctuation of a character string)
- Units of measurement (such as meters, dollars, nanoseconds)
- Range or enumeration of possible values (such as 0–99)
- Accuracy (how correct) and precision (number of significant digits)
- Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether business rules apply
- Security and privacy constraints
- Sources (setting/sending entities) and recipients (using/receiving entities)

Characteristics of communication methods that the interfacing entity(ies) will use for the interface, such as:
- Communication links/bands/frequencies/media and their characteristics
- Message formatting
- Flow control (such as sequence numbering and buffer allocation)
- Data transfer rate, whether periodic/aperiodic, and interval between transfers
- Routing, addressing, and naming conventions
- Transmission services, including priority and grade
- Safety/security/privacy considerations, such as encryption, user authentication, compartmentalization, and auditing

Characteristics of protocols the interfacing entity(ies) will use for the interface, such as:
- Priority/layer of the protocol
- Packeting, including fragmentation and reassembly, routing, and addressing
- Legality checks, error control, and recovery procedures
- Synchronization, including connection establishment, maintenance, termination
- Status, identification, and any other reporting features

Other characteristics, such as physical compatibility of the interfacing entity(ies) (such as dimensions, tolerances, loads, voltages and plug compatibility)

2.5.10 Appendices

The vendor may provide descriptive material and data supplementing the various sections of the body of the Software Specifications. The content and arrangement of appendices shall be at the discretion of the vendor. Topics recommended for amplification or treatment in appendix form include:
Glossary: A listing and brief definition of all software module names and variable names, with reference to their locations in the software structure. Abbreviations, acronyms, and terms should be included, if they are either uncommon in data processing and software development or are used in an unorthodox semantic
References: A list of references to all related vendor documents, data, standards, and technical sources used in software development and testing
Program Analysis: The results of software configuration analysis algorithm analysis and selection, timing studies, and hardware interface studies that are reflected in the final software design and coding

2.6 System Security Specification

Vendors shall submit a system security specification that addresses the security requirements of Volume I, Section 7. This specification shall describe the level of security provided by the system in terms of the specific security risks addressed by the system, the means by which each risk is addressed, the process used to test and verify the effective operation of security capabilities and, for systems that use public telecommunications networks as defined in Volume I, Section 6, the means used to keep the security capabilities of the system current to respond to the evolving threats against these systems.

Information provided by the vendor in this section of the TDP may be duplicative of information required by other sections. Vendors may cross reference to information provided in other sections provided that the means used provides a clear mapping to the requirements of this section.

Information submitted by the vendor shall be used to assist in developing and executing the system certification test plan. The Security Specification shall contain the sections identified below.

2.6.1 Access Control Policy

The vendor shall specify the features and capabilities of the access control policy recommended to purchasing jurisdictions to provide effective voting system security. The access control policy shall address the general features and capabilities and individual access privileges indicated in Volume I, Subsection 7.2.

2.6.2 Access Control Measures

The vendor shall provide a detailed description of all system access control measures and mandatory procedures designed to permit access to system states in accordance with the access policy, and to prevent all other types of access to meet the specific requirements of Volume I, Subsection 7.2.

The vendor also shall define and provide a detailed description of the methods used to preclude unauthorized access to the access control capabilities of the system itself.

2.6.3 Equipment and Data Security

The vendor shall provide a detailed description of system capabilities and mandatory procedures for purchasing jurisdictions to prevent disruption of the voting process and corruption of voting data to meet the specific requirements of Volume I, Subsection 7.3. This information shall address measures for polling place security and central count location security.

2.6.4 Software Installation

The vendor shall provide a detailed description of the system capabilities and mandatory procedures for purchasing jurisdictions to ensure secure software (including firmware) installation to meet the specific requirements of Volume I, Subsection 7.4. This information shall address software installation for all system components.

2.6.5 Telecommunications and Data Transmission Security

The vendor shall provide a detailed description of the system capabilities and mandatory procedures for purchasing jurisdictions to ensure secure data transmission to meet the specific requirements of Volume I, Subsection 7.5:

For all systems, this information shall address access control, and prevention of data interception

For systems that use public communications networks as defined in Volume I, Section 6, this information shall also include:

i. Capabilities used to provide protection against threats to third party products and services

ii. Policies and processes used by the vendor to ensure that such protection is updated to remain effective over time

iii. Policies and procedures used by the vendor to ensure that current versions of such capabilities are distributed to user jurisdictions and are installed effectively by the jurisdiction

iv. A detailed description of the system capabilities and procedures to be employed by the jurisdiction to diagnose the occurrence of a denial of service attack, to use an alternate method of voting, to determine when it is appropriate to resume voting over the network, and to consolidate votes cast using the alternate method

v. A detailed description of all activities to be performed in setting up the system for operation that are mandatory to ensure effective system security, including testing of security before an election

vi. A detailed description of all activities that should be prohibited during system setup and during the timeframe for voting operations, including both the hours when polls are open and when polls are closed

2.6.6 Other Elements of an Effective Security Program

The vendor shall provide a detailed description of the following additional procedures required for use by the purchasing jurisdiction:

Administrative and management controls for the voting system and election management, including access controls Internal security procedures, including operating procedures for maintaining the security of the software for each system function and operating mode

Adherence to, and enforcement of, operational procedures (e.g., effective password management)

Physical facilities and arrangements

Organizational responsibilities and personnel screening

This documentation shall be prepared such that these requirements can be integrated by the jurisdiction into local administrative and operating procedures.

2.7 System Test and Verification Specification

The vendor shall provide test and verification specifications for:

Development test specifications

National certification test specifications

2.7.1 Development Test Specifications

The vendor shall describe the plans, procedures, and data used during software development and system integration to verify system logic correctness, data quality, and security. This description shall include:

Test identification and design, including:

Test structure

Test sequence or progression

Test conditions

Standard test procedures, including any assumptions or constraints

Special purpose test procedures including any assumptions or constraints

Test data; including the data source, whether it is real or simulated, and how test data are controlled

Expected test results

Criteria for evaluating test results

Additional details for these requirements are provided by MIL–STD–498, Software Test Plan and Software Test Description. In the event that test data are not available, the accredited test lab shall design test cases and procedures equivalent to those ordinarily used during product verification.

2.7.2 National Certification Test Specifications

The vendor shall provide specifications for verification and validation of overall software performance. These specifications shall cover:

Control and data input/output

Acceptance criteria

Processing accuracy

Data quality assessment and maintenance

Ballot interpretation logic

Exception handling

Security

Production of audit trails and statistical data

The specifications shall identify procedures for assessing and demonstrating the suitability of the software for election use.

2.8 System Operations Procedures

This documentation shall provide all information necessary for system use by all personnel who support pre-election and election preparation, polling place activities and central counting activities, as applicable, with regard to all system functions and operations identified in Subsection 2.3 above. The nature of the instructions for operating personnel will depend upon the overall system design and required skill level of system operations support personnel.

The system operations procedures shall contain all information that is required for the preparation of detailed system operating procedures, and for operator training, as described below.

2.8.1 Introduction

The vendor shall provide a summary of system operating functions and modes, in sufficient detail to permit understanding of the system's capabilities and constraints. The roles of operating personnel shall be identified and related to the operating modes of the system. Decision criteria and conditional operator functions (such as error and failure recovery actions) shall be described.

The vendor shall also list all reference and supporting documents pertaining to the use of the system during election operations.

2.8.2 Operational Environment

The vendor shall describe the system environment, and the interface between the user or operator and the system. The vendor shall identify all facilities, furnishings, fixtures, and utilities that will be required for equipment operations, including equipment that operates at the:

Polling place
Central count facility
Other locations

2.8.3 System Installation and Test Specification

The vendor shall provide specifications for validation of system installation, acceptance, and readiness. These specifications shall address all components of the system and all locations of installation (e.g., polling place, central count facility), and shall address all elements of system functionality and operations identified in Subsection 2.3 above, including:

Pre-voting functions
Voting functions
Post-voting functions
General capabilities

These specifications also serve to provide guidance to the procuring agency in developing its acceptance test plan and procedures according to the agency's contract provisions, and the election laws of the state.

2.8.4 Operational Features

The vendor shall provide documentation of system operating features that meets the following requirements:

A detailed description of all input, output, control, and display features accessible to the operator or voter
Examples of simulated interactions to facilitate understanding of the system and its capabilities
Sample data formats and output reports
Illustrate and describe all status indicators and information messages

2.8.5 Operating Procedures

The vendor shall provide documentation of system operating procedures that meets the following requirements:

Provides a detailed description of procedures required to initiate, control, and verify proper system operation
Provides procedures that clearly enable the operator to assess the correct flow of system functions (as evidenced by system-generated status and information messages)
Provides procedures that clearly enable the operator to intervene in system operations to recover from an abnormal system state
Defines and illustrates the procedures and system prompts for situations where operator intervention is required to load, initialize, and start the system
Defines and illustrates procedures to enable and control the external interface to the system operating environment if supporting hardware and software are involved. Such information also shall be provided for the interaction of the system with other data processing systems or data interchange protocols
Provides administrative procedures and off-line operator duties (if any) if they relate to the initiation or termination of system operations, to the assessment of system status, or to the development of an audit trail
Supports successful ballot and program installation and control by election officials, provides a detailed work plan or other form of documentation providing a schedule and steps for the software and ballot installation, which includes a table outlining the key dates, events and deliverables
Supports diagnostic testing, specifies diagnostic tests that may be employed to identify problems in the system, verifies the correction of maintenance problems; and isolates and diagnoses faults from various system states

2.8.6 Operations Support

The vendor shall provide documentation of system operating procedures that meets the following requirements:

Defines the procedures required to support system acquisition, installation, and readiness testing. These procedures may be provided by reference, if they are contained either in the system hardware specifications, or in other vendor documentation
Describes procedures for providing technical support, system maintenance and correction of defects, and for incorporating hardware upgrades and new software releases

2.8.7 Appendices

The vendor may provide descriptive material and data supplementing the various sections of the body of the System Operations Manual. The content and arrangement of appendices shall be at the discretion of the vendor. Topics recommended for discussion include:

Glossary: A listing and brief definition of all terms that may be unfamiliar to persons not trained in either voting systems or computer operations
References: A list of references to all vendor documents and to other sources related to operation of the system
Detailed Examples: Detailed scenarios that outline correct system responses to faulty operator input; Alternative procedures may be specified depending on the system state
Manufacturer's Recommended Security Procedures: This appendix shall contain the security procedures that are to be executed by the system operator

2.9 System Maintenance Manual

The system maintenance procedures shall provide information in sufficient detail to support election workers, information systems personnel, or maintenance personnel in the adjustment or removal and replacement of components or modules in the field. Technical documentation needed solely to support the repair of defective components or modules ordinarily done by the manufacturer or software developer is not required.

Recommended service actions to correct malfunctions or problems shall be discussed, along with personnel and expertise required to repair and maintain the system; and equipment, materials, and facilities needed for proper maintenance. This manual shall include the sections listed below.

2.9.1 Introduction

The vendor shall describe the structure and function of the equipment (and related software) for election preparation, programming, vote recording, tabulation, and reporting in sufficient detail to provide an overview of the system for maintenance, and for identification of faulty hardware or software. The description shall include a concept of operations that fully describes such items as:

The electrical and mechanical functions of the equipment
How the processes of ballot handling and reading are performed (paper-based systems)
How vote selection and casting of the ballot are performed (DRE systems); How transmission of data over a network is performed (DRE systems, where applicable)
How data are handled in the processor and memory units

How data output is initiated and controlled
How power is converted or conditioned
How test and diagnostic information is acquired and used

2.9.2 Maintenance Procedures

The vendor shall describe preventive and corrective maintenance procedures for hardware and software.

2.9.2.1 Preventive Maintenance Procedures

The vendor shall identify and describe:

All required and recommended preventive maintenance tasks, including software tasks such as software backup, database performance analysis, and database tuning
Number and skill levels of personnel required for each task
Parts, supplies, special maintenance equipment, software tools, or other resources needed for maintenance
Any maintenance tasks that must be coordinated with the vendor or a third party (such as coordination that may be needed for off-the-shelf items used in the system)

2.9.2.2 Corrective Maintenance Procedures

The vendor shall provide fault detection, fault isolation, correction procedures, and logic diagrams for all operational abnormalities identified by design analysis and operating experience.

The vendor shall identify specific procedures to be used in diagnosing and correcting problems in the system hardware (or user-controlled software). Descriptions shall include:

Steps to replace failed or deficient equipment
Steps to correct deficiencies or faulty operations in software
Modifications that are necessary to coordinate any modified or upgraded software with other software modules
The number and skill levels of personnel needed to accomplish each procedure
Special maintenance equipment, parts, supplies, or other resources needed to accomplish each procedure
Any coordination required with the vendor, or other party, for off the shelf items

2.9.3 Maintenance Equipment

The vendor shall identify and describe any special purpose test or maintenance equipment recommended for fault isolation and diagnostic purposes.

2.9.4 Parts and Materials

Vendors shall provide detailed documentation of parts and materials needed to operate and maintain the system. Additional requirements apply for paper-based systems.

2.9.4.1 Common Standards

The vendor shall provide a complete list of approved parts and materials needed for maintenance. This list shall contain sufficient descriptive information to identify all parts by:

Type
Size
Value or range
Manufacturer's designation
Individual quantities needed
Sources from which they may be obtained

2.9.4.2 Paper-based Systems

For marking devices manufactured by multiple external sources, the vendor shall provide a listing of sources and model numbers that are compatible with the system.

The TDP shall specify the required paper stock, size, shape, opacity, color, watermarks, field layout, orientation, size and style of printing, size and location of punch or 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.

2.9.5 Maintenance Facilities and Support

The vendor shall identify all facilities, furnishings, fixtures, and utilities that will be required for equipment maintenance. In addition, vendors shall specify the assumptions made with regard to any parameters that impact the mean time to repair. These factors shall include at a minimum:

Recommended number and locations of spare devices or components to be kept on hand for repair purposes during periods of system operation
Recommended number and locations of qualified maintenance personnel who need to be available to support repair calls during system operation Organizational affiliation (i.e., jurisdiction, vendor) of qualified maintenance personnel

2.9.6 Appendices

The vendor may provide descriptive material and data supplementing the various sections of the body of the System Maintenance Manual. The content and arrangement of appendices shall be at the discretion of the vendor. Topics recommended for amplification or treatment in appendices include:

Glossary: A listing and brief definition of all terms that may be unfamiliar to persons not trained in either voting systems or computer maintenance
References: A list of references to all vendor documents and other sources related to maintenance of the system
Detailed Examples: Detailed scenarios that outline correct system responses to every conceivable faulty operator input; alternative procedures may be specified depending on the system state
Maintenance and Security Procedures: This appendix shall contain technical illustrations and schematic representations of electronic circuits unique to the system

2.10 Personnel Deployment and Training Requirements

The vendor shall describe the personnel resources and training required for a jurisdiction to operate and maintain the system.

2.10.1 Personnel

The vendor shall specify the number of personnel and skill levels required to perform each of the following functions:

Pre-election or election preparation functions (*e.g.*, entering an election, contest and candidate information; designing a ballot; generating pre-election reports
System operations for voting system functions performed at the polling place
System operations for voting system functions performed at the central count facility
Preventive maintenance tasks
Diagnosis of faulty hardware or software
Corrective maintenance tasks
Testing to verify the correction of problems

A description shall be presented of which functions may be carried out by user personnel, and those that must be performed by vendor personnel.

2.10.2 Training

The vendor shall specify requirements for the orientation and training of the following personnel:

Poll workers supporting polling place operations
System support personnel involved in election programming
User system maintenance technicians
Network/system administration personnel (if a network is used)
Information systems personnel
Vendor personnel

2.11 Configuration Management Plan

Vendors shall submit a Configuration Management Plan that addresses the configuration management requirements of Volume I, Section 9. This plan shall describe all policies, processes, and procedures employed by the vendor to carry out these requirements. Information submitted by the vendor shall be used by the accredited test lab to assist in developing and executing the system certification test plan. This information is particularly important to support the design of test plans for system modifications. A well-organized, robust and detailed Configuration Management Plan will enable the accredited test lab to more readily determine the nature and scope of tests needed to fully test the modifications. The Configuration Management Plan shall contain the sections identified below.

2.11.1 Configuration Management Policy

The vendor shall provide a description of its organizational policies for configuration management, addressing the specific requirements of Volume I, Subsection 9.2. These requirements pertain to:

Scope and nature of configuration management program activities
Breadth of application of vendor's policy and practices to the voting system

2.11.2 Configuration Identification

The vendor shall provide a description of the procedures and naming conventions used to address the specific requirements of Volume I, Subsection 9.3. These requirements pertain to:

Classifying configuration items into categories and subcategories
Uniquely numbering or otherwise identifying configuration items
Naming configuration items

2.11.3 Baseline and Promotion

The vendor shall provide a description of the procedures and naming conventions used to address the specific requirements of Volume I, Subsection 9.4. These requirements pertain to:

Establishing a particular instance of a system component as the starting baseline
Promoting subsequent instances of a component to baseline throughout the system development process for the first complete version of the system submitted for testing
Promoting subsequent instances of a component to baseline status as the component is maintained throughout its life cycle until system retirement (i.e., the system is no longer sold or maintained)

2.11.4 Configuration Control Procedures

The vendor shall provide a description of the procedures used by the vendor to approve and implement changes to a configuration item to prevent unauthorized additions, changes, or deletions to address the specific requirements of Volume I, Subsection 9.5. These requirements pertain to:

Developing and maintaining internally developed items
Developing and maintaining third party items
Resolving internally identified defects
Resolving externally identified and reported defects

2.11.5 Release Process

The vendor shall provide a description of the contents of a system release, and the procedures and related conventions by which the vendor installs, transfers, or migrates the system to accredited voting system testing laboratories and customers to address the specific requirements of Volume I, Subsection 9.6. These requirements pertain to:

A first release of the system to an accredited test lab
A subsequent maintenance or upgrade release of a system, or particular components, to an accredited test lab
The initial delivery and installation of the system to a customer
A subsequent maintenance or upgrade release of a system, or particular components, to a customer

2.11.6 Configuration Audits

The vendor shall provide a description of the procedures and related conventions for the two audits required by Volume I, Subsection 9.7. These requirements pertain to:

Physical configuration audit that verifies the voting system components submitted for certification testing to the vendor's technical documentation
Functional configuration audit that verifies the system performs all the functions described in the system documentation

2.11.7 Configuration Management Resources

The vendor shall provide a description of the procedures and related conventions for maintaining information about configuration management tools required by Volume I, Subsection 9.8. These requirements pertain to information regarding:

Specific tools used, current version, and operating environment

Physical location of the tools, including designation of computer directories and files
Procedures and training materials for using the tools

2.12 Quality Assurance Program

Vendors shall submit a Quality Assurance Program that addresses the quality assurance requirements of Volume I, Section 8. This plan shall describe all policies, processes, and procedures employed by the vendor to ensure the overall quality of the system for its initial development and release and for subsequent modifications and releases. This information is particularly important to support the design of test plans by the accredited test lab. A well-organized, robust and detailed Quality Assurance Program will enable the accredited test lab to more readily determine the nature and scope of tests needed to test the system appropriately. The Quality Assurance Program shall, at a minimum, address the topics indicated below.

2.12.1 Quality Assurance Policy

The vendor shall provide a description of its organizational policies for quality assurance, including:

Scope and nature of Quality Assurance activities
Breadth of application of vendor's policy and practices to the voting system

2.12.2 Parts and Materials Tests

The vendor shall provide a description of its practices for parts and materials tests and examinations that meet the requirements of Volume I, Subsection 8.5.

2.12.3 Quality Conformance Inspections

The vendor shall provide a description of its practices for quality conformance inspections that meet the requirements of Volume I, Subsection 8.6. For each test performed, the record of tests provided shall include:

Test location
Test date
Individual who conducted the test
Test outcomes

2.12.4 Documentation

The vendor shall provide a description of its practices for documentation of the system and system development process that meet the requirements of Volume I, Subsection 8.7.

2.13 System Change Notes

Vendors submitting modifications for a system that has been tested previously and received national certification shall submit system change notes. These will be used by the accredited test lab to assist in developing and executing the test plan for the modified system. The system change notes shall include the following information:

Summary description of the nature and scope of the changes, and reasons for each change

A listing of the specific changes made, citing the specific system configuration items changed and providing detailed references to the documentation sections changed

The specific sections of the documentation that are changed (or completely revised documents, if more suitable to address a large number of changes)

Documentation of the test plan and procedures executed by the vendor for testing the individual changes and the system as a whole, and records of test results

3 Functionality Testing

Table of Contents

3 Functionality Testing

3.1 Scope

This section contains a description of the testing to be performed to confirm the functional capabilities of a voting system submitted for national certification. It describes the scope and basis for functionality testing, outlines the general sequence of tests within the overall test process, and provides guidance on testing for accessibility.

3.2 Breadth of Functionality Testing

In order to best complement the diversity of the voting systems industry, the certification testing process is not rigidly defined. Although there are basic functionality testing requirements, additions or variations in testing are appropriate to the use of specific technologies and configurations, system capabilities, and the outcomes of previous testing.

3.2.1 Basic Functionality Testing Requirements

The accredited test lab shall design and perform procedures to test a voting system against the functional requirements outlined in Volume I, Section 2. Test procedures shall be designed and performed that address:

Overall system capabilities
Pre-voting functions
Voting functions
Post-voting functions
System maintenance
Transportation and storage

The specific procedures to be used shall be identified in the National Certification Test Plan prepared by the accredited test lab. These procedures may replicate testing performed by the vendor and documented in the vendor's TDP, but shall not rely on vendor testing as a substitute for independent functionality testing.

Recognizing variations in system design and the technologies employed by different vendors, the accredited test lab shall design test procedures that account for such variations and reflect the system-specific functional capabilities in Volume I, Section 2.

3.2.2 Testing to Reflect Technologies

Voting systems are not designed according to a standard design template. Instead, system design reflects the vendor's selections from a variety of technologies and design configurations. Such variation is recognized in the definitions of voting systems in Volume I, Section 1, and serves as the basis for delineating various functional capability requirements.

Functional capabilities will vary according to the relative complexity of a system and the manner in which the system integrates various technologies. Therefore, the testing procedure designed and performed for a particular system shall reflect the specific technologies and design configurations used by that system.

3.2.3 Testing to Reflect Additional Capabilities

The requirements for voting system functionality provided by Volume I, Section 2 reflect a minimum set of capabilities. Vendors may, and often do, provide additional capabilities in systems in order to respond to the requirements of individual states. These additional capabilities shall be identified by the vendor within the TDP, as described in Volume II, Section 2. Based on this information, the accredited test lab shall design and perform system functionality testing for these additional functional capabilities.

3.2.4 Testing to Reflect Previously Tested Capabilities

The required functional capabilities of voting systems defined in Volume I, Section 2 reflect a broad range of system functionality needed to support the full life cycle of an election, including post election activities. Many systems submitted for certification are designed to address this scope, and are to be tested accordingly.

However, some new systems using a combination of new subsystems or system components interfaced with the components of a previously certified system. For example, a vendor can submit a voting system certification testing that has a new DRE voting device, but that integrates the election management component from a previously certified system.

In this situation, the vendor shall identify in the TDP the functional capabilities supported by new subsystems/components and those supported by subsystems/components taken from a previously certified system. The vendor shall indicate in its system design documentation and configuration management records the scope and nature of any modifications made to the re-used subsystems or components. This will assist the accredited test lab to develop efficient test procedures that rely in part on the results of testing of the previously certified subsystems or components.

In this situation the accredited test lab may design and perform a test procedure that draws on the results of testing performed previously on re-used subsystems or components. However, irrespective of previous testing performed, the scope of testing shall include certain functionality tests:

All functionality performed by new subsystems/modules

All functionality performed by modified subsystems/modules

Functionality that is accomplished using any interfaces to new modules, or that shares inputs or outputs from new modules

All functionality related to vote tabulation and election results reporting

All functionality related to audit trail maintenance

3.3 General Test Sequence

There is no required sequence for performing the system certification tests. For a system not previously certified, the accredited test lab may perform tests using generic test ballots, and schedule the tests in a convenient order, provided that prerequisite conditions for each test have been satisfied before the test is initiated.

Regardless of the sequence of testing used, the full certification testing process shall include functionality testing for all system functions of a voting system. Generally, in depth functionality testing will follow testing of the system hardware and the source code review of the software. The accredited test lab will usually conduct functionality testing as an integral element of the system integration testing described in Section 6.

Some functionality tests for the voting functions defined in Volume I, Section 2.may be performed as an integral part of hardware testing, enabling a more efficient testing process. Ballots processed and counted during hardware operating tests for precinct count and central count systems may serve to satisfy part of the functionality testing, provided that the ballots were cast using a test procedure that is equivalent to the procedures indicated below.

3.3.1 Testing in Parallel with Precinct Count Systems

For testing voting functions defined in Volume I, Sections 2, the following procedures shall be performed during the functionality tests of voting equipment and precinct counting equipment.

The procedure to prepare election programs shall:

Verify resident firmware, if any
Prepare software (including firmware) to simulate all ballot format and logic options for which the system will be used
Verify program memory device content
Obtain and design test ballots with formats and voting patterns sufficient to verify performance of the test election programs

The procedures to program precinct ballot counters shall:

Install program and data memory devices, or verify presence if resident
Verify operational status of hardware as specified in Volume II, Section 4

The procedures to simulate opening of the polls shall:

Perform procedures required to prepare hardware for election operations
Obtain ''zero'' printout or other evidence that data memory has been cleared
Verify audit log of pre-election operations
Perform procedure required to open the polling place and enable ballot counting

The procedure to simulate counting ballots shall cast test ballots in a number sufficient to demonstrate proper processing, error handling, and generation of audit data as specified in Volume I, Sections 2 and 5

The procedure to simulate closing of polls shall:

Perform hardware operations required to disable ballot counting and close the polls
Obtain data reports and verify correctness
Obtain audit log and verify correctness

These procedures need not be performed in the sequence listed, provided the necessary precondition of each procedure has been met.

3.3.2 Testing in Parallel with Central Count Systems

For testing voting functions defined in Volume I, Sections 2, the following procedures shall be performed during the functional tests.

The procedure to prepare election programs shall:

Verify resident firmware, if any
Prepare software (including firmware) to simulate all ballot format and logic options for which the system will be used, and to enable simulation of counting ballots from at least 10 polling places or precincts
Verify program memory device content
Procure test ballots with formats, voting patterns, and format identifications sufficient to verify performance of the test election programs

The procedure to simulate counting ballots shall count test ballots in a number sufficient to demonstrate proper processing, error handling, and generation of audit data as specified in Volume I, Sections 2 and 5

The procedure to simulate election reports shall:

Obtain reports at polling places or precinct level
Obtain consolidated reports
Provide query access, if this is a feature of the system
Verify correctness of all reports and queries
Obtain audit log and verify correctness

They need not be performed in the sequence listed, provided the necessary preconditions of each procedure have been met.

3.4 Functionality Testing for Accessibility

Volume I, Section 4 prescribes the requirements for voting system accessibility to satisfy the provisions of HAVA 301(a)(4) and 241(b)(5). To demonstrate conformance to these requirements, vendors shall conduct summative usability tests of accessible voting equipment with blind and visually impaired individuals and individuals lacking fine motor control. A description of the testing performed, the population of test subjects participating, and the results shall be documented using the Common Industry Format (CIF) by the vendor and submitted as part of the Technical Data Package. The test labs shall review this information during the system certification documentation review.

3.5 Testing for Systems that Operate on Personal Computers

For systems intended to use non-standard voting devices, such as a personal computer, provided by the local jurisdiction, the accredited test lab shall conduct functionality tests using hardware provided by the vendor that meets the minimum configuration specifications defined by the vendor.

Section 4 provides additional information on hardware to be used to conduct functionality testing of such voting devices, as well as hardware to be used to conduct security testing and other forms of testing.

4 Hardware Testing

Table of Contents

4 Hardware Testing

4 Hardware Testing

4.1 Scope

This section contains a description of the testing to be performed to confirm the proper functioning of the hardware components of a voting system. It describes the scope and basis for functionality testing, required test conditions for conducting hardware testing, guidance for the use of test fixtures, test log data requirements, and test practices for specific non-operating and operating environmental tests.

4.2 Basis of Hardware Testing

This section addresses the focus and applicability of hardware testing and specifies the vendor's obligations to produce hardware to conduct such tests.

4.2.1 Testing Focus and Applicability

The accredited test lab shall design and perform procedures that test the voting system hardware requirements identified in Volume I, Section 4. Test procedures shall be designed and performed for both operating and non-operating environmental tests:

Operating environmental tests apply to the entire system, including hardware components that are used as part of the voting system telecommunications capability

Non-operating tests apply to those elements of the system that are intended for use at poll site voting locations, such as voting machines and precinct counters. These tests address environmental conditions that may be encountered by the voting system hardware at the voting location itself, or while in storage or transit to or from the poll site

Additionally, compatibility of this equipment with the voting system environment shall be determined through functional tests integrating the standard product with the remainder of the system.

All hardware components that are custom-designed for election use shall be tested in accordance with the applicable procedures contained in this section. Unmodified COTS hardware will not be subject to all tests. Generally such equipment has been designed to rigorous industrial standards and has been in wide use, permitting an evaluation of its performance history. To enable reduced testing of such equipment, vendors shall provide the manufacturer specifications and evidence that the equipment has been tested to the equivalent of these Guidelines.

The specific testing procedures to be used shall be identified in the National Certification Test Plan prepared by the accredited test lab. These procedures may replicate testing performed by the vendor and documented in the vendor's TDP, but shall not rely on vendor testing as a substitute for hardware testing performed by the accredited test lab.

4.2.2 Hardware Provided by Vendor

The hardware submitted for national certification testing shall be equivalent, in form and function, to the actual production versions of the hardware units. Engineering or developmental prototypes are not acceptable unless the vendor can show that the equipment to be tested is equivalent to standard production units in both performance and construction.

4.3 Test Conditions

Certification tests may be performed in any facility capable of supporting the test environment. Preparation for testing, arrangement of equipment, verification of equipment status, and the execution of procedures shall be witnessed by at least one independent, qualified observer who shall certify that all test and data acquisition requirements have been satisfied.

When a test is to be performed at ''standard'' or ''ambient'' conditions, this requirement shall refer to a nominal laboratory environment at prevailing atmospheric pressure and relative humidity.

Otherwise, all tests shall be performed at the required temperature and electrical supply voltage, regulated within the following tolerances:

Temperature of +/−4 degrees F

Electrical supply voltage +/−2 voltage alternating current

4.4 Test Log Data Requirements

The accredited test lab shall maintain a test log of the procedure employed. This log shall identify the system and equipment by model and serial number. Test environment conditions shall be noted.

In the event that the accredited test lab deems it necessary to deviate from requirements pertaining to the test environment, the equipment arrangement and method of operation, the specified test procedure, or the provision of test instrumentation and facilities, the deviation shall be recorded in the test log. A discussion of the reasons for the deviation and the effect of the deviation on the validity of the test procedure shall also be provided.

4.5 Test Fixtures

The use of test fixtures or ancillary devices to facilitate hardware testing is encouraged. These fixtures and devices may include arrangements for automating the operation of voting devices and the acquisition of test data.

The use of a fixture to ensure correctness in casting ballots by hand is recommended. Such a fixture may consist of a template, with apertures in the desired location, so that selections may be made rapidly. Such a template will eliminate or greatly minimize errors in activating test ballot patterns, while reducing the amount of time required to cast a test ballot.

For systems that use a light source as a means of detecting voter selections, the generation of a suitable optical signal by an external device is acceptable. For systems that rely on the physical activation of a switch, a mechanical fixture with suitable motion generators is acceptable.

To speed up the process of testing and to eliminate human error in casting test ballots the tests may use a simulation device with appropriate software. Such simulation is recommended if it covers all voting data detection and control paths that are used in casting an actual ballot. In the event that only partial simulation is achieved, then an independent method and test procedure must be used to validate the proper operation of those portions of the system not tested by the simulator.

If the vendor provides a means of simulating the casting of ballots, the simulation device is subject to the same performance, reliability, and quality requirements that apply to the voting device itself so as not to contribute errors to the test processes.

4.6 Non-operating Environmental Tests

This section addresses a range of tests for voting machines and precinct counters, as such devices are stored between elections and are transported between the storage facility and polling place.

4.6.1 General

Environmental tests of non-operating equipment are intended to simulate exposure to physical shock and vibration associated with handling and transportation of voting equipment and precinct counters between a jurisdiction's storage facility and precinct polling places. These tests additionally simulate the temperature and humidity conditions that may be encountered during storage in an uncontrolled warehouse environment or precinct environment. The procedures and conditions of these tests correspond generally to those of MIL-STD–810D, ''Environmental Test Methods and Engineering Guidelines,'' 19 July 1983.

In most cases, the severity of the test conditions has been reduced to reflect commercial, rather than military, practice.

Systems exclusively designed with system-level COTS hardware whose configuration has not been modified in any manner are not subject to this segment of hardware testing. Systems made up of individual COTS components such as hard drives, motherboards, and monitors that have been packaged to build a voting machine or other device will be required to undergo the hardware testing.

Prior to each test, the equipment shall be shown to be operational by means of the procedure contained in Subsection 4.6.1.5. The equipment may then be prepared as if for actual transportation or storage, and subjected to appropriate test procedures outlined. After each procedure has been completed, the equipment status will again be verified as in Subsection 4.6.1.5.

The following requirements for equipment preparation, functional tests, and inspections shall apply to each of the non-operating test procedures.

4.6.1.1 Pretest Data

The test technician shall verify that the equipment is capable of normal operation. Equipment identification, environmental conditions, equipment configuration, test instrumentation, operator tasks, time-of-day or test time, and test results shall be recorded.

4.6.1.2 Preparation for Test

The equipment shall be prepared as for the expected non-operating use, as noted below. When preparation for transport between the storage site and the polling place is required, the equipment shall be prepared with any protective enclosures or internal restraints that the vendor specifies for such transport. When preparation for storage is required, the equipment shall be prepared using any protective enclosures or internal restraints that the vendor specifies for storage.

4.6.1.3 Mechanical Inspection and Repair

After the test has been completed, the devices shall be removed from their containers, and any internal restraints shall be removed. The exterior and interior of the devices shall be inspected for evidence of mechanical damage, failure, or dislocation of internal components. Devices shall be adjusted or repaired, if necessary.

4.6.1.4 Electrical Inspection and Adjustment

After completion of the mechanical inspection and repair, routine electrical maintenance and adjustment may be performed, according to the manufacturer's standard procedure.

4.6.1.5 Operational Status Check

When all tests, inspections, repairs, and adjustments have been completed, normal operation shall be verified by conducting an operational status check.

During this process, all equipment shall be operated in a manner and under environmental conditions that simulate election use to verify the functional status of the system. Prior to the conduct of each of the environmental hardware non-operating tests, a supplemental test shall be made to determine that the operational state of the equipment is within acceptable performance limits.

The following procedures shall be followed to verify the equipment status:

Step 1: Arrange the system for normal operation.

Step 2: Turn on power, and allow the system to reach recommended operating temperature.

Step 3: Perform any servicing, and make any adjustments necessary, to achieve operational status.

Step 4: Operate the equipment in all modes, demonstrating all functions and features that would be used during election operations.

Step 5: Verify that all system functions have been correctly executed.

4.6.1.6 Failure Criteria

Upon completion of each non-operating test, the system hardware shall be subject to functional testing to verify continued operability. If any portion of the voting machine or precinct counter hardware fails to remain fully functional, the testing will be suspended until the failure is identified and corrected by the vendor. The system will then be subject to a retest.

4.6.2 Bench Handling Test

The bench handling test simulates stresses faced during maintenance and repair of voting machines and ballot counters.

4.6.2.1 Applicability

All systems and components, regardless of type, shall meet the requirements of this test. This test is equivalent to the procedure of MIL-STD–810D, Method 516.3, Procedure VI.

4.6.2.2 Procedure

Step 1: Place each piece of equipment on a level floor or table, as for normal operation or servicing.

Step 2: Make provision, if necessary, to restrain lateral movement of the equipment or its supports at one edge of the device. Vertical rotation about that edge shall not be restrained.

Step 3: Using that edge as a pivot, raise the opposite edge to an angle of 45 degrees, to a height of four inches above the surface, or until the point of balance has been reached, whichever occurs first.

Step 4: Release the elevated edge so that it may drop to the test surface without restraint.

Step 5: Repeat steps 3 and 4 for a total of six events.

Step 6: Repeat steps 2, 3, and 4 for the other base edges, for a total of 24 drops for each device.

4.6.3 Vibration Test

The vibration test simulates stresses faced during transport of voting machines and ballot counters between storage locations and polling places.

4.6.3.1 Applicability

All systems and components, regardless of type, shall meet the requirements of this test. This test is equivalent to the procedure of MIL-STD–810D, Method 514.3, Category 1-Basic Transportation, Common Carrier.

4.6.3.2 Procedure

Step 1: Install the test item in its transit or combination case as prepared for transport.

Step 2: Attach instrumentation as required to measure the applied excitation.

Step 3: Mount the equipment on a vibration table with the axis of excitation along the vertical axis of the equipment.

Step 4: Apply excitation as shown in MIL–STD–810D, Method 514.3–1, ''Basic transportation, common carrier, vertical axis'', with low frequency excitation cutoff at 10 Hz, for a period of 30 minutes.

Step 5: Repeat steps 2 and 3 for the transverse and longitudinal axes of the equipment with the excitation profiles shown in Figures 514.3–2 and 514.3–3, respectively. (Note: The total excitation period equals 90 minutes, with 30 minutes excitation along each axis.)

Step 6: Remove the test item from its transit or combination case and verify its continued operability.

4.6.4 Low Temperature Test

The low temperature test simulates stresses faced during storage of voting machines and ballot counters.

4.6.4.1 Applicability

All systems and components, regardless of type, shall meet the requirements of this test. This test is equivalent to the procedure of MIL–STD–810D, Method 502.2, Procedure I–Storage. The minimum temperature shall be −4 degrees F.

4.6.4.2 Procedure

Step 1: Arrange the equipment as for storage. Install it in the test chamber.

Step 2: Lower the internal temperature of the chamber at any convenient rate, but not so rapidly as to cause condensation in the chamber, and in any case no more rapidly than 10 degrees F per minute, until an internal temperature of −4 degrees F has been reached.

Step 3: Allow the chamber temperature to stabilize. Maintain this temperature for a period of 4 hours after stabilization.

Step 4: Allow the internal temperature of the chamber to return to standard laboratory conditions, at a rate not exceeding 10 degrees F per minute.

Step 5: Allow the internal temperature of the equipment to stabilize at laboratory conditions before removing it from the chamber.

Step 6: Remove the equipment from the chamber and from its containers, and inspect the equipment for evidence of damage.

Step 7: Verify continued operability of the equipment.

4.6.5 High Temperature Test

The high temperature test simulates stresses faced during storage of voting machines and ballot counters.

4.6.5.1 Applicability

All systems and components, regardless of type, shall meet the requirements of this test. This test is equivalent to the procedure of MIL–STD–810D, Method 501.2, Procedure I–Storage. The maximum temperature shall be 140 degrees F.

4.6.5.2 Procedure

Step 1: Arrange the equipment as for storage. Install it in the test chamber.

Step 2: Raise the internal temperature of the chamber at any convenient rate, but in any case no more rapidly than 10 degrees F per minute, until an internal temperature of 140 degrees F has been reached.

Step 3: Allow the chamber temperature to stabilize. Maintain this temperature for a period of 4 hours after stabilization.

Step 4: Allow the internal temperature of the chamber to return to standard laboratory conditions, at a rate not exceeding 10 degrees F per minute.

Step 5: Allow the internal temperature of the equipment to stabilize at laboratory conditions before removing it from the chamber.

Step 6: Remove the equipment from the chamber and from its containers, and inspect the equipment for evidence of damage.

Step 7: Verify continued operability of the equipment.

4.6.6 Humidity Test

The humidity test simulates stresses faced during storage of voting machines and ballot counters.

4.6.6.1 Applicability

All systems and components regardless of type shall meet the requirements of this test. This test is similar to the procedure of MIL–STD–810D, Method 507.2, Procedure I–Natural Hot-Humid. It is intended to evaluate the ability of the equipment to survive exposure to an uncontrolled temperature and humidity environment during storage. This test lasts for ten days.

4.6.6.2 Procedure

Step 1: Arrange the equipment as for storage. Install it in the test chamber.

Step 2: Adjust the chamber conditions to those given in MIL–STD–810D Table 507.2–I, for the time 0000 of the HotHumid cycle (Cycle 1).

Step 3: Perform a 24-hour cycle with the time and temperature-humidity values specified in Figure 507.2–1, Cycle 1.

Step 4: Repeat Step 2 until 5, 24-hour cycles have been completed.

Step 5: Continue with the test commencing with the conditions specified for time = 0000 hours.

Step 6: At any convenient time in the interval between time = 120 hours and time = 124 hours, place the equipment in an operational configuration, and perform a complete operational status check as defined in Subsection 4.6.1.5.

Step 7: If the equipment satisfactorily completes the status check, continue with the sixth 24-hour cycle.

Step 8: Perform 4 additional 24-hour cycles, terminating the test at time = 240 hours.

Step 9: Remove the equipment from the test chamber and inspect it for any evidence of damage.

Step 10: Verify continued operability of the equipment.

4.7 Environmental Tests, Operating

This section addresses a range of tests for all voting system equipment, including equipment for both precinct count and central count systems.

4.7.1 Temperature and Power Variation Tests

This test is similar to the low temperature and high temperature tests of MIL-STD–810-D, Method 502.2 and Method 501.2, with test conditions that correspond to the requirements of the performance standards. This procedure tests system operation under various environmental conditions for at least 163 hours. During 48 hours of this operating time, the device shall be in a test chamber. For the remaining hours, the equipment shall be operated at room temperature. The system shall be powered for the entire period of this test; the power may be disconnected only if necessary for removal of the system from the test chamber.

Operation shall consist of ballot-counting cycles, which vary with system type. An output report need not be generated after each counting cycle. The interval between reports, however, should be no more than 4 hours to keep to a practical minimum the time between the occurrence of a failure or data error and its detection.

Test Ballots per Counting Cycle

Precinct count systems—100 ballots/hour

Central count systems—300 ballots/hour

The recommended pattern of votes is one chosen to facilitate visual recognition of the reported totals; this pattern shall exercise all possible voting locations. System features such as data quality tests, error logging, and audit reports shall be enabled during the test.

Each operating cycle shall consist of processing the number of ballots indicated above.

Step 1: Arrange the equipment in the test chamber. Connect as required and provide for power, control, and data service through enclosure wall.

Step 2: Set the supply voltage at 117 voltage alternating current.

Step 3: Power the equipment, and perform an operational status check as in Section 4.6.1.5.

Step 4: Set the chamber temperature to 50 degrees F, observing precautions against thermal shock and condensation.

Step 5: Begin 24 hour cycle.

Step 6: At T=4 hrs, lower the supply voltage to 105 vac.

Step 7: At T=8 hrs, raise the supply voltage to 129 vac.

Step 8: At T=11:30 hrs, return the supply voltage to 117 vac and return the chamber temperature to lab ambient, observing precautions against thermal shock and condensation.

Step 9: At T=12:00 hrs, raise the chamber temperature to 95 degrees Fahrenheit.

Step 10: Repeat Steps 5 through 8, with temperature at 95 degrees Fahrenheit, complete at T=24 hrs.

Step 11: Set the chamber temperature at 50 degrees Fahrenheit as in Step 4.

Step 12: Repeat the 24 hour cycle as in Steps 5–10, complete at T=48 hrs.

Step 13: After completing the second 24 hour cycle, disconnect power from the system and remove it from the chamber if needed.

Step 14: Reconnect the system as in Step 2, and continue testing for the remaining period of operating time required until the ACCEPT/REJECT criteria of Subsection 4.7.1.1 have been met.

4.7.1.1 Data Accuracy

As indicated in Volume I, Section 4, data accuracy is defined in terms of ballot position error rate. This rate applies to the voting functions and supporting equipment that capture, record, store, consolidate, and report the specific selections, and absence of selections, made by the voter for each ballot position. Volume I, Subsection 4.1.1 identifies the specific functions to be tested.

For each processing function, the system shall achieve a target error rate of no more than one in 10,000,000 ballot positions, with a maximum acceptable error rate in the test process of one in 500,000 ballot positions. This error rate includes errors from any source while testing a specific processing function and its related equipment.

This error rate is used to determine the vote position processing volume used to test system accuracy for each function:

If the system makes one error before counting 26,997 consecutive ballot positions correctly, it will be rejected. The vendor is then required to improve the system

If the system reads at least 1,549,703 consecutive ballot positions correctly, it will be accepted

If the system correctly reads more than 26,997 ballot positions but less than 1,549,703 when the first error occurs, the testing will have to be continued until another 1,576,701 consecutive ballot positions are counted without error (a total of 3,126,404 with one error)

Appendix C provides further details of the calculation for this testing volume.

4.7.2 Maintainability Test

The accredited test lab shall test for maintainability based on the provisions of Volume I, Section 4 for maintainability, including both physical attributes and additional attributes regarding the ease of performing maintenance activities. These tests include:

Examining the physical attributes of the system to determine whether significant impediments exist for the performance of those maintenance activities that are to be performed by the jurisdiction. These activities shall be identified by the vendor in the system maintenance procedures portion of the TDP

Performing activities designated as maintenance activities for the jurisdiction in the TDP, in accordance with the instructions provided by the vendor in the system maintenance procedures, noting any difficulties encountered

Should significant impediments or difficulties be encountered that are not remedied by the vendor, the accredited test lab shall include such findings in the certification test results of the certification test report.

4.7.3 Reliability Test

The accredited test lab shall test for reliability based on the provisions of Volume I, Section 4 for the acceptable Mean Time Between Failure (MBTF). The MBTF shall be measured during the conduct of other system performance tests specified in this section, and shall be at least 163 hours. Appendix C provides further details of the calculation for this testing period.

4.7.4 Availability Test

The accredited test lab shall assess the adequacy of system availability based on the provisions of Volume I, Section 4. As described in this section, availability of voting system equipment is determined as a function of reliability, and the mean time to repair the system in the event of failure.

Availability cannot be tested directly before the voting system is deployed in jurisdictions, but can be modeled mathematically to predict availability for a defined system configuration. This model shall be prepared by the vendor, and shall be validated by the accredited testing laboratory.

The model shall reflect the equipment used for a typical system configuration to perform the following system functions:

For all paper-based systems:

Recording voter selections (such as by ballot marking)

Scanning the marks on paper ballots and converting them into digital data

For all DRE systems:

Recording and storing the voter's ballot selections

For precinct-count systems (paper-based and DRE):

Consolidation of vote selection data from multiple precinct-based systems to generate jurisdiction-wide vote counts, including storage and reporting of the consolidated vote data

For central-count systems (paper-based and DRE):

Consolidation of vote selection data from multiple counting devices to generate jurisdiction-wide vote counts, including storage and reporting of the consolidated vote data

The model shall demonstrate the predicted availability of the equipment that supports each function. This demonstration shall reflect the equipment reliability, mean time to repair, and assumptions concerning equipment availability and deployment of maintenance personnel stated by the vendor in the TDP.

4.8 Other Environmental Tests

This section addresses a range of tests for all voting system equipment, including equipment for both precinct count and central count systems.

The test for power disturbance disruption shall be conducted in compliance with the test specified in IEC 61000–4–11 (1994–06).

The test for electromagnetic radiation shall be conducted in compliance with the FCC Part 15 Class B requirements by testing per ANSI C63.4.

The test for electrostatic disruption shall be conducted in compliance with the test specified in IEC 61000–4–2 (1995–01).

The test for electromagnetic susceptibility shall be conducted in compliance with the test specified in IEC 61000–4–3 (1996).

The test for electrical fast transient protection shall be conducted in compliance with the test specified in IEC 61000–4–4 (1995–01).

The test for lightning surge protection shall be conducted in compliance with the test specified in IEC 61000–4–5 (1995–02).

The test for conducted RF immunity shall be conducted in compliance with the test specified in IEC 61000–4–6 (1996–04).

The test for AC magnetic fields RF immunity shall be conducted in compliance with the test specified in IEC 61000–4–8 (1993–06).

5 Software Testing

Table of Contents

5 Software Testing

5.1 Scope

This section contains a description of the testing to be performed by the accredited test lab to confirm the proper functioning of the software components of a voting system submitted for certification testing. It describes the scope and basis for software testing, the initial review of documentation to support software testing, and the review of the voting system source code. Further testing of the voting system software is addressed in the following sections:

Section 3 for specific tests of voting system functionality

Section 6 for testing voting system security and for testing the operation of the voting system software together with other voting system components

5.2 Basis of Software Testing

The accredited test lab shall design and perform procedures that test the voting system software requirements identified in Volume I, Section 5. All software components designed or modified for election use shall be tested in accordance with the applicable procedures contained in this section.

Unmodified, general purpose COTS non-voting software e.g., operating systems, programming language compilers, data base management systems, and Web browsers) is not subject to the detailed examinations specified in this section. However, the accredited test lab shall examine such software to confirm the specific version of software being used against the design specification to confirm that the software has not been modified. Portions of COTS software that have been modified by the vendor in any manner are subject to review.

Unmodified COTS software is not subject to code examination. However, source code generated by a COTS package and embedded in software modules for compilation or interpretation shall be provided in human readable form to the accredited test lab. The accredited test lab may inspect COTS source code units to determine testing requirements or to verify the code is unmodified.

The accredited test lab may inspect the COTS generated software source code in preparation of test plans and to provide some minimal scanning or sampling to check for embedded code or unauthorized changes. Otherwise, the COTS source code is not subject to the full code review and testing. For purposes of code analysis, the COTS units shall be treated as unexpanded macros.

Compatibility of the voting system software components or subsystems with one another, and with other components of the voting system environment, shall be determined through functional tests integrating the voting system software with the remainder of the system.

The specific procedures to be used shall be identified in the National Certification Test Plan prepared by the accredited test lab. These procedures may replicate testing performed by the vendor and documented in the vendor's TDP, but shall not rely on vendor testing as a substitute for software testing performed by the accredited test lab.

Recognizing the variations in system design and the technologies employed by different vendors, the accredited test lab shall design test procedures that account for these variations.

5.3 Initial Review of Documentation

Prior to initiating the software review, the accredited test lab shall verify that the documentation submitted by the vendor in the TDP is sufficient to enable:

Review of the source code

Design and conduct tests at every level of the software structure to verify that the software meets the vendor's design specifications and the requirements of the performance guidelines

5.4 Source Code Review

The accredited test lab shall compare the source code to the vendor's software design documentation to ascertain how completely the software conforms to the vendor's specifications. Source code inspection shall also assess the extent to which the code adheres to the requirements in Volume I, Section 5

5.4.1 Control Constructs

Voting system software shall use the control constructs identified in this section as follows:

If the programming language used does not provide these control constructs, the vendor shall provide them (that is, comparable control structure logic). The constructs shall be used consistently throughout the code. No other constructs shall be used to control program logic and execution

While some programming languages do not create programs as linear processes, stepping from an initial condition, through changes, to a conclusion, the program components nonetheless contain procedures (such as ''methods'' in object-oriented languages). Even in these programming languages, the procedures must execute through these control constructs (or their equivalents, as defined and provided by the vendor)

Operator intervention or logic that evaluates received or stored data shall not re-direct program control within a program routine. Program control may be re-directed within a routine by calling subroutines, procedures, and functions, and by interrupt service routines and exception handlers (due to abnormal error conditions). Do-While (False) constructs and intentional exceptions (used as GoTos) are prohibited

Conventional constructs that are inherent to the development language are permitted but must be documented in the code, adjacent to their use.

Illustrations of the following control construct techniques are provided in Figures 1 through 4.

Fig. 1 Sequence
Fig. 2 If-Then-Else
Fig. 3 Do-While
Fig. 4 Do-Until
Fig. 5 Case
Fig. 6 General loop, including the special case FOR loop

5.4.1.1 Replacement Rule

In the constructs shown, any 'process' may be replaced by a simple statement, a subroutine or function call, or any of the control constructs. In Fig 4–1 for example, ''Process A'' may be a simple statement and ''Process B'' another Sequence construct.

Using the replacement rule to replace one or both of the processes in the Sequence construct with other Sequence constructs, a large block of sequential code may be formed. The entire chain is recognized as a Sequence construct and is sometimes called a BLOCK construct. In many languages, a Sequence may need to be marked with special symbols or punctuation to delimit where it starts and where it ends. For example, a ''BEGIN'' and ''END'' may be used. This allows the scope of a Sequence used as ''Process C'' in the IF-THEN-ELSE (Fig 4–2) to be recognized as completing the IF-THEN-ELSE rather than part of a higher level Sequence that included the IF-THEN-ELSE as a component.

Figures 1-6

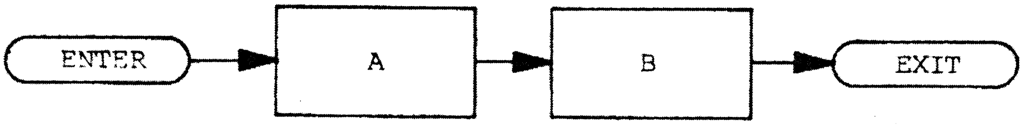


Figure 1 SEQUENCE

Control flows from "Process A" to the next in sequence, "Process B"

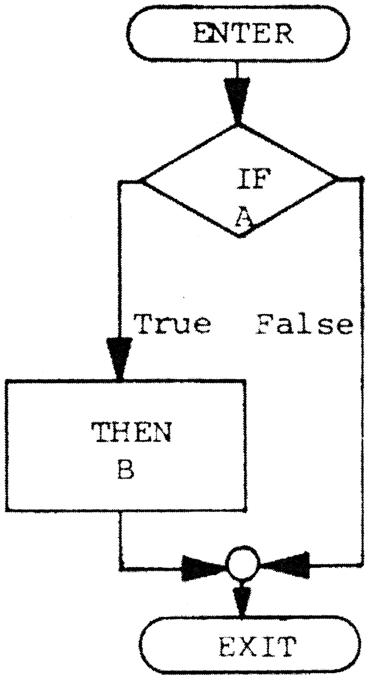


Figure 2 IF-THEN-ELSE

*In Figure 2, flow of control will skip a process pending the condition of "A."

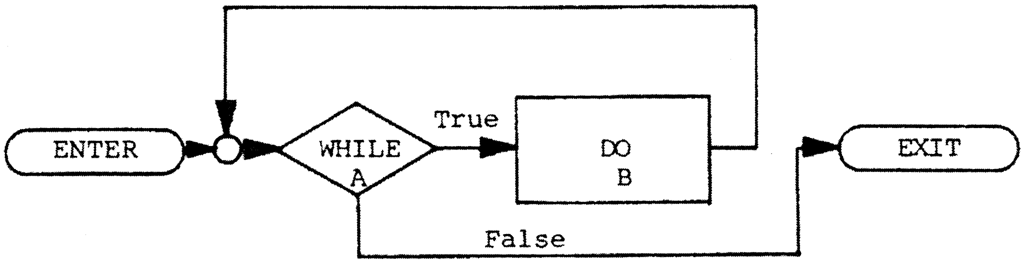


Figure 3 DO-WHILE

In Figure 4-3, condition "A" is evaluated. If found to be true, then control is passed to Process "B" and condition "A" is reevaluated. If condition "A" is found to be false, then control is passed out of the loop. Note that, if B is a BLOCK, the "DO" may be recognized as the opening symbol. A terminating symbol is needed from the language used.

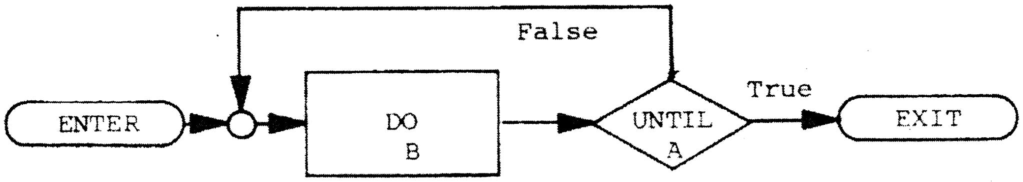


Figure 4 DO-UNTIL

Figure 4-4 is similar to a DO-WHILE, except that the test of condition A is performed after "Process B" has executed and the DO is performed upon a false "A" condition.. If condition "A" is true, control is passed out of the loop.

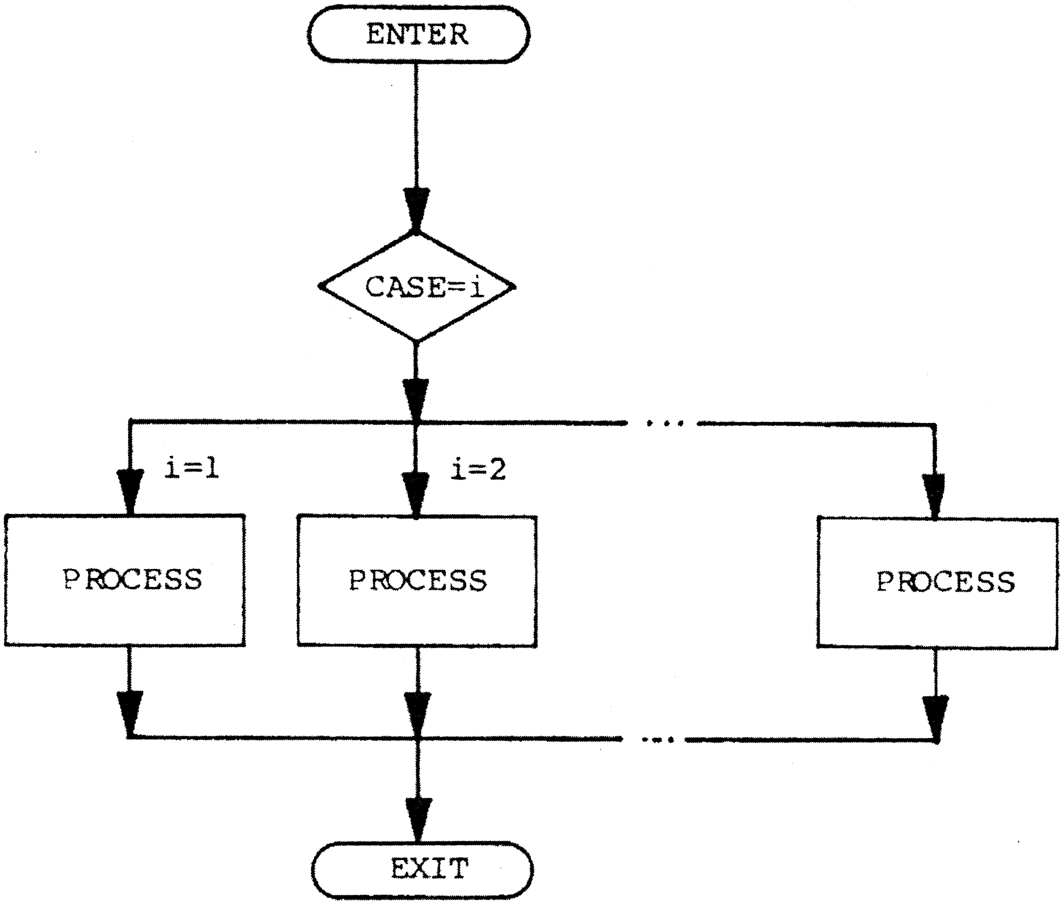


Figure 5 CASE

Control is passed to a Process based on the value of i.

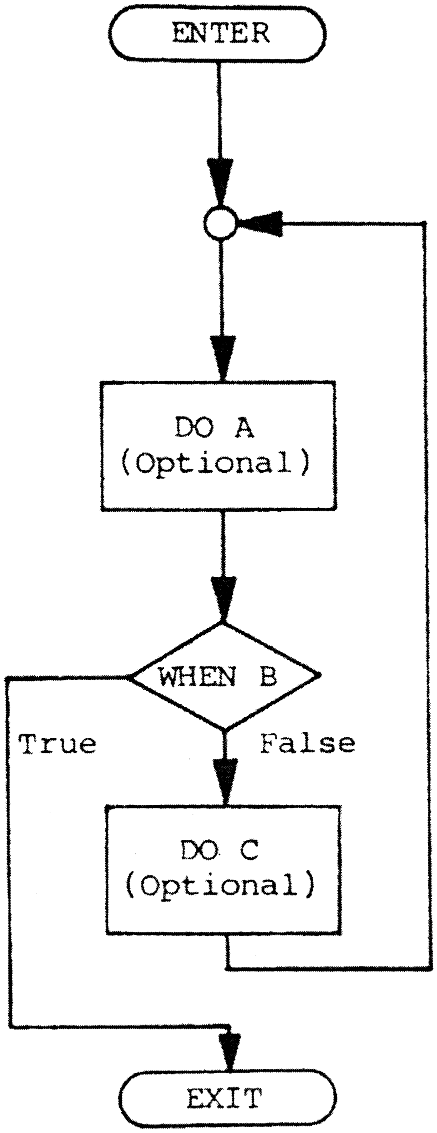


Figure 6 General LOOP

Optional process A is executed. Condition B is then evaluated. If found to be false, optional process C is executed and control is passed to process A. Condition B is then evaluated again. If condition B is true, then control is passed out of the loop.

A special case of the GENERAL LOOP is the FOR loop. The FOR loop is not strictly essential, as it can be programmed as a DO-WHILE loop. The FOR loop executes on a counter. The control FOR statement defines a counter variable or variables, a test for ending the loop, and a standard method of changing the variable(s) on each pass such as incrementing or decrementing. For example,

"FOR c = 0; c < 10; c + 1

DO process A;''

The counter is initialized to zero, if the counter test is false, the DO process is executed and the counter is incremented (or decremented). Once the counter test is true, control exits from the loop without incrementing the counter. The implementation of the FOR loop in many languages, however, can be error prone. The use of the FOR loop shall include strictly enforced coding conventions to avoid common errors such as a loop that never ends.

The GENERAL LOOP should not be used where one of the other loop structures will serve. It is error prone and may not be supported in many languages without using GOTOs type redirections. However, if defined in the language, it may be useful in defining some loops where the exit needs to occur in the middle. Also, in other languages the GENERAL LOOP logic can be used to simulate the other control constructs. Like the special case, the use of the GENERAL LOOP shall require the strict enforcement of coding conventions to avoid problems.

5.4.2 Assessment of Coding Conventions

The accredited test lab shall test for compliance with the coding conventions specified by the vendor. If the vendor does not identify an appropriate set of coding conventions in accordance with the provisions of Volume I, Subsection 5.2.6, the accredited test lab shall review the code to ensure that it:

Uses uniform calling sequences. All parameters shall either be validated for type and range on entry into each unit or the unit comments shall explicitly identify the type and range for the reference of the programmer and tester. Validation may be performed implicitly by the compiler or explicitly by the programmer

Has the return explicitly defined for callable units such as functions or procedures (do not drop through by default) for C-based languages and others to which this applies, and in the case of functions, has the return value explicitly assigned. Where the return is only expected to return a successful value, the C convention of returning zero shall be used or the use of another code justified in the comments. If an uncorrected error occurs so the unit must return without correctly completing its objective, a non-zero return value shall be given even if there is no expectation of testing the return. An exception may be made where the return value of the function has a data range including zero

Does not use macros that contain returns or pass control beyond the next statement

For those languages with unbound arrays, provides controls to prevent writing beyond the array, string, or buffer boundaries

For those languages with pointers or which provide for specifying absolute memory locations, provides controls that prevent the pointer or address from being used to overwrite executable instructions or to access inappropriate areas where vote counts or audit records are stored

For those languages supporting case statements, has a default choice explicitly defined to catch values not included in the case list

Provides controls to prevent any vote counter from overflowing. Assuming the counter size is large enough such that the value will never be reached is not adequate

Is indented consistently and clearly to indicate logical levels

Excluding code generated by commercial code generators, is written in small and easily identifiable modules, with no more than 50% of all modules exceeding 60 lines in length, no more than 5% of all modules exceeding 120 lines in length, and no modules exceeding 240 lines in length. ''Lines'' in this context, are defined as executable statements or flow control statements with suitable formatting and comments. The reviewer should consider the use of formatting, such as blocking into readable units, which supports the intent of this requirement where the module itself exceeds the limits. The vendor shall justify any module lengths exceeding this standard

Where code generators are used, the source file segments provided by the code generators should be marked as such with comments defining the logic invoked and, if possible, a copy of the source code provided to the accredited test lab with the generated source code replaced with an unexpanded macro call or its equivalent

Has no line of code exceeding 80 columns in width (including comments and tab expansions) without justification

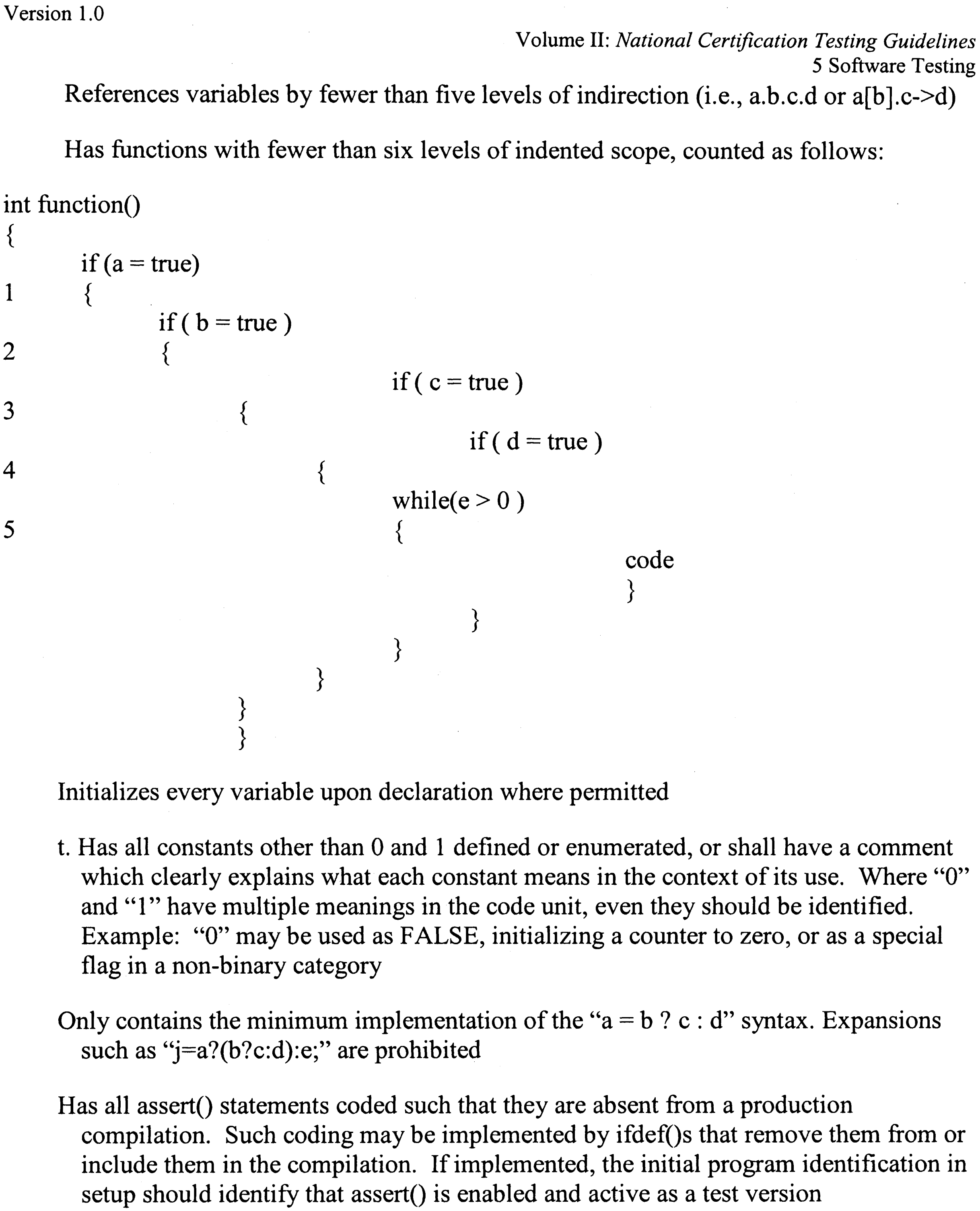
Contains no more than one executable statement and no more than one flow control statement for each line of source code

In languages where embedded executable statements are permitted in conditional expressions, the single embedded statement may be considered a part of the conditional expression. Any additional executable statements should be split out to other lines

Avoids mixed-mode operations. If mixed mode usage is necessary, then all uses shall be identified and clearly explained by comments

Upon exit() at any point, presents a message to the user indicating the reason for the exit()

Uses separate and consistent formats to distinguish between normal status and error or exception messages. All messages shall be self-explanatory and shall not require the operator to perform any look-up to interpret them, except for error messages that require resolution by a trained technician



References variables by fewer than five levels of indirection (i.e., a.b.c.d or a[b].c->d)

Has functions with fewer than six levels of indented scope, counted as follows:

```
int function()
{
        if (a = true)
1       {
                if ( b = true )
2               {
                                        if ( c = true )
3                       {
                                                if ( d = true )
4                               {
                                        while(e > 0 )
5                                       {
                                                                code
                                                                }
                                                }
                                        }
                                }
                        }
                        }
```

Initializes every variable upon declaration where permitted

t. Has all constants other than 0 and 1 defined or enumerated, or shall have a comment which clearly explains what each constant means in the context of its use. Where "0" and "1" have multiple meanings in the code unit, even they should be identified. Example: "0" may be used as FALSE, initializing a counter to zero, or as a special flag in a non-binary category

Only contains the minimum implementation of the "a = b ? c : d" syntax. Expansions such as "j=a?(b?c:d):e;" are prohibited

Has all assert() statements coded such that they are absent from a production compilation. Such coding may be implemented by ifdef()s that remove them from or include them in the compilation. If implemented, the initial program identification in setup should identify that assert() is enabled and active as a test version

6 System Integration Testing

Table of Contents

6 System Integration Testing

6 System Integration Testing

6.1 Scope

This section contains a description of the testing to be performed by the accredited test lab to confirm the proper functioning of the fully integrated components of a voting system submitted for national certification testing. It describes the scope and basis for integration testing, testing of internal and external system interfaces, testing of security capabilities, and the configuration audits, including the testing of system documentation.

System level certification tests address the integrated operation of both hardware and software, along with any telecommunications capabilities. The system level certification tests shall include the tests (functionality, volume, stress, usability, security, performance, and recovery) indicated in the National Certification Test Plan, described in Appendix A. These tests assess the system's response to a range of both normal and abnormal conditions initiated in an attempt to compromise the system. These tests may be part of the audit of the system's functional attributes, or may be conducted separately.

The system integration tests include two audits: a Physical Configuration Audit that focuses on physical attributes of the system, and a Functional Configuration Audit that focuses on the system's functional attributes, including attributes that go beyond the specific requirements of the Standards.

6.2 Basis of Integration Testing

This subsection addresses the basis for integration testing, the system baseline for testing, and data volumes for testing.

6.2.1 Testing Breadth

The accredited test lab shall design and perform procedures that test the voting system capabilities for the system as a whole. These procedures follow the testing of the systems hardware and software, and address voting system requirements defined in Volume I, Sections 2, 4, 5 and 6.

These procedures shall also address the requirements for testing system functionality provided in Section 3. Where practical, the accredited test lab will perform coverage reporting of the software branches executed in the functional testing. The selection of the baseline test cases will follow an operational profile of the common procedures, sequencing, and options among the shared state requirements and those that are specifically recognized and supported by the vendor. The accredited test lab will use the coverage report to identify any portions of the source code that were not covered and determine:

The additional functional tests that are needed
Where more detailed source code review is needed
Both of the above

The specific procedures to be used shall be identified in the National Certification Test Plan. These procedures may replicate testing performed by the vendor and documented in the vendor's TDP, but shall not rely on vendor testing as a substitute for testing performed by the accredited test lab.

Recognizing variations in system design and the technologies employed by different vendors, the accredited test lab shall design test procedures that account for these variations.

6.2.2 System Baseline for Testing

The system level certification tests are conducted using the version of the system intended to be sold by the vendor and delivered to jurisdictions. To ensure that the system version tested is the correct version, the accredited test lab shall witness the build of the executable version of the system immediately prior to or as part of, the physical configuration audit. Additionally, should components of the system be modified or replaced during the testing process, the accredited test lab shall require the vendor to conduct a new ''build'' of the system to ensure that the certified executable release of the system is built from tested components.

6.2.3 Testing Volume

For all systems, the total number of ballots to be processed by each precinct counting device during these tests shall reflect the maximum number of active voting positions and the maximum number of ballot styles that the TDP claims the system can support.

6.3 Testing Interfaces of System Components

The accredited test lab shall design and perform test procedures that test the interfaces of all system modules and subsystems with each other against the vendor's specifications. These tests shall be documented in the National Certification Test Plan, and shall include the full range of system functionality provided by the vendor's specifications, including functionality that exceeds the specific requirements of these Guidelines.

Some voting systems may use components or subsystems from previously tested and qualified systems, such as ballot preparation. For these scenarios, the accredited test lab shall, at a minimum:

Confirm that the version of previously approved components and subsystems is unchanged
Test all interfaces between previously approved modules/subsystems and all other system modules and subsystems. Where a component is expected to interface with several different products, especially from different manufacturers, the vendor shall provide a public data specification of files or data objects used to exchange information

Some systems use telecommunications capabilities. For those systems that do use such capabilities, components that are located at the polling place or separate vote counting location shall be tested for effective interface, accurate vote transmission, failure detection, and failure recovery. For voting systems that use telecommunications lines or networks that are not under the control of the election official (e.g., public telephone networks), the accredited test lab shall test the interface of vendor-supplied components with these external components for effective interface, vote transmission, failure detection, and failure recovery.

6.4 Security Testing

The accredited test lab shall design and perform test procedures that test the security capabilities of the voting system against the requirements defined in Volume I, Section 7. These procedures shall focus on the ability of the system to detect, prevent, log, and recover from the broad range of security risks identified. These procedures shall also examine system capabilities and safeguards claimed by the vendor in the TDP to go beyond these risks. The range of risks tested is determined by the design of the system and potential exposure to risk. Regardless of system design and risk profile, all systems shall be tested for effective access control and physical data security.

For systems that use public telecommunications networks, including the Internet, to transmit election management data or official election results (such as ballots or tabulated results), the accredited test lab shall conduct tests to ensure that the system provides the necessary identity-proofing, confidentiality, and integrity of transmitted data. These tests shall be designed to confirm that the system is capable of detecting, logging, preventing, and recovering from types of attacks known at the time the system is submitted for certification.

The accredited test lab may meet these testing requirements by confirming proper implementation of proven commercial security software. In this case, the vendor must provide the published standards and methods used by the U.S. Government to test and accept this software, or it may provide references to free, publicly available publications of these standards and methods, such as government web sites.

At its discretion, the accredited test lab may conduct or simulate attacks on the system to confirm the effectiveness of the system's security capabilities, employing test procedures approved by the EAC.

6.4.1 Access Control

The accredited testing laboratory shall conduct tests of system capabilities and review the access control policies and procedures submitted by the vendor to identify and verify the access control features implemented as a function of the system. For those access control features built in as components of the voting system, the accredited test lab shall design tests to confirm that these security elements work as specified.

Specific activities to be conducted by the accredited test lab shall include:

A review of the vendor's access control policies, procedures and system capabilities to confirm that all requirements of Volume I, Subsection 7.2 have been addressed completely

Specific tests designed by the accredited test lab to verify the correct operation of all documented access control procedures and capabilities, including tests designed to circumvent controls provided by the vendor. These tests shall include:

Performing the activities that the jurisdiction will perform in specific accordance with the vendor's access control policy and procedures to create a secure system, including procedures for software and firmware installation (as described in Volume I, Subsection 7.4)

Performing tests intended to bypass or otherwise defeat the resulting security environment. These tests shall include simulation of attempts to physically destroy components of the voting system in order to validate the correct operation of system redundancy and backup capabilities

This review applies to the full scope of system functionality. It includes functionality for defining the ballot and other pre-voting functions, as well as functions for casting and storing votes, vote canvassing, vote reporting, and maintenance of the system's audit trail.

6.4.2 Data Interception and Disruption

For systems that use telecommunications to transmit official voting data, the accredited test lab shall review, and conduct tests of, the data interception and prevention safeguards specified by the vendor in its TDP. The accredited test lab shall evaluate safeguards provided by the vendor to ensure their proper operation, including the proper response to the detection of efforts to monitor data or otherwise compromise the system.

For systems that use public communications networks the accredited test lab shall also review the vendor's documented procedures for maintaining protection against newly discovered external threats to the telecommunications network. This review shall assess the adequacy of such procedures in terms of:

Identification of new threats and their impact

Development or acquisition of effective countermeasures

System testing to ensure the effectiveness of the countermeasures

Notification of client jurisdictions that use the system of the threat and the actions that should be taken

Distribution of new system releases or updates to current system users

Confirmation of proper installation of new system releases

6.5 Usability and Accessibility Testing

The vendor shall design and perform procedures that test the usability and accessibility of the voting system as defined in Volume I, Section 3. Test procedures shall confirm that:

All voting machines meet the usability requirements specified in Volume I, Subsection 3.1

Voting machines intended for use by voters with disabilities provide the capabilities required by Volume I, Subsection 3.2

Voting machines intended for use by voters with disabilities operate consistently with vendor specifications and documentation

6.6 Physical Configuration Audit

The Physical Configuration Audit compares the voting system components submitted for qualification to the vendor's technical documentation, and shall include the following activities:

The audit shall establish a configuration baseline of the software and hardware to be tested. It shall also confirm whether the vendor's documentation is sufficient for the user to install, validate, operate, and maintain the voting system. MIL–STD–1521 can be used as a guide when conducting this audit

The test agency shall examine the vendor's source code against the submitted documentation during the Physical Configuration Audit to verify that the software conforms to the vendor's specifications. This review shall include an inspection of all records of the vendor's release control system. If changes have been made to the baseline version, the accredited test lab shall verify that the vendor's engineering and test data are for the software version submitted for certification

If the software is to be run on any equipment other than a COTS mainframe data processing system, minicomputer, or microcomputer, the Physical Configuration Audit shall also include a review of all drawings, specifications, technical data, and test data associated with the system hardware. This examination shall establish the system hardware baseline associated with the software baseline

To assess the adequacy of user acceptance test procedures and data, vendor documents containing this information shall be reviewed against the system's functional specifications. Any discrepancy or inadequacy in the vendor's plan or data shall be resolved prior to beginning the system integration functional and performance tests

All subsequent changes to the baseline software configuration made during the course of testing shall be subject to re-examination. All changes to the system hardware that may produce a change in software operation shall also be subject to re-examination

The vendor shall provide a list of all documentation and data to be audited, cross-referenced to the contents of the TDP. Vendor technical personnel shall be available to assist in the performance of the Physical Configuration Audit.

6.7 Functional Configuration Audit

The Functional Configuration Audit encompasses an examination of vendor tests, and the conduct of additional tests, to verify that the system hardware and software perform all the functions described in the vendor's documentation submitted for the TDP. It includes a test of system operations in the sequence in which they would normally be performed, and shall include the following activities. MIL–STD–1521 may be used as a guide when conducting this audit:

The accredited test lab shall review the vendor's test procedures and test results to determine if the vendor's specified functional requirements have been adequately tested. This examination shall include an assessment of the adequacy of the vendor's test cases and input data to exercise all system functions, and to detect program logic and data processing errors, if such be present

The accredited test lab shall perform or supervise the performance of additional tests to verify nominal system performance in all operating modes, and to verify on a sampling basis the vendor's test data reports. If vendor developmental test data is incomplete, the accredited test lab shall design and conduct all appropriate module and integrated functional tests. The functional configuration audit may be performed in the facility either of the accredited test lab or of the vendor, and shall use and verify the accuracy and completeness of the System Operations, Maintenance, and Diagnostic Testing Manuals

The vendor shall provide a list of all documentation and data to be audited, cross-referenced to the contents of the TDP. Vendor technical personnel shall be available to assist in the performance of the Functional Configuration Audit.

7 Quality Assurance Testing

Table of Contents

7 Quality Assurance Testing

7.1 Scope

This section contains a description of the examination performed by the accredited test lab to verify conformance with the requirements for configuration management and quality assurance of voting systems. It describes the scope and basis for the examinations, the general sequence of the examinations within the overall test process, and provides guidance on the substantive focus of the examinations.

7.2 Basis of Examinations

The accredited test lab shall design and perform procedures that examine documented vendor practices for quality assurance and configuration management as addressed by Volume I, Sections 8 and 9 and Section 2.

Examination procedures shall be designed and performed to ensure:

Conformance with the requirements to provide information on vendor practices required by these Guidelines

Conformance of system documentation and other information provided by the vendor with the documented practices for quality assurance and configuration management

The Guidelines do not require on-site examination of the vendor's quality assurance and configuration management practices during the system development process. However, the accredited test lab can conduct several activities while at the vendor site to witness the system build that enable assessment of the vendor's quality assurance and configuration management practices. These include surveys, interviews with individuals at all levels of the development team, and examination of selected internal work products such as system change requests and problem tracking logs.

It is recognized that examinations of vendor practices, and determinations of conformance, entail a significant degree of professional judgment. These guidelines for vendor practices identify specific areas of focus but heavily rely on the expertise and professional judgment, of the accredited test lab.

The specific procedures used by the accredited test lab shall be identified in the Qualification Test Plan. Recognizing variations in vendors' quality assurance and configuration management practices and procedures, the accredited test lab shall design examination procedures that account for these variations.

7.3 General Examinations Sequence

There is no required sequence for performing the examinations of quality assurance and configuration management practices. No other testing is dependent on the performance and results of these examinations. However, examinations pertaining to configuration management, in particular those pertaining to configuration identification, will generally be useful in understanding the conventions used to define and document the components of the system and will assist with other elements of the certification test process.

7.3.1 Vendor Practices in Parallel with Other Certification Testing

While not required, the accredited test lab is encouraged to initiate the examinations of quality assurance and configuration management practices early in the overall testing sequence, and to conduct them in parallel with other testing of the voting system. Conducting these examinations in parallel is recommended to minimize the overall duration of the testing process.

7.3.2 Functional Configuration Audit and System Integration Testing

As described in Volume I, Section 9, the functional configuration audit verifies that the voting system performs all the functions described in the system documentation. To help ensure an efficient test process, this audit shall be conducted by the accredited test lab as an element of the system integration testing that confirms the proper functioning of the system as a whole.

7.4 Examination of Configuration Management Practices

The examination of configuration management practices shall address the full scope of requirements described in Volume I, Section 9, and the documentation requirements described in Section 2. In addition to confirming that all required information has been submitted, the accredited test lab shall determine the vendor's conformance with the documented configuration management practices.

7.4.1 Configuration Management Policy

The accredited test lab shall examine the vendor's documented configuration management policy to confirm that it:

Addresses the full scope of the system, including components provided by external suppliers
Addresses the full breadth of system documentation

7.4.2 Configuration Identification

The accredited test lab shall examine the vendor's documented configuration identification practices policy to confirm that it:

Describes clearly the basis for classifying configuration items into categories and subcategories, for numbering of configuration items; and for naming of configuration items
Describes clearly the conventions used to identify the version of the system as a whole and the versions of any lower level elements (e.g., subsystems, individual elements) if such lower level version designations are used

7.4.3 Baseline, Promotion, and Demotion Procedures

The accredited test lab shall examine the vendor's documented baseline, promotion, and demotion procedures to confirm that they:

Provide a clear, controlled process that promotes components to baseline status when specific criteria defined by the vendor are met; and
Provide a clear, controlled process for demoting a component from baseline status when specific criteria defined by the vendor are met.

7.4.4 Configuration Control Procedures

The accredited test lab shall examine the vendor's configuration control procedures to confirm that they:

Are capable of providing effective control of internally developed system components
Are capable of providing effective control of components developed or supplied by third parties

7.4.5 Release Process

The accredited test lab shall examine the vendor's release process to confirm that it:

Provides clear accountability for moving forward with the release of the initial system version and subsequent releases
Provides the means for clear identification of the system version being replaced
Confirms that all required internal vendor tests and audits prior to release have been completed successfully
Confirms that each system version released to customers has been certified
Confirms that each system release has been received by the customer
Confirms that each system release has been installed successfully by the customer

7.4.6 Configuration Audits

The accredited test lab shall examine the vendor's configuration audit procedures to confirm that they:

Are sufficiently broad in scope to address the entire system, including system documentation
Are conducted with appropriate timing to enable effective control of system versions
Are sufficiently rigorous to confirm that all system documentation prepared and maintained by the vendor matches the actual system functionality, design, operation, and maintenance requirements

7.4.7 Configuration Management Resources

The accredited test lab shall examine the configuration management resource information submitted by the vendor to determine whether sufficient information has been provided to enable another organization to clearly identify the resources used and acquire them for use. This examination is intended to ensure that in the event the vendor concludes business operations, sufficient information has been provided to enable an in-depth audit of the system should such an audit be required by election officials and/or a law enforcement organization.

7.5 Examination of Quality Assurance Practices

The examination of quality assurance practices shall address the full scope of requirements described in Volume I, Section 8, and the documentation requirements described in Volume II, Section 2. The accredited test lab shall confirm that all required information has been submitted, and assess whether the vendor's quality assurance program provides for:

Clearly measurable quality standards
An effective testing program throughout the system development life cycle
Application of the quality assurance program to external providers of system components and supplies
Comprehensive monitoring of system performance in the field and diagnosis of system failures
Effective record keeping of system failures to support analysis of failure patterns and potential causes
Effective processes for notifying customers of system failures and corrective measures that need to be taken, and for confirming that such measures are taken

In addition to the general examinations described above, the accredited test lab shall focus on the specific elements of the vendor's quality assurance program indicated below.

7.5.1 Quality Assurance Policy

The accredited test lab shall examine the vendor's quality assurance policy to confirm that it:

Addresses the full scope of the voting system
Clearly designates a senior level individual accountable for implementation and oversight of quality assurance activities
Clearly designates the individuals, by position within the vendor's organization, who are to conduct each quality assurance activity
Provides procedures that determine compliance with, and correct deviations from, the quality assurance program at a minimum annually

7.5.2 Parts and Materials Tests

The accredited test lab shall examine the vendor's parts and materials special tests and examinations to confirm that they:

Identify appropriate criteria that are used to determine the specific system components for which special tests are required to confirm their suitability for use in a voting system
Are designed in a manner appropriate to determine suitability
Have been conducted and documented for all applicable parts and materials

7.5.3 Quality Conformance Inspections

The accredited test lab shall examine the vendor's quality conformance plans, procedures and, inspection results to confirm that:

All components have been tested according to the test requirements defined by the vendor
All components have passed the requisite tests

For each test, the test documentation identifies:

Test location
Test date
Individual who conducted the test
Test outcome

7.5.4 Documentation

The accredited test lab shall examine the vendor's voting system documentation to confirm that it meets the content requirements of Volume I, Subsection 8.7, and Section 2, and is written in a manner suitable for use by purchasing jurisdictions.

Appendix A: National Certification Test Plan

Table of Contents

Appendix A: National Certification Test Plan

A.1 Scope

This Appendix contains a recommended outline for the National Certification Test Plan, which is to be prepared by the test lab. The primary purpose of the test plan is to document the test lab's development of the complete or partial certification test. A sample outline is provided in Figure A–1 at the end of this Appendix.

It is intended that the test lab use this Appendix as a guide in preparing a detailed test plan, and that the scope and detail of the requirements for certification be tailored to the type of hardware, and the design and complexity of the software being tested. Required hardware tests are defined in Section 4, whereas software and system-level tests must be developed based on the vendor pre-certification tests and information available on the specific software's physical and functional configuration.

Prior to development of any test plan, the test lab must obtain the Technical Data Package (TDP) from the vendor submitting the voting system for certification. The TDP contains information necessary to the development of the test plan, such as the vendor's Hardware Specifications, Software Specifications, System Operating Manual and System Maintenance Manual.

It is specified by the Guidelines that voting systems incorporating the vendor's software and COTS hardware need only be submitted for software and system level tests. Recertification of systems with modified software or hardware is also anticipated. The test lab shall alter the test plan outline as required by these situations.

The following discussion describes the individual sections of the recommended National Certification Test Plan. The test lab shall include the identification, and a brief description of, the hardware and software to be tested, and any special considerations that affect the test design and procedure.

A.1.1 References

The test lab shall list all documents that contain material used in preparing the test plan. This list shall include specific references to applicable portions of the guidelines, and to the vendor's TDP.

A.1.2 Terms and Abbreviations

The test lab shall list and define all terms and phrases relevant to the hardware, the software, or the test plan.

A.2 Pre-certification Tests

The test lab shall evaluate vendor tests, or other lab tests in determining the scope of testing required for system certification. Pre-certification test activities may be particularly useful in designing software functional test cases and tests of system security. The test lab shall summarize pre-certification test results that support the discussion of the preceding section.

A.3 Materials Required for Testing

The following materials must be provided to the test lab to facilitate testing of the voting system:

Software
Equipment
Test materials
Deliverable materials
Proprietary data

A.3.1 Software

The test lab shall list all software required for the performance of hardware, software, telecommunications, security and system integration tests. If the test environment requires supporting software such as operating systems, compilers, assemblers, or database managers, then this software shall also be listed.

A.3.2 Equipment

The test lab shall list all equipment required for the performance of the hardware, software, telecommunications, security and system integration tests. This list shall include system hardware, general purpose data processing and communications equipment, and test instrumentation, as required.

A.3.3 Test Materials

The test lab shall list all test materials required in the performance of the test including, as applicable, test ballot layout and generation materials, test ballot sheets, test ballot cards and control cards, standard and optional output data report formats, and any other materials used to simulate preparation for, and conduct of, elections.

A.3.4 Deliverable Materials

The test lab shall list all documents and materials to be delivered as a part of the system, such as:

Hardware specification
Software specification
Voter, operator, hardware, and software maintenance manuals
Program listings, facsimile ballots, tapes
Sample output report formats

A.3.5 Proprietary Data

The test lab shall list and describe all documentation and data that are proprietary to the vendor, and hence are subject to restrictions with respect to test lab use, release, or disclosure.

A.4 Test Specifications

The test lab shall cite the pertinent hardware qualitative examinations and quantitative tests that follow from Volume I, Sections 2, 4, 5, 6, 7 and 8. The test lab shall also describe the specific test requirements that follow from the design of the software and telecommunications capabilities under test.

The certification test shall include hardware, software and telecommunications design and the development and conduct of all tests to demonstrate satisfactory performance. Environmental, non-operating tests shall be performed in the categories of simulated environmental conditions specified by the vendor or user requesting the tests. Environmental operating tests shall be performed under varying temperatures. Other functional tests shall be conducted in an environment that simulates, as nearly as possible, the intended use environment.

Test hardware and software shall be identical to that designed to be used together in the voting system, except that software intended for use with general purpose off-the-shelf hardware may be tested using any equivalent equipment capable of supporting its operation and functions.

A.4.1 Hardware Configuration and Design

The test lab shall document the hardware configuration and design in detail sufficient to identify the specific equipment being tested. This document shall provide a basis for the specific test design and include a brief description of the intended use of the hardware.

A.4.2 Software System Functions

The test lab shall describe the software functions in sufficient detail to provide a foundation for selecting the test case designs and conditions described in Section A.4.3. On the basis of this test case design, the test lab shall prepare a table delineating software functions and how each shall be tested.

A.4.3 Test Case Design

The test lab shall examine the test case design of the following aspects of the voting system:

Hardware qualitative examination design
Hardware environmental test case design
Software module test case design and data
Software functional test case design
System level test case design

A.4.3.1 Hardware Qualitative Examination Design

The test lab shall review the results, submitted by the vendor, of any previous examinations of the equipment to be tested. The results of these examinations shall be compared to the performance characteristics specified by Section 2 of the Guidelines concerning the requirements for:

Overall system capabilities
Pre-voting functions
Voting functions
Post-voting functions

In the event that a review of the results of previous examinations indicates problem areas, the test lab shall provide a description of further examinations required prior to conducting the environmental and system level tests. If no previous examinations have been performed, or records of these tests are not available, the test agency shall specify the appropriate tests to be used in the examination.

A.4.3.2 Hardware Environmental Test Case Design

The test lab shall review the documentation, submitted by the vendor, of the results and design of any previous environmental tests of the equipment submitted for testing. The test design and results shall be compared to the tests described in Section 1. The test lab shall cite any additional tests required, based on this review and those tests requested by the vendor or the state. The test lab shall also cite any environmental tests that are not to be conducted, and note the reasons why.

For complete certification, environmental tests shall include the following tests, depending upon the design and intended use of the hardware:

Non-operating tests, including the:
Bench handling test
Vibration test
Low temperature test
High temperature test
Humidity test
Operating tests involving a series of procedures that test system reliability and accuracy under various temperatures and voltages relevant to election use

A.4.3.3 Software Module Test Case Design and Data

The test lab shall review the vendor's program analysis, documentation, and, if available, module test case design. The test lab shall evaluate the test cases for each module, with respect to flow control parameters and data on both entry and exit. All discrepancies between the Software Specifications and the test case design shall be corrected by the vendor prior to initiation of the certification test.

If the vendor's module test case design does not provide conclusive coverage of all program paths, then the test lab shall perform an independent analysis to assess the frequency and consequence of error of the untested paths. The test lab shall design additional module test cases, as required, to provide coverage of all modules containing untested paths with potential for untrapped errors.

The test lab shall also review the vendor's module test data in order to verify that the requirements of the Software Specifications have been demonstrated by the data. In the event that the vendor's module test data are insufficient, the test lab shall provide a description of additional module tests, prerequisite to the initiation of functional tests.

A.4.3.4 Software Functional Test Case Design

The test lab shall review the vendor's test plans and data to verify that the individual performance requirements described in Subsection 2.5.3, are reflected in the software.

As a part of this process, the test lab shall review the vendor's functional test case designs. The test lab shall prepare a detailed matrix of system functions and the test cases that exercise them. The test lab shall also prepare a test procedure describing all test ballots, operator procedures, and the data content of output reports. Abnormal input data and operator actions shall be defined. Test cases shall also be designed to verify that the system is able to handle and recover from these abnormal conditions.

The vendor's test case design may be evaluated by any standard or special method appropriate; however, emphasis shall be placed on those functions where the vendor data on module development reflects significant debugging problems, and on functional tests that resulted in disproportionately high error rates.

The test lab shall define ACCEPT/REJECT criteria for certification using the Software Specifications and, if the software runs on special hardware, the associated Hardware Specifications to determine acceptable ranges of performance.

The test lab shall describe the functional tests to be performed. Depending upon the design and intended use of the voting system, all or part of the functions listed below shall be tested.

Ballot preparation subsystem
Test operations performed prior to, during, and after processing of ballots, including:
Logic tests to verify interpretation of ballot styles, and recognition of precincts to be processed
Accuracy tests to verify ballot reading accuracy
Status tests to verify equipment statement and memory contents
Report generation to produce test output data
Report generation to produce audit data records

Procedures applicable to equipment used in the polling place for:

Opening the polling place and enabling the acceptance of ballots and maintaining a count of processed ballots
Monitoring equipment status

Verifying equipment response to operator input commands
Generating real-time audit messages
Closing the polling place and disabling the acceptance of ballots
Generating election data reports
Transfer of ballot counting equipment, or a detachable memory module, to a central counting location
Electronic transmission of election data to a central counting location

Procedures applicable to equipment used in a central counting place:

Initiating the processing of a ballot deck or programmable memory device for one or more precincts
Monitoring equipment status
Verifying equipment response to operator input commands
Verifying interaction with peripheral equipment, or other data processing systems
Generating real-time audit messages
Generating precinct-level election data reports
Generating summary election data reports
Transfer of a detachable memory module to other processing equipment
Electronic transmission of data to other processing equipment
Producing output data for interrogation by external display devices

A.4.3.5 System-level Test Case Design

The test lab shall provide a description of system tests of both the software and hardware. For software, these tests shall be designed according to the stated design objective without consideration of its functional specification. The test lab shall independently prepare the system test cases to assess the response of the hardware and software to a range of conditions, such as:

Volume tests: These tests investigate the system's response to processing more than the expected number of ballots/voters per precinct, to processing more than the expected number of precincts, or to any other similar conditions that tend to overload the system's capacity to process, store, and report data.

Stress tests: These tests investigate the system's response to transient overload conditions. Polling place devices shall be subjected to ballot processing at the high volume rates at which the equipment can be operated to evaluate software response to hardware-generated interrupts and wait states. Central counting systems shall be subjected to similar overloads, including, for systems that support more than one card reader, continuous processing through all readers simultaneously.

Usability tests: These tests are designed to exercise characteristics of the software such as response to input control or text syntax errors, error message content, audit message content, and other features contained in the software design objectives but not directly related to a functional specification.

Accessibility tests: The test lab shall review the vendor's documentation of the usability and accessibility testing performed during system development.

Security tests: These tests are designed to defeat the security provisions of the system including modification or disruption of pre-voting, voting, and post voting processing; unauthorized access to, deletion, or modification of data, including audit trail data; and modification or elimination of security mechanisms.

Performance tests: These tests verify accuracy, processing rate, ballot format handling capability, and other performance attributes claimed by the vendor.

Recovery tests: These tests verify the ability of the system to recover from hardware and data errors.

A.5 Test Data

A.5.1 Data Recording

The test lab shall identify all data recording requirements (e.g.; what is to be measured, how tests and results are to be recorded). The test lab shall also design or approve the design of forms or other recording media to be employed. The test lab shall supply any special instrumentation (e.g., pulse measuring device) needed to satisfy the data requirements.

A.5.2 Test Data Criteria

The test lab shall describe the criteria against which test results will be evaluated, such as the following:

Tolerances: These criteria define the acceptable range for system performance. These tolerances shall be derived from the applicable hardware performance requirements contained in Volume I, Section 4

Samples: These criteria define the minimum number of combinations or alternatives of input and output conditions that can be exercised to constitute an acceptable test of the parameters involved

Events: These criteria define the maximum number of interrupts, halts or other system breaks that may occur due to non-test conditions. This count shall not include events from which recovery occurs automatically or where a relevant status message is displayed

A.5.3 Test Data Reduction

The test lab shall describe the techniques to be used for processing test data. These techniques may include manual, semi-automatic, or fully automatic reduction procedures. However, semi-automatic and automatic procedures must be demonstrated to be capable of handling the test data accurately and properly. They shall also produce an item-by-item comparison of the data and the embedded acceptance criteria as output.

A.6 Test Procedure and Conditions

The test lab shall describe the test conditions and procedures for performing the tests. If tests are not to be performed in random order, this section shall contain the rationale for the required sequence, and the criteria that must be met, before the sequence can be continued. This section shall also describe the procedure for setting up the equipment in which the software will be tested, for system initialization, and for performing the tests. Each of the following sections that contain a description of a test procedure shall also contain a statement of the criteria by which readiness and successful completion shall be indicated and measured.

A.6.1 Facility Requirements

The test lab shall describe the space, equipment, instrumentation, utilities, manpower, and other resources required to support the test program.

A.6.2 Test Set-up

The test lab shall describe the procedure for arranging and connecting the system hardware with the supporting hardware and telecommunications equipment, if applicable. It shall also describe the procedure required to initialize the system, and to verify that it is ready to be tested.

A.6.3 Test Sequence

The test lab shall state any restrictions on the grouping or sequence of tests in this section.

A.6.4 Test Operations Procedures

The test lab shall provide the step-by-step procedures for each test case to be conducted. Each step shall be assigned a test step number and this number, along with critical test data and test procedures information, shall be tabulated onto a test report form for test control and the recording of test results.

In this section, the test lab shall also identify all test operations personnel, and their respective duties. In the event that the operator procedure is not defined in the vendor's operations or user manual, the test lab shall also provide a description of the procedures to be followed by the test personnel.

Figure 1

Test Plan Outline

1 Introduction

1.1 References
1.2 Terms and Abbreviations

2 Pre-certification Tests

Pre-certification Test Activity
2.2 Pre-certification Test Results

3 Materials Required for Testing

3.1 Software
3.2 Equipment
3.3 Test Materials
3.4 Deliverable Materials
Proprietary Data

4 Test Specification

4.1 equirements
4.2 Hardware Configuration and Design
4.3 Software System Functions
4.4 Test Case Design
4.4.1 Hardware Qualitative Examination Design
4.4.2 Hardware Environmental Test Case Design
4.4.3 Software Module Test Case Design and Data
4.4.4 Software Functional Test Case Design and Data
4.4.5 System-level Test Case Design

5 Test Data

5.1 Data Recording
5.2 Test Data Criteria
5.3 Test Data Reduction

6 Test Procedure and Conditions

6.1 Facility Requirements
6.2 Test Set-up
6.3 Test Sequence
Test Operations Procedures

Appendix B: National Certification Test Report

Table of Contents

B National Certification Test Report

Appendix B: National Certification Test Report

B.1 Scope

This Appendix contains a recommended outline for the National Certification Test Report to be prepared by the accredited test lab. The test report shall be organized so as to facilitate the presentation of conclusions and recommendations regarding system acceptability, a summary of the test operations, a summary of the test results, the test data records, and the analyses that support the conclusions and recommendations. The content of the report may vary based on the scope of review conducted.

B.1.1 New Certification Test Report

A full report is prepared for the initial certification testing of a voting system. This document consists of five main sections: Introduction, Certification Test Background, System Identification, System Overview, and Certification Test Results.

Detailed information about the test operations and findings, and test data, are included as appendices to the report.

Sections B.2 through B.7 describe the contents of the individual sections of this report.

B.1.2 Changes to Previously Certified Test Report

This report addresses a wide range of scenarios. After a preliminary review of the submitted changes, the accredited test lab may determine that:

A review of all change documentation against the baseline materials is sufficient for recommendation for certification
All changes must be retested against the previously certified baseline
The scope of the changes is substantial enough that a complete retest of the software is required

The format of this report will vary, based on the type of review that is performed. If only a review of change documentation against the baseline materials is performed the report is quite simple. It consists of an Introduction, a Version Description, the Testing Approach, and a Results Summary. A more extensive report is prepared, for changes that have extensive impact on the system design and/or operations.

B.2 Certification Test Background

This section contains the following information:

General information about the certification test process
A list and definition of all terms and nomenclature peculiar to the hardware, the software, or the test report

B.3 System Identification

This section gives information about the tested software and supporting hardware, including:

System name and major subsystems (or equivalent)
System version
Test support hardware
Specific documentation provided in the vendor's TDP used to support testing

B.4 System Overview

This section describes the voting system in terms of its overall design structure, technologies used, processing capacity claimed by the vendor for system components (such as ballot counters, voting machines, vote consolidation equipment), and mode of operation. It may also identify other products that interface with the voting system.

B.5 Certification Test Results and Recommendation

This section provides a summary of the results of the testing process, and indicates any special considerations that affect the conclusions derived from the test results. This summary includes:

The acceptability of the system design and construction based on the performance of the system hardware, software and communications, and on the source code inspection
The degree to which the hardware and software meet the vendor's specifications and the guidelines, and the acceptability of the vendor's technical and user documentation
General findings on the maintainability of the system including, where applicable, notation of specific maintenance activities that are determined to be difficult to perform
Identification and description of any deficiencies that remain uncorrected after completion of the certification test and that have caused or are judged to be capable of causing, the loss or corruption of voting data, providing sufficient detail to support a recommendation to reject the system being tested. Similarly, any deficiency in compliance with the security, accuracy, data retention, and audit requirements are fully described
A specific recommendation to the EAC for approval or rejection

Of note, any uncorrected deficiency that does not involve the loss or corruption of voting data shall not necessarily be cause for rejection. Deficiencies of this type may include failure to fully achieve the levels of performance specified in Volume I or failure to fully implement formal programs for quality assurance and configuration management described in Volume I, Sections 8 and 9. The nature of the deficiency is described in detail sufficient to support the recommendation either to accept or to reject the system. The recommendation is based on consideration of the probable effect the deficiency will have on safe and efficient system operation during all phases of election use.

B.6 Appendix—Test Operations and Findings

This appendix provides additional detail about the test results to enable the understanding of test results and recommendation. This information is organized in a manner that reflects the Certification Test Plan. Summaries of the results of hardware examinations, operating and non-operating hardware tests, software module tests, software function tests, and system-level tests (including security and telecommunications tests, and the results of the Physical and Functional Configuration Audits) are provided.

B.7 Appendix—Test Data Analysis

This appendix provides summary records of the test data and the details of the analysis. The analysis includes a comparison of the vendor's hardware and software specifications to the test data, together with any mathematical or statistical procedure used for data reduction and processing.

Appendix C: National Certification Test Design Criteria

Table of Contents

C National Certification Test Design Criteria

Appendix C: National Certification Test Design Criteria

C.1 Scope

This appendix describes the guiding principles used to design the voting system certification testing process conducted by the accredited test lab.

Certification tests are designed to demonstrate that the system meets or exceeds the requirements of the Guidelines. The tests are also used to demonstrate compliance with other levels of performance claimed by the manufacturer.

Certification tests must satisfy two separate and possibly conflicting sets of considerations. The first is the need to produce enough test data to provide confidence in the validity of the test and its apparent outcome. The second is the need to achieve a meaningful test at a reasonable cost, and cost varies with the difficulty of simulating expected real-world operating conditions and with test duration. It is the test designer's job to achieve an acceptable balance of these constraints.

The rationale for, and statistical methods of, the test designs required by the Guidelines are discussed below. Technical descriptions of these designs can be found in any of several books on testing and statistical analysis.

C.2 Approach to Test Design

The certification tests specified in the Guidelines are primarily concerned with assessing the magnitude of random errors. They are also, however, capable of detecting bias errors that would result in the rejection of the system.

Test data typically produce two results. The first is an estimate of the true value of some system attribute such as speed, error rate, etc. The second is the degree of certainty that the estimate is a correct one. The estimate of an attribute's value may or may not be greatly affected by the duration of the test. Test duration, however, is very important to the degree of certainty; as the length of the test increases, the level of uncertainty decreases. An efficient test design will produce enough data over a sufficient period of time to enable an estimate at the desired level of confidence.

There are several ways to design tests. One approach involves the pre-selection of some test parameter, such as the number of failures or other detectable factors. The essential element of this type of design is that the number of observations is independent of their results. The test may be designed to terminate after 1,000 hours or 10 days, or when 5 failures have been observed. The number of failures is important because the confidence interval (uncertainty band) decreases rapidly as the number of failures increases. However, if the system is highly reliable or very accurate, the length of time required to produce a predetermined number of failures or errors using this method may be unachievably long.

Another approach is to determine that the actual value of some attribute need not be learned by testing, provided that the value can be shown to be better than some level. The test would not be designed to produce an estimate of the true value of the attribute but instead to show, for example, that reliability is at least 123 hours or the error rate is no greater than one in ten million characters.

The latter design approach, which was chosen for the Guidelines, uses what is called Sequential Analysis. Instead of the test duration being fixed, it varies depending on the outcome of a series of observations. The test is terminated as soon as a statistically valid decision can be reached that the factor being tested is at least as good as, or no worse than, the predetermined target value. A sequential analysis test design called the ''Wald Probability Ratio Test'' is used for reliability and accuracy testing.

C.3 Probability Ratio Sequential Test (PRST)

The design of a Probability Ratio Sequential Test (PRST) requires that four parameters be specified:

H0, the null hypothesis
H1, the alternate hypothesis
a, the producer's risk
b, the consumer's risk

The Guidelines anticipate using the PRST for testing both time-based and event-based failures.

This test design provides decision criteria for accepting or rejecting one of two test hypotheses: the null hypothesis, which is the Nominal Specification Value (NSV), or the alternate hypothesis, which is the MAV. The MAV could be either the Minimum Acceptable Value, or the Maximum Acceptable Value, depending upon what is being tested. Performance may be specified by means of a single value or by two values. When a single value is specified, it shall be interpreted as an upper or lower single-sided 90 percent confidence limit. If two values, these shall be interpreted as a two-sided 90 percent confidence interval, consisting of the NSV and MAV.

In the case of Mean Time Between Failure (MTBF), for example, the null hypothesis is that the true MTBF is at least as great as the desired value (NSV), while the alternate hypothesis is that the true value of the MTBF is less than some lower value (Minimum Acceptable Value). In the case of error rate, the null hypothesis is that the true error rate is less than some very small desired value (NSV), while the alternate hypothesis is that the true error rate is greater than some larger value that is the upper limit for acceptable error (Maximum Acceptable Value).

C.4 Time-based Failure Testing Criteria

The equivalence between a number of events and a time period can be established when the operating scenarios of a system can be determined with precision. Some of the performance test criteria of Volume II, Section 4, use this equivalence.

System acceptance or rejection can be determined by observing the number of relevant failures that occur during equipment operation. The probability ratio for this test is derived from the exponential probability distribution. This distribution implies a constant hazard rate for equipment failure that is not dependent on the time of testing or the previous failures. In that case, two or more systems may be tested simultaneously to accumulate the required number of test hours, and the validity of the data is not affected by the number of operating hours on a particular unit of equipment. However, for environmental operating hardware tests, no unit shall be subjected to less than two complete 24-hour test cycles in a test chamber as required by Volume II, Subsection 4.7.1.

In this case, the null hypothesis is that the Mean Time Between Failure (MTBF), as defined in Volume I, Subsection 4.3.3 is at least as great as some value, here the Nominal Specification Value. The alternate hypothesis is that the MTBF is no better than some value, here the Minimum Acceptable Value.

For example, a typical system operations scenario for environmental operating hardware tests will consist of approximately 45 hours of equipment operation. Broken down, this time allotment involves 30 hours of equipment setup and readiness testing and 15 hours of elections operations. If the Minimum Acceptable Value is defined as 45 hours, and a test discrimination ratio of 3 is used (in order to produce an acceptably short expected time of decision), then the Nominal Specification Value equals 135 hours.

With a value of decision risk equal to 10 percent, there is no more than a 10 percent chance that a system would be rejected when, in fact, with a true MTBF of at least 135 hours, the system would be acceptable. It also means that there is no more than a 10 percent chance that a system would be accepted with a true MTBF lower than 45 hours when it should have been rejected.

Therefore,

H0: MTBF = 135 hours
H1: MTBF = 45 hours
a = 0.10
b = 0.10.

Under this PRST design, the test is terminated and an ACCEPT decision is reached when the cumulative number of equipment hours in the second column of the following table has been reached, and the number of failures is equal to or less than the number shown in the first column. The test is terminated and a REJECT decision is reached when the number of failures occurs in less than the number of hours specified in the third column. Here, the minimum time to accept (on zero failures) is 169 hours. In the event that no decision has been reached by the times shown in the last table entries, the test is terminated, and the decision is declared as indicated. Any time that 7 or more failures occur, the test is terminated and the equipment rejected. If, after 466 hours of operation, the cumulative failure score is less than 7.0, then the equipment is accepted.

Number of failures	Accept if time greater than	Reject if time less than
0	169	Continue test
1	243	Continue test
2	317	26
3	392	100
4	466	175
5	466	249
6	466	323
7	N/A	(1)

(1) Terminate and REJECT

This test is based on the table of test times of the truncated PRST design V-D in the Military Handbook MIL-HDBK–781A that is designated for discrimination ratio 3 and a nominal value of 0.10 for both a and b. The Handbook states that the true producer risk is 0.111 and the true consumer risk is 0.109. Using the theoretical formulas for either the untruncated or truncated tests will lead to different numbers.

The test design will change if given a different set of parameters. Some jurisdictions may find the Minimum Acceptable Value of 45 hours unacceptable for their needs. In addition, it may be appropriate to use a different discrimination ratio, or different, Consumer's and Producer's risk. Also, before using tests based on the MTBF, it should be determined whether time-based testing is appropriate rather than event-based or another form of testing. If MTBF-based procedures are chosen, then the appropriateness of the assumption of a constant hazard rate with exponential failures should in turn be assessed.

C.5 Accuracy Testing Criteria

Some voting system performance attributes are tested by inducing an event or series of events, and the relative or absolute time intervals between repetitions of the event has no significance. Although equivalence between a number of events and a time period can be established when the operating scenarios of a system can be determined with precision, another type of test is required when such equivalence cannot be established. It uses event-based failure frequencies to arrive at ACCEPT/REJECT criteria. This test may be performed simultaneously with time-based tests.

For example, the failure of a device is usually dependent on the processing volume that it is required to perform. The elapsed time over which a certain number of actuation cycles occur is, under most circumstances, not important. Another example of such an attribute is the frequency of errors in reading, recording, and processing vote data.

The error frequency, called ''ballot position error rate,'' applies to such functions as process of detecting the presence or absence of a voting punch or mark, or to the closure of a switch corresponding to the selection of a candidate.

Certification and acceptance test procedures that accommodate event-based failures are, therefore, based on a discrete, rather than a continuous probability distribution. A Probability Ratio Sequential Test using the binomial distribution is recommended. In the case of ballot position error rate, the calculation for a specific device (and the processing function that relies on that device) is based on:

HO: Desired error rate = 1 in 10,000,000
H1: Maximum acceptable error rate = 1 in 500,000
a = 0.05
b = 0.05

and the minimum error-free sample size to accept for qualification tests is 1,549,703 votes.

The nature of the problem may be illustrated by the following example, using the criteria contained in the Guidelines for system error rate. A target for the desired accuracy is established at a very low error rate. A threshold for the worst error rate that can be accepted is then fixed at a somewhat higher error rate. Next, the decision risk is chosen, that is, the risk that the test results may not be a true indicator of either the system's acceptability or unacceptability. The process is as follows:

The desired accuracy of the voting system, whatever its true error rate (which may be far better), is established as no more than one error in every ten million characters (including the null character)

If it can be shown that the system's true error rate does not exceed one in every five hundred thousand votes counted, it will be considered acceptable. This is more than accurate enough to declare the winner correctly in almost every election

A decision risk of 5 percent is chosen, to be 95 percent sure that the test data will not indicate that the system is bad when it is good or good when it is bad

This results in the following decision criteria:

d. If the system makes one error before counting 26,997 consecutive ballot positions correctly, it will be rejected. The vendor is then required to improve the system

e. If the system reads at least 1,549,703 consecutive ballot positions correctly, it will be accepted

f. If the system correctly reads more than 26,997 ballot positions but less than 1,549,703 when the first error occurs, the testing will have to be continued until another 1,576,701 consecutive ballot positions are counted without error (a total of 3,126,404 with one error)

[FR Doc. 06–3100 Filed 4–11–06; 8:45 am]

BILLING CODE 6820–KF–P