ELECTION ASSISTANCE COMMISSION

Technical Guidelines Development Committee (TGDC); Initial Report: Voluntary Voting System Guidelines Version I

AGENCY: United States Election Assistance Commission.

ACTION: Notice; publication of TGDC recommendations for voluntary voting system guidelines.

SUMMARY: The Help America Vote Act of 2002 (HAVA) Section 221(f) directs the Technical Guidelines Development Committee (TGDC) to publish its recommendations to the Executive Director of the U.S. Election Assistance Commission (EAC) at the time EAC adopts voluntary voting system guidelines. In 2004, the EAC formed the TGDC to create an initial set of recommendations for guidelines as directed by HAVA. 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, which are published here. These recommendations were used by the EAC in producing the EAC's proposed 2005 Voluntary Voting System Guidelines which were published for public comment in June 2005, 70 FR 37378 (June 29, 2005). Following revision of its proposed guidelines to reflect the comments received, the EAC adopted the final 2005 Voluntary Voting System Guidelines on December 13, 2005. This final document is being concurrently published as required by HAVA.

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

Thomas R. Wilkey,

Executive Director, U.S. Election Assistance Commission.

BILLING CODE 6820–KF–P

UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899-
OFFICE OF THE DIRECTOR

MAY 0 6 2005

Ms. Carol Paquette
Interim Executive Director
U.S. Election Assistance Commission
1225 New York Avenue, N.W.
Suite 1100
Washington D.C. 20005

Dear Ms. Paquette:

Public Law 107-252, the Help America Vote Act (HAVA), requires the Technical Guidelines Development Committee (TGDC) to provide an initial set of recommendations for voluntary voting system guidelines to the Executive Director of the U.S. Election Assistance Commission (EAC) no later than nine months after all members of the TGDC have been appointed. The membership of the TGDC was completed on August 9, 2004.

As adopted by the TGDC at its April 2005 plenary session, the enclosed document, "Voluntary Voting System Guidelines Version 1: Initial Report" (VVSG Version 1), serves as the initial set of recommendations mandated by HAVA in Section 221.

I am most gratified to deliver this document to you within the time frame stipulated in HAVA. As chairman of the Committee, I note that the recommendations were adopted unanimously and represent many hours of volunteered expertise by the members of the TGDC with technical assistance from NIST scientists.

I look forward to the review of VVSG Version 1 by the EAC, the Standards and Advisory Boards, and the American public.

Sincerely,

Hratch G. Semerjian
Chairman
Technical Guidelines Development Committee

Enclosure

Voluntary Voting System Guidelines Version I

Initial Report

May 9, 2005

PRODUCT OF THE TECHNICAL GUIDELINES DEVELOPMENT COMMITTEE WITH TECHNICAL ASSISTANCE FROM THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

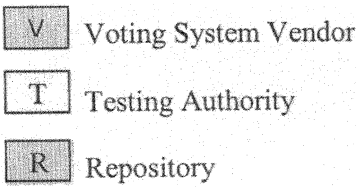
Voluntary Voting System Guidelines—Overview

This section provides an overview of the Voluntary Voting System Guidelines (VVSG), Version 1. The VVSG was created in response to the Help America Vote Act (HAVA) of 2002 and is based on the initial set of recommendations of the Technical Guidelines Development Committee (TGDC) mandated by HAVA. The VVSG Version 1 augments the Voting Systems Standard (VSS) of 2002 (VSS–2002), which was promulgated by the Federal Election Commission (FEC). This overview serves as an explanation of how the VVSG Version 1 differs from the VSS–2002 and provides a basis for further improvements. In addition, it provides a high level overview of the major sections of the two volumes that make up VVSG Version 1.

Document Structure

This document presents the voluntary voting system guidelines as a single document consisting of two volumes: Volume I, the performance provisions of the guidelines and Volume II, the testing specification. Sections of this document augment the VSS–2002, by either replacing VSS–2002 sections or adding new sections. New material is indicated by distinct header information on each page. The header information is in a gray shaded box and includes the words ''NEW MATERIAL''. The footer information also includes the words ''NEW MATERIAL''. Additionally, line numbers have been added to these pages.

In the new sections that contain requirements or informative characteristics, each requirement or characteristic is numbered according to a hierarchical scheme in which higher-level requirements (such as ''provide accessibility for blind voters'') are supported by lower level requirements (''provide an audio-tactile interface''). These sections are: Sections 2.2.7, 6.0.1, 6.0.2, 6.0.3, 6.0.4, and Appendix D. Additionally, each requirement or characteristic indicates to whom it applies (*i.e.*, responsible entity) as well as which stage of the voting process (*i.e.*, pre-voting, voting, post-voting) is affected. There are three responsible entities: voting system vendor (V), testing authority (T), and repository (R). To aid the reader, a colored box with the first letter of the responsible entity, *i.e.*, V, T, or R accompanies the name of the entity, as follows:



The three stages of the voting process are indicated by a presenting a box with all three stages and using a strikeout font to indicate the stages that are not applicable, as follows:

Pre-Voting	~~Voting~~	~~Post-Voting~~

Indicates the pre-voting stage is the only stage that applies.

Pre-Voting	Voting	Post-Voting

Indicates all three stages apply.

Background

The Help America Vote Act (HAVA) established the Technical Guidelines Development Committee to assist the Election Assistance Commission (EAC) with the development of voluntary voting system guidelines. HAVA directs the National Institute of Standards and Technology (NIST) to chair the TGDC and to provide technical support to the TGDC in the development of these guidelines. The TGDC's initial set of recommendations for these guidelines were presented to the Election Assistance Commission in May 2005, in accordance with HAVA's nine-month deadline.

VVSG Version 1 is intended to assist State election officials in preparing for the 2006 election. This document augments the VSS–2002 to address the critical areas of accessibility, usability and computer security. In addition, the VVSG includes an improved glossary to promote common understanding, a conformance clause, and an updated Appendix on error rates.

It is important to note that the VVSG Version 1 is an interim set of guidelines. The EAC is working with both the TGDC and NIST to create a redesigned VVSG (called VVSG Version 2) that will address a large range of issues including rewriting the requirements, if necessary, to make them more precise and testable and address key human factors and computer security issues. These new requirements will affect the basic design of voting systems to such a degree that these types of changes cannot reasonably be made and tested in time for the 2006 election cycle.

Brief History of Voting Systems Standards and Guidelines

In 1975, the National Bureau of Standards (now the National Institute of Standards and Technology) and the Office of the Federal Elections (the Office of Election Administration's predecessor at the General Accounting Office) produced a joint report, *Effective Use of Computing Technology in Vote Tallying.* This report concluded that a basic cause of computer-related election problems was the lack of appropriate technical skills at the state and local level to develop or implement sophisticated Standards against which voting system hardware and software could be tested. A subsequent Congressionally-authorized study produced by the FEC and the National Bureau of Standards detailed the need for a federal agency to develop national performance Standards that could be used as a tool by state and local election officials in the testing, certification, and procurement of computer-based voting systems.

In 1984, Congress appropriated funds for the FEC to develop voluntary national Standards for computer-based voting systems. The FEC formally approved the *Performance and Test Standards for Punchcard, Marksense and Direct Recording Electronic Voting Systems in* January 1990. This document is generally referred to as the *Voting Systems Standards,* or *1990 VSS.*

The national testing effort was developed and overseen by the National

Association of State Election Director's Voting Systems Board, which is composed of election officials and independent technical advisors. NASED's testing program was initiated in 1994 and more than 30 voting systems or components of voting systems have gone through the (NASED's) testing and qualification process. In addition, many systems have subsequently been certified at the state level using the Standards in conjunction with functional and technical requirements developed by state and local policymakers to address the specific needs of their jurisdictions.

As the qualification process matured and qualified systems were used in the field, the Voting Systems Board, in consultation with the testing labs, was able to identify 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 necessity for continued FEC involvement, citing the importance of keeping the Standards current in its reflection of modern and emerging technologies employed by voting system vendors. Following a Requirements Analysis released in 1999, the Commission authorized the Office of Election Administration to revise the Standards to reflect contemporary needs of the elections community. This resulted in the 2002 Voting Systems Standards.

In 2002, Congress passed HAVA, which created a new process for improving voluntary voting system guidelines. A new federal entity was created, the Election Assistance Commission, to oversee the process. The EAC established the Technical Guidelines Development Committee in accordance with the requirements of section 221 of HAVA pursuant to the Federal Advisory Committee Act, 5 U.S.C. App. 2. The TGDC's objectives and duties were to act in the public interest to assist the EAC in the development of the voluntary voting system guidelines. The membership, as defined by HAVA, includes:

- The Director of the National Institute of Standards and Technology (NIST) who shall serve as its chair,
- Members of the Standards Board,
- Members of the Board of Advisors,
- Members of the Architectural and Transportation Barrier, and Compliance Board (Access Board),
- A representative of the American National Standards Institute,
- A representative of the IEEE,
- Two representatives of the NASED selected by such Association who are not members of the Standards Board or Board of Advisors, and who are not of the same political party, and
- Other individuals with technical and scientific expertise relating to voting systems and voting equipment.

The TGDC first met in August, 2004 and delivered the Voluntary Voting System Guidelines in May, 2005. This initial set of recommendations augments the VSS–2002 by including security measures for auditability, wireless communications and software distribution and setup, and improvements to the accessibility and usability design sections of the VSS–2002. The TGDC also recommended that the VSS–2002 be replaced with a far-reaching guideline that would address in-depth security, performance-based guidelines for usability testing, and an overhaul of the standards and test methods to meet today's more rigorous needs for electronic voting systems.

Issues Addressed by the VVSG Version 1

The VVSG Version 1 adds or significantly changes eight technical topics of the VSS–2002. In addition, there are three organizational changes in the new sections. All other material remains the same.

Conformance Clause

The VSS–2002 did not include a conformance clause. One has been written and inserted as Section 1.7. The previous material in Section 1.7, the Outline, has been moved to 1.8.

Conformance is defined as the fulfillment by a product, process, or service of requirements as specified in a standard or specification. Conformance testing is the determination of whether an implementation (i.e., product, process, or service) faithfully satisfies the requirements and thus, conforms.

The conformance clause of a standard specification is a high-level description of what is required of implementers and developers. It, in turn, refers to other parts of the standard. The conformance clause may specify minimal requirements for certain functions and minimal requirements for implementation-dependent values. It may also specify the permissibility of extensions, options, and alternative approaches and how they are to be handled.

Human Factors

In the VSS–2002 Volume 1 Section 2.2.7 addressed Accessibility and Section 3.4.9 addressed Human Engineering—Controls and Displays. The VSS–2002 also contained Appendix C on Usability. The VVSG Version 1 replaces all of these items with a new Section 2.2.7 that addresses Human Factors including accessibility, usability, and limited English proficiency. This new sections incorporates the two NASED Technical Guides (Guide #1 and Guide #2). Future versions of the VVSG will contain performance-based requirements.

Security Overview and Appendix D

A new security section was added as Section 6.0. It contains four parts: an Overview and three topic areas. The overview was added to explain the VVSG approach to security. Future versions of the VVSG will require independent dual verification. There are many ways known today to achieve independent dual verification and more ways may be developed. Current methods include dual process systems, witness systems, cryptographic-based systems, optical scan systems, and paper audit trails. A new Appendix D expands on this overview with an in-depth discussion of independent dual verification systems. Independent dual verification is a new area in voting systems and it is expected to evolve significantly in VVSG Version 2. The Security Overview is an informative (non-normative) section of the VVSG Version 1. Requirements for voter verified paper audit trail systems, which are a type of independent dual verification system, are specified in a separate section. Version 2 of the VVSG will have complete requirements for at least three additional methods.

Voter Verified Paper Audit Trails

The VSS–2002 contained no requirements for voter verified paper audit trails. The VVSG Version 1 is providing requirements for voter verified paper audit trails (VVPAT) so that States that choose to implement VVPAT or States that are considering implementation can utilize these requirements to help ensure the effective operation of these systems. The EAC, TGDC, and NIST are taking no position with respect to the implementation of VVPAT systems and are neither requiring nor endorsing voter verified paper audit trails. Methods other than VVPAT can provide ways to achieve independent dual verification. These other methods are described in the Security Overview.

Wireless Technology

The TGDC concluded that the use of wireless technology introduces risk and

should be approached with caution. Therefore, the VVSG Version 1 includes a new section on wireless that augments the general telecommunications requirements in Volume 1, Section 5. in Section 5. The VVSG Version 1 requires that wireless transmissions be encrypted to protect against a variety of security problems.

Software Distribution and Setup Validation

The VSS–2002 contains many requirements to help voting officials validate the software and the setup of voting system software and hardware. Subsequent to the publication of the VSS–2002, the EAC invited all voting software vendors to submit their software to a national software repository maintained by NIST. This section of the VVSG Version 1 builds on the VSS–2002 to include use of this repository and other validation mechanisms.

Glossary

This glossary contains terms from the VSS–2002 as well as the inclusion of additional terms needed to understand voting and related areas such as security, human factors, and testing. Each term includes a definition and its source as well as an association as to the domain for which the term applies. Having a common set of terminology forms the basis for understanding requirements and for discussing improvements. The glossary is also available in a web-based on-line version at *http://www.nist.gov/votingglossary.*

Error Rates

Volume II, Appendix C addresses error rates. This appendix contains revised procedures to test that systems meet the indicated error rates. These apply to errors introduced by the system, defined as a ballot position error rate, and not by a voter's action. Further research on human interface and usability issues is needed to enable the development of Standards for error rates that account for human error.

There were concerns about the VSS–2002 Appendix regarding the numbers listed in the probability ratio sequential test (PRST) of the Mean Time Before Failure (MTBF) that (1) the numbers do not correspond to the numbers for the same table in the 1990 VSS, even though the stated assumptions do not change, and (2) the numbers from neither the 1990 nor the 2002 tables correspond to numbers that would result from standard PRST formulas listed in standard references such as the military handbook MIL–HDBK–781A. To address these concerns, the revised Appendix has replaced the numbers in the table with those that would indicated by the truncated PRST design from MIL–HDBK–781A with the corresponding parameters and made it more clear in the text that a truncated design was chosen. Using standard theoretical formulas leads to somewhat different numbers, but the revised Appendix C uses numbers from the MIL–HDBK–781A because they may be considered more standard and produce a less drastic change. Also, in the 1990 VSS, there was an appendix devoted to the definition and use of ''partial failures.'' This appendix was eliminated from the VSS–2002. The new version eliminated the paragraph and diagram in Appendix C that used partial failures.

The new version also includes statements reminding users to be cognizant of the assumptions involved in tests that use time-based exponential failure times and constant failure rates. Given the concerns that have been stated about appropriate testing times, note that the given table is appropriate only for the stated parameters, and that officials should assess the appropriateness of whatever parameters are used in testing.

Best Practices for Voting Officials

The VSS–2002 contained requirements for voting systems and for testing entities. However, requirements for human factors, wireless communications, VVPAT, software distribution and setup validation depend not only on voting systems providing specific capabilities but on voting officials developing and carrying out appropriate procedures. Consequently, the VVSG Version 1 contains Best Practices for voting officials. The new sections in VVSG Version 1 define each requirement as pertaining to voting systems, vendor repository, or test authorities, or voting officials. The requirements for voting officials are collected in Appendix C of Volume 1. (Appendix C had previously been Usability.)

Voting Process

The VSS–2002 defined three major stages of voting: pre-voting, voting, and post-voting. The stage for each requirement is marked in the new sections. The VVSG Version 2 will have a more detailed voting process model and will allow for finer granularity.

Summary of Content of Volume I

Volume I contains performance standards for electronic components of voting systems. In addition to containing a glossary (Appendix A), applicable references (Appendix B), Best Practices (Appendix C) and Security Overview (Appendix D). Volume I is divided into nine sections:

Section 1—Introduction: This section provides an introduction to the Standards, addressing the following topics:

- Objectives and usage of the Standards,
- Development history for initial Standards,
- Update of the Standards,
- Accessibility for individuals with disabilities,
- Definitions of key terms,
- Application of the Standards and test specifications,
- Conformance clause, and
- Outline of contents.

Section 2—Functional Capabilities: This section contains Standards detailing the functional capabilities required of a voting system. This section sets out precisely what it is that a voting system is required to do. This section also sets forth the minimum actions a voting system must be able to perform to be eligible for qualification. For organizational purposes, functional capabilities are categorized by the phase of election activity in which they are required:

- *Overall 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.
- *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 or ballot pages, the installation of ballots and ballot counting software (including firmware), and system and equipment tests.
- *Voting Capabilities:* These functional capabilities include all operations conducted at the polling place by voters and officials including the generation of status messages.
- *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.
- *Maintenance, Transportation and Storage Capabilities:* These capabilities are necessary to maintain, transport, and store voting system equipment.

For each functional capability, common standards are specified. In recognition of the diversity of voting

systems, some of the standards have additional requirements that apply only if the system incorporates certain functions (for example, voting systems employing telecommunications to transmit voting data) or configurations (for example, a central count component). Where system-specific standards are appropriate, common standards are followed by standards applicable to specific technologies (i.e., paper-based or DRE) or intended use (i.e., central or precinct count).

Section 3—Hardware Standards: This section describes the performance requirements, physical characteristics, and design, construction, and maintenance characteristics of the hardware and related components of a voting system. This section focuses on a broad range of devices used in the design and manufacture of voting systems, such as:

- For paper ballots: Printers, cards, boxes, transfer boxes, and readers,
- For electronic systems: Ballot displays, ballot recorders, precinct vote control units,
- For voting devices: Punching and marking devices and electronic recording devices,
- Voting booths and enclosures,
- Equipment used to prepare ballots, program elections, consolidate and report votes, and perform other elections management activities,
- Fixed servers and removable electronic data storage media, and
- Printers.

The Standards specify the minimum values for the relevant attributes of hardware, such as:

- Accuracy,
- Reliability,
- Stability under normal environmental operating conditions and when equipment is in storage and transit,
- Power requirements and ability to respond to interruptions of power supply,
- Susceptibility to interference from static electricity and magnetic fields,
- Product marking, and
- Safety.

Section 4—Software Standards: This section describes the design and performance characteristics of the software embodied in voting systems, addressing both system level software and voting system application software. The requirements of this section are intended to ensure that the overall objectives of accuracy, logical correctness, privacy, system integrity, and reliability are achieved. Although this section emphasizes software, the software standards may influence hardware design in some voting systems.

The requirements of this section apply to all software developed for use in voting systems, including:

- Software provided by the voting system vendor and its component suppliers, and
- Software furnished by an external provider where the software is potentially used in any way during voting system operation.

The general standards in this section apply to software used to support the broad range of voting system activities, including pre-voting, voting and post-voting activities. System specific Standards are defined for ballot counting, vote processing, the creation of an unalterable audit trail, and the generation of output reports and files. Voting system software is also subject to the security requirements of Section 6.

Section 5—Telecommunications Standards: This section describes the requirements for the telecommunications components of voting systems. Additionally, it defines the acceptable levels of performance against these characteristics. For the purpose of the Standards, telecommunications is defined as the capability to transmit and receive data electronically regardless of whether the transmission is localized within the polling place or the data is transmitted to a geographically distinct location. The requirements in this section represent functional and performance requirements for the transmission of data that are used to operate the system and report official election results. Where applicable, this section specifies minimum values for critical performance and functional attributes involving telecommunications hardware and software components.

This section addresses telecommunications hardware and software across a broad range of technologies such as dial-up communications technologies, high-speed telecommunications lines (public and private), cabling technologies, communications routers, modems, modem drivers, channel service units (CSU)/data service units (DSU), and dial-up networking applications software.

Additionally, this section applies to voting-related transmissions over public networks, such as those provided by regional telephone companies 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 data over public networks, this section applies to telecommunications components installed and operated at settings supervised by election officials, such as polling places or central offices.

Section 6—Security Standards: This section starts with an overview that provides a description of a new approach to securing voting systems called independent dual verification. The overview introduces the concept of independent dual verification and explains several approaches for achieving it. Appendix D further explores independent dual verification. Independent dual verification is not required in VVSG Version 1, but will be required in Version 2. Following the overview are 3 new sections describing requirements for voter verified paper audit trails, wireless technology and software distribution and setup. The remainder of the section is unchanged from VSS–2002 and describes the security capabilities for a voting system, encompassing the system's hardware, software, communications, and documentation. The requirements of this section recognize that no predefined set of security Standards will address and defeat all conceivable or theoretical threats. However, the Standards articulate requirements to achieve acceptable levels of integrity, reliability, and inviolability. Ultimately, the objectives of the security Standards for voting systems are to:

- Establish and maintain controls that can ensure that accidents, inadvertent mistakes, and errors are minimized,
- Protect the system from intentional manipulation and fraud,
- Protect the system from malicious mischief,
- Identify fraudulent or erroneous changes to the system, and
- Protect secrecy in the voting process.

These Standards 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, the Standards identify several types of risk that must be addressed, including:

- Unauthorized changes to system capabilities for defining ballot formats, casting and recording votes, calculating vote totals consistent with defined ballot formats, and reporting vote totals,
- Alteration of voting system audit trails,
- Altering a legitimately cast vote,
- Preventing the recording of a legitimately cast 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, to unauthorized individuals, and

• 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 cast by the voter.

Section 7—Quality Assurance: In the Standards, quality assurance is a vendor function with associated practices that confirms throughout the system development and maintenance life-cycle that a voting system conforms with the Standards and other requirements of state and local jurisdictions. Quality assurance focuses on building quality into a system and reducing dependence on system tests at the end of the life-cycle to detect deficiencies.

This section describes the responsibilities of the voting system vendor for designing and implementing a quality assurance program to ensure that the design, workmanship, and performance requirements of the Standards are achieved in all delivered systems and components. These responsibilities include:

• Development of procedures for identifying and procuring parts and raw materials of the requisite quality, and for their inspection, acceptance, and control.

• Documentation of hardware and software development processes.

• Identification and enforcement of all requirements for in-process inspection and testing that the manufacturer deems necessary to ensure proper fabrication and assembly of hardware, as well as installation and operation of software or firmware.

• Procedures for maintaining all data and records required to document and verify the quality inspections and tests.

Section 8—Configuration Management: This section contains specific requirements for configuration management of voting systems. For the purposes of the Standards, configuration management is defined as a set of activities and associated practices that assures full knowledge and control of the components of a system, beginning with its initial development, progressing throughout its development and construction, and continuing with its ongoing maintenance and enhancement. This section describes activities in terms of their purpose and outcomes. It does not describe specific procedures or steps to be employed to accomplish them—these are left to the vendor to select.

The requirements of this section address a broad set of record keeping, audit, and reporting activities that include:

• Identifying discrete system components,

• Creating records of formal baselines of all components,

• Creating records of later versions of components,

• Controlling changes made to the system and its components,

• Submitting new versions of the system to Independent Test Authorities (ITA)s,

• Releasing new versions of the system to customers,

• Auditing the system, including its documentation, against configuration management records,

• Controlling interfaces to other systems, and

• Identifying tools used to build and maintain the system.

Vendors are required to submit documentation of these procedures to the ITA as part of the Technical Data Package for system qualification testing. Additionally, as articulated in state or local election laws, regulations, or contractual agreements with vendors, authorized election officials or their representatives reserve the right to inspect vendor facilities and operations to determine conformance with the vendor's reported configuration management procedures.

Section 9—Overview of Qualification Tests: This section provides an overview for the qualification testing of voting systems. Qualification testing is the process by which a voting system is shown to comply with the requirements of the Standards and the requirements of its own design and performance specifications. 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 qualification test process is intended to discover errors that, should they occur in actual election use, could result in failure to complete election operations in a satisfactory manner. This section describes the scope of qualification testing, its applicability to voting system components, documentation that is must be submitted by the vendor, and the flow of the test process. This section also describes differences between the test process for initial qualification testing of a system and the testing for modifications and re-qualification after a qualified system has been modified.

Since 1994, the testing described in this section has been performed by an ITA that is certified by NASED. For the future, HAVA provides for EAC-accredited testing authorities. HAVA tasks the Director of NIST to assist the EAC by recommending laboratories for EAC accreditation. NIST's National Voluntary Laboratory Accreditation Program (NVLAP) is developing a program to evaluate competent laboratories. While laboratories are being evaluated for recommendation by the Director, testing will continue to be done by the ITAs previously certified by NASED. The testing may be conducted by one or more ITAs for a given system, depending on the nature of tests to be conducted and the expertise of the certified ITA. The testing process involves the assessment of, but is not limited to:

• Absolute correctness of all ballot processing software, for which no margin for error exists,

• Operational accuracy in the recording and processing of voting data, as measured by the error rate articulated in Volume I, Section 3,

• Operational failure 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, and

• Completeness and accuracy of the system documentation and configuration management records to enable purchasing jurisdictions to effectively install, test, and operate the system.

Summary of Volume II Content

Section 1—Introduction: This section provides an overview of Volume II, addressing the following topics:

• Objectives of Volume II,

• General contents of Volume II,

• Qualification testing focus,

• Qualification testing sequence,

• Evolution of testing, and

• Outline of contents.

Section 2—Technical Data Package: This section contains a description of vendor documentation relating to the voting system that shall be submitted with the system as a precondition for qualification testing. These items are necessary to define the product and its method of operation; to provide the vendor's technical and test data supporting the its claims of the system's functional capabilities and performance levels; and to document instructions and procedures governing system operation and field maintenance. The content of the Technical Data Package (TDP) shall contain a complete description of the following information about the system:

- Overall system design, including subsystems, modules, and interfaces,
- Specific functional capabilities,
- Performance and design specifications,
- Design constraints and compatibility requirements,
- Personnel, equipment, and facilities necessary for system operation, maintenance, and logistical support,
- Vendor practices for assuring system quality during the system's development and subsequent maintenance, and
- Vendor practices for managing the configuration of the system during development and for modifications to the system throughout its life-cycle.

Section 3—Functionality Testing: This section contains a description of the testing to be performed by the ITA to confirm the functional capabilities of a voting system submitted for qualification testing. It describes the scope and basis for functional testing, the general sequence of tests within the overall test process, and provides guidance on testing for accessibility. It also discusses testing of functionality of systems that operate on personal computers.

Section 4—Hardware Testing: This section contains a description of the testing to be performed by the ITAs to confirm the proper functioning of the hardware components of a voting system submitted for qualification testing. This section requires ITAs to design and perform procedures that test the voting system hardware for both operating and non-operating environmental 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 test laboratory or shop environment. The non-operating tests are intended to evaluate the ability of the system hardware to withstand exposure to various environmental conditions incidental to voting system storage, maintenance, and transportation. The procedures are based on test methods contained in Military Standards (MIL–STD) 810D, 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 ensures that the hardware meets or exceeds the minimum requirements for reliability, data reading, and processing accuracy contained in Section 3 of Volume I. Although 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 has in most cases been reduced from that specified in the Military Standards to reflect commercial, rather than military, practice.

Section 5—Software Testing: This section contains a description of the testing to be performed by the ITAs to confirm the proper functioning of the software components of a voting system submitted for qualification testing. It describes the scope and basis for software testing, the initial review of documentation to support software testing, and the review of voting system source code.

The software qualification tests encompass a number of interrelated examinations. The examinations include selective review of source code for conformance with the vendor's stated standards, and other system documentation provided by the vendor. The code inspection is complemented by a series of functional tests to verify the proper performance of all system functions controlled by the software.

Section 6—System Level Integration Testing: This section contains a description of the testing conducted by the ITAs to confirm the proper functioning of the fully integrated components of a voting system submitted for qualification testing. It describes the scope and basis for integration testing, testing of internal and external system interfaces, testing of security capabilities, testing of accessibility features, and the configuration audits, including the evaluation of claims made in the system documentation.

System-level qualification tests address the integrated operation of hardware, software and telecommunications capabilities (where applicable) to assess the system's response to a range of both normal and abnormal conditions in an attempt to compromise the system.

Section 7—Examination of Vendor Practices for Configuration Management and Quality Assurance: This section contains a description of examinations conducted by the ITAs to evaluate the extent to which vendors meet the requirements for configuration management and quality assurance. It describes the scope and basis for the examinations and the general sequence of the examinations. It also provides guidance on the substantive focus of the examinations.

In reviewing configuration management practices, the ITAs examine the vendor's:

- Configuration management policy,
- Configuration identification policy,
- Baseline, promotion and demotion procedures,
- Configuration control procedures,
- Release process and procedures, and
- Configuration audit procedures.

In reviewing quality assurance practices, the ITAs examine the vendor's:

- Quality assurance policy,
- Parts and materials tests and examinations,
- Quality conformance plans, procedures and inspection results, and
- Voting system documentation.

Volume I, Section 1

Table of Contents

Introduction

1.1 Objectives and Usage of the Voting System Standards

State and local officials today are confronted with increasingly complex voting system technology and an increased risk of voting system failure. Responding to calls for assistance from the states, the United States Congress authorized the Federal Election Commission (FEC) to develop voluntary national voting systems standards for computer-based systems. The resulting FEC Voting System Standards (''the

Standards'') seek to aid state and local election officials in ensuring that new voting systems are designed to function accurately and reliably, thus ensuring the system's integrity. States are free to adopt the Standards in whole or in part. States may also choose to enact stricter performance requirements for systems used in their jurisdictions.

The Standards specify minimum functional requirements, performance characteristics, documentation requirements, and test evaluation criteria. For the most part, the Standards address what a voting system should reliably do, not how system components should be configured to meet these requirements. It is not the intent of the Standards to impede the design and development of new, innovative equipment by vendors. Furthermore, the Standards balance risk and cost by requiring voting systems to have essential, but not excessive, capabilities.

The Standards are not intended to define appropriate election administration practices. However, the total integrity of the election process can only be ensured if implementation of the Standards is coupled with effective election administration practices.

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

- Authorities responsible for the analysis and testing of such systems in support of qualification and/or certification of systems for purchase within a designated jurisdiction;
- State and local agencies evaluating voting systems to be procured within their jurisdictions; and
- Designers and manufacturers of voting systems.

1.2 Development History for Initial Standards

Much of the groundwork for the Standards' development was laid by a national study conducted in 1975 by the National Bureau of Standards, now known as the National Institute of Standards and Technology (NIST). This study was requested by the FEC's Office of Election Administrator's predecessor, the Office of Federal Elections of the General Accounting Office. The report, ''*Effective Use of Computing Technology in Vote-Tallying*,'' made a number of recommendations bearing directly on the Standards project. After analyzing computer-related election problems encountered in the past, the report concluded that one of the basic causes for these difficulties was the lack of appropriate technical skill at the state and local level for developing or implementing sophisticated and complex standards against which voting system hardware and software could be tested.

Following the release of this report, Congress mandated that the FEC, with the cooperation and assistance of the National Bureau of Standards, study and report on the feasibility of developing ''voluntary engineering and procedural performance standards for voting systems used in the United States.'' (2 U.S.C. 431 Note) The resulting 1983 study cited a substantial number of technical and managerial problems that affected the integrity of the vote counting process. It also asserted the need for a federal agency to develop national performance standards that could be used as a tool by state and local election officials in the testing, certification, and procurement of computer-based voting systems. In 1984, Congress approved initial funding for the Standards.

The FEC held a series of public hearings in developing the initial Standards. State and local election officials, election system vendors, technical consultants, and others reviewed drafts of the proposed criteria. The FEC considered their many comments and made appropriate revisions. Before final issuance, the FEC publicly announced the availability of the latest draft of the Standards in the **Federal Register** and requested that all interested parties submit final comments. The FEC meticulously reviewed all responses to the notice and incorporated corrections and suitable suggestions. Ultimately, the final product was the result of considerable deliberation, close consultation with election officials, and careful consideration of comments from all interested parties.

In January 1990, the FEC issued the performance standards and testing procedures for punchcard, marksense, and direct recording electronic (DRE) voting systems. The 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 is covered by the Standards.

1.3 Update of the Standards

Today, over two-thirds of the States have adopted the Standards in whole or in part. As a result, the voting systems marketed today are dramatically improved. Election officials are better assured that the voting systems they procure will work accurately and reliably. Voting system failures are declining and now primarily involve pre-Standard equipment, untested equipment configurations, or the mismanagement of tested equipment. Overall, systems integrity and the election processes have improved markedly.

However, advances in voting technology, legislative changes, and the proliferation of electronic voting systems make an update of the Standards necessary. The industry has been marked by widespread integration of personal computer technology and non-mainframe servers into DRE voting systems.

In addition, voting systems need to be responsive to the Americans with Disabilities Act (ADA) of 1990 and guidelines developed to assist in implementing the ADA.

1.4 Accessibility for Individuals With Disabilities

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 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 designed to meet the diverse needs of voters with a broad range of disabilities. The FEC has adopted the entirety of the Access Board's recommendations and incorporated them into the Standards. These recommendations comprise the bulk of the accessibility provisions found in Section 2.2.7. Implementing these provisions, however, will not entirely eliminate the need to accommodate the needs of some disabled voters by human interface.

The FEC anticipates that during the lifetime of this version of the Standards increased obligations will be placed upon election officials at every jurisdictional level to provide voting equipment tailored to meet the needs of voters with disabilities. To facilitate jurisdictions in meeting accessibility needs, the Standards mandate that every voting system incorporate some accessible voting capabilities. The

Standards also mandate that systems incorporating a DRE component meet specific technological requirements. To do so, it is anticipated that a vendor will have to either configure all of the system's voting stations to meet the accessibility specifications or will have to design a unique station that conforms to the accessibility requirements and is part of the overall voting system configuration.

Under no circumstances should compliance with requirements for accessibility be viewed as mutually exclusive from compliance with any other provision of the Standards. If a voting system contains a machine uniquely designed to meet the accessibility requirements, such a machine will be tested for compliance with the accessibility requirements, as well as for compliance with all of the DRE standards, in order to ensure that an accessible machine does not unintentionally abrogate the mandates of the Standards.

1.5 Definitions

The Standards contain terms describing function, design, documentation, and testing attributes of equipment and computer programs. 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, and a glossary of those terms is contained in Appendix A. Nontechnical terms not listed in Appendix A shall be interpreted according to their standard dictionary definitions.

Additionally, the following terms are defined below:

- Voting system;
- Paper-based voting system;
- Direct record electronic (DRE) voting system;
- Public network direct record electronic (DRE) voting system;
- Precinct count voting system; and
- Central count voting system.

1.5.1 Voting System

A voting system is a combination of mechanical, electromechanical, or electronic equipment. It includes the software required to program, control, and support the equipment that is used to define ballots; to cast and count votes; to report and/or display election results; and to maintain and produce all audit trail information. A voting system may also include the transmission of results over telecommunication networks.

Additionally, a voting system includes the associated documentation used to operate the system, maintain the system, identify system components and their versions, test the system during its development and maintenance, maintain records of system errors and defects, and determine specific changes made after system qualification. By definition, this includes all documentation required in Section 9.4.

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. However, the Standards recognize that as the industry develops unique solutions to various challenges and as voting systems become more responsive to the needs of election officials and voters, the rigid dichotomies between voting system types may be blurred. Innovations that use a fluid understanding of system types can greatly improve the voting system industry, but only if controls are in place to monitor and control integrity through the proper evaluation of the system brought for qualification.

As such, vendors that submit a system that integrates components from more than one traditional system type or a system that includes components not addressed in this Standard shall submit the results of all beta tests of the new system. Vendors also shall submit a proposed test plan to the appropriate independent test authority recognized by the National Association of State Election Directors (NASED) to conduct national qualification testing of voting systems. The Standards permit vendors to produce or utilize interoperable components of a voting system that are tested within the full voting system configuration.

1.5.2 Paper-Based Voting System

A Paper-Based Voting System, (referred to in the initial Standards as a Punchcard and Marksense [P&M] Voting System) records votes, counts votes, and produces a tabulation of the vote count from votes cast on paper cards or sheets. A punchcard voting system allows a voter to record votes by means of holes punched in designated voting response locations. A marksense voting system allows a voter to record votes by means of marks made by the voter directly on the ballot, usually in voting response locations. Additionally, a paper based system may record votes using other approaches whereby the voter's selections are 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 voters selections.

1.5.3 Direct Record Electronic (DRE) Voting System

A Direct Record 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.

1.5.4 Public Network Direct Record Electronic (DRE) Voting System

A Public Network Direct Record Electronic (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 as defined in Section 5.1.2. 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 Standards, 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 discussed in Section 5 and 6 apply.

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.

1.5.5 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 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.

1.5.6 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 place. The systems produce a printed report of the vote count, and may produce a report stored on electronic media.

1.6 Application of the Standards and Test Specifications

The Standards apply 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 results;
- Display results on-site or remotely; and
- Maintain and produce all audit trail information.

In general, the Standards define functional requirements and performance characteristics that can be assessed by a series of defined tests. Standards are mandatory requirements and are designated by use of the term ''shall.''

Some voting systems use one or more readily available commercial off-the-shelf (COTS) devices (such as card readers, printers, or personal computers) or software products (such as operating systems, programming language compilers, or database management systems). COTS devices and software are exempted from certain portions of the qualification testing process as defined herein, as long as such products are not modified for use in a voting system.

Generally, voting systems are subject to the following three testing phases prior to being purchased or leased:

- Qualification tests;
- State certification tests; and
- State and/or local acceptance tests.

1.6.1 Qualification Tests

Qualification tests validate that a voting system meets the requirements of the Standards and performs according to the vendor's specifications for the system. Such 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. Qualification tests address individual system components or elements, as well as the integrated system as a whole.

Since 1994, qualification tests for voting systems have been performed by Independent Test Authorities (ITAs) certified by the National Association of State Election Directors (NASED). NASED has certified an ITA for either the full scope of qualification testing or a distinct subset of the total scope of testing. To date, ITAs have been certified only for distinct subsets of testing. Upon the successful completion of testing by an ITA, the ITA issues a Qualification Test Report to the vendor and NASED. The qualification test report remains valid for as long as the voting system remains unchanged.

Upon receipt of test reports that address the full scope of testing, NASED issues a Qualification Number that indicates the system has been tested by certified ITAs for compliance with the Standards and qualifies for the certification process of states that have adopted the Standards. The Qualification Number applies to the system as a whole, and does not apply to individual system components or untested configurations.

After a system has completed qualification testing, further examination of a 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 appropriate ITA based on the nature and scope of changes made and the scope of the ITA's role in NASED qualification. The ITA will determine the extent to which the modified system should be resubmitted for qualification testing and the extent of testing to be conducted.

Generally, a voting system remains qualified under the standards against which it was tested, as long as no modifications not approved by an ITA are made to the system. However, if a new threat to a particular voting system is discovered, it is the prerogative of NASED to determine which qualified voting systems are vulnerable, whether those systems need to be retested, and the specific tests to be conducted. In addition, when new standards supersede the standards under which the system was qualified, it is the prerogative of NASED to determine when systems that were qualified under the earlier standards will lose their qualification, unless they are tested to meet current standards.

Among other things, qualification testing complements and evaluates the vendor's developmental testing and beta testing. The ITA 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 Standards as well as the system's performance specifications. The ITA 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 qualification 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.

1.6.2 Certification Tests

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 qualified through the Standards;
- 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; and
- Define acceptance tests.

Precise certification test scripts are not included in the Standards, 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 qualification 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, 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

Standards. By design, the Standards, and qualification testing of voting systems for compliance with the Standards, do not address these additional requirements. However, qualification testing addresses all capabilities of a voting system stated by the vendor in the system documentation submitted to an ITA, including additional capabilities that are not required by the Standards.

1.6.3 Acceptance Tests

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 qualified by NASED 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 qualification and certification tests; and
- Establish a baseline for any future required audits of the system.

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

1.7 Conformance Clause

1.7.1 Scope and Applicability

The Voluntary Voting System Guidelines (VVSG) define requirements for conformance of voting systems. Conformance is defined in terms of requirements that voting system vendors claiming conformance to these Guidelines shall meet. The VVSG also provides the framework, procedures, and requirements that testing authorities responsible for the qualification of voting systems shall follow in order to qualify a voting system for EAC certification. The requirements and procedures in the VVSG may also be used by States to certify voting systems. To ensure that correct voting system software has been distributed without modification, the VVSG includes requirements for a national software repository. Finally, the VVSG provides guidance in the form of best practices to voting officials. These best practices are not mandated and are not subject to testing by testing authorities to qualify voting systems. They are provided as adjuncts to the technical requirements for voting systems in order to ensure the integrity of the voting process and to assist States in properly setting up, deploying, and operating voting systems.

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

1. Designers and manufacturers of voting systems,
2. Testing authorities responsible for the analysis and testing of voting systems in support of qualification of systems for purchase within a designated jurisdiction,
3. National software repositories, either maintained by the National Institute of Standard and Technology (NIST) or other EAC designated repository,
4. (Optionally) Voting officials, including election judges, poll workers, ballot designers and officials responsible for the installation, operation, and maintenance of voting machines, and
5. (Optionally) testing authorities responsible for the State certification of voting systems.

Minimum requirements specified in these guidelines include:

- Functional requirements,
- Performance characteristics,
- Documentation requirements,
- Test evaluation criteria, and
- Procedural requirements.

1.7.2 Conformance Framework

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

1.7.2.1 Applicable Entities

The requirements, prohibitions, options, and guidance specified in these guidelines apply to voting systems, voting system vendors, testing authorities, and repositories.

In general, requirements for designers and manufacturers of voting systems in these guidelines apply to all voting systems, unless prefaced with explanatory narrative describing unique applicability. Other terms in these guidelines shall be construed as synonymous with ''all voting systems.'' They are:

- ''all systems,''
- ''systems,''
- ''the system,''
- ''the voting system,'' and
- ''each voting system.''

The term ''voting system vendor'' imposes documentation or testing requirements on voting systems, via 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 testing authorities are indicated by referring to Independent Testing Authority (ITA) and EAC accredited testing authority. Under HAVA, ITAs have been replaced by EAC accredited testing authorities. In these guidelines, EAC accredited testing authority and ITA shall be considered equivalent. In addition, the National Association of State Election Directors (NASED) activities specified in these guidelines shall be performed by the Election Assistance Commission (EAC).

The term ''repository'' will be used to designate requirements levied on the national software repository maintained at NIST or any other EAC designated repository. The repository maintained at NIST is called the National Software Reference Library (NSRL).

Guidance and best practices for voting officials are indicated by the notation ''*Best Practices for Voting Officials*'' preceding the best practice statement.

1.7.2.2 Relationship Among Entities

Although conformance is defined for voting systems, it is the voting system vendor that needs to implement these requirements and provide the necessary documentation with the system. In order to claim conformance to the Voluntary Voting Systems Guidelines, the voting system vendor shall satisfy the minimum requirements specified in the VVSG, including implementation of functionality, prescribed software coding and assurance practices, and preparation of the Technical Data Package (TDP). In order to claim that a voting system is qualified, the voting system vendor shall satisfy the requirements for qualification testing and successfully complete the test campaign with an ITA/testing authority.

An ITA/EAC accredited test authority shall satisfy the requirements for conducting qualification testing. The ITA/EAC accredited test authority may use an operational environment that is derived from the VVSG best practice guidelines for voting 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 voting system vendor's documentation and as specified by the VVSG. Additionally, the ITA/EAC accredited test authority shall coordinate and deliver the requisite documentation to the EAC and copies of voting system software to the repository. Note that in the VVSG, these

requirements and the relationship between the ITA/EAC accredited test authority and the certification authority is with NASED, not the EAC.

The EAC is assuming the responsibility for certification of voting systems from NASED.

The VVSG provides guidance denoted as ''Best Practices for Voting Officials.'' This guidance may be used to allow jurisdictions to incorporate appropriate procedures to help ensure that their voting systems are reliable, accessible, usable, and secure. Furthermore, this guidance may be used in training and incorporated into written procedures for properly conducting the election and operating voting systems.

Figure 1 provides an illustration of these relationships.

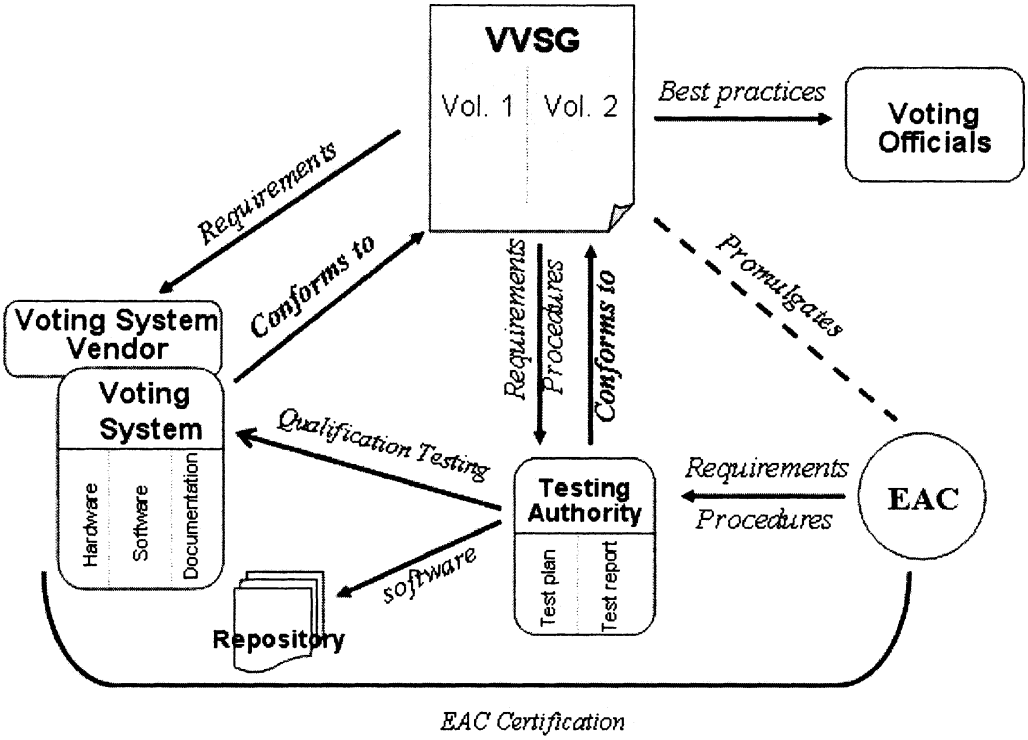


Figure 1 Relationship between entities

1.7.2.3 Structure of Requirements

Sections of this document that augment the VSS–2002, by either replacing VSS–2002 sections or adding new sections, are indicated by line numbers, footer information (i.e., New Material, date, etc.) at the bottom of pages with new material, and hierarchically structured requirements. Each requirement is numbered according to a hierarchical scheme in which higher-level requirements (such as ''provide accessibility for blind voters'') are supported by lower-level requirements (''provide an audio-tactile interface''). Thus, requirements are contained (i.e., nested) within other requirements. A nested requirement or lower-level requirement is a 'child' to its 'parent' or higher-level requirement.

Some of these 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, children requirements are testable, and (2) they often provide the structure and rationale for the lower-level requirements. Satisfying the lower-level requirement will result in satisfying its higher-level 'parent' requirement.

1.7.2.4 Conformance Designations

A voting system conforms if all the mandatory requirements that apply to the voting system are fulfilled. An implementation statement (see Section 1.7.6) or similar mechanism is used to describe the capabilities, features and optional functions that have been implemented and are subject to conformance and qualification testing. There is no concept of partial conformance, *e.g.*, a voting system is 80% conforming.

1.7.3 Normative Language

The following keywords are used to convey conformance requirements.

- *Shall*—to indicate a mandatory requirement to be followed (implemented) in order to conform. Synonymous with ''is required to.''
- *Is prohibited*—to indicate a mandatory requirement that indicates something that is not permitted (allowed), in order to conform. Synonymous with ''shall not.''
- *Should, Is encouraged*—to indicate an optional recommended action, one that is particularly suitable, without mentioning or excluding others. Synonymous with ''is permitted and recommended.''
- *May*—to indicate an optional, permissible action. Synonymous with ''is permitted.''

Normative text is directly applicable to achieving conformance to this document. Informative parts of this document include examples, extended explanations, and other matter that contain information necessary for proper understanding of the VVSG and conformance to it. Some sections in the VSSG have narrative text prefixed by the keywords: Discussion or Best Practices for Voting Officials. This text is informative and has no bearing on conformance.

1.7.4 Categorizing Requirements

In addition to defining a common set of requirements that apply to all voting systems, the VVSG categorizes some requirements into related groups of functionality to address equipment type, ballot tabulation location, and voting system component (*e.g.*, election management system). Hence, not all requirements apply to all voting systems. Specifically, if a category is not applicable to a voting system, then the requirements in that category are not applicable. For example, requirements categorized as ''DRE Systems'' (as in Volume I, Section 2.4.9) are not applicable to paper-based voting systems and thus are ignored by paper-based 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 Direct Record Electronic (DRE) Voting Systems. Additionally, voting systems are further categorized, in these guidelines, 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 VVSG defines specific requirements for systems that fall within these four categories as well as various combinations of these categories.

Other categories for which requirements are defined include: election management systems (EMS), methods of independent verification, and telecommunication components.

1.7.5 Extensions

Extensions are additional functions, features, and/or capabilities included in a voting system that are not required by the VVSG. To accommodate the needs of States that may impose additional requirements beyond those listed in these guidelines and to accommodate changes in technology, these guidelines allow extensions. Thus, a voting system may include extensions and still be conformant to the VVSG. The use of extensions shall not contradict nor cause the nonconformance of functionality defined in the VVSG.

1.7.6 Implementation Statement

An implementation statement provides information about a voting system, by documenting the requirements that have been implemented by the voting system. It can also be used to highlight optional features and capabilities supported by the voting system, as well as to document any extensions (*i.e.*, additional functionality beyond what is required in the standard). An implementation statement may take the form of a checklist, to be completed for each voting system for which a claim of conformance to the VVSG or subset of the VVSG is desired.

An implementation statement provides a concise summary and a quick overview of requirements that have been implemented. The implementation statement may also be used to identify the subset of a test suite that would be applicable to the voting system being tested.

If an implementation statement is provided, it shall include identifying information about the voting system, including at a minimum versioning and date information. Additionally, a narrative description of the voting system shall be included in the implementation statement.

1.8 Outline of Contents

The organization of the Standards has been simplified to facilitate its use. *Volume I, Voting System Performance Standards,* is intended for use by the broadest audience, including voting system developers, equipment manufacturers and suppliers, independent test authorities, local agencies that purchase and deploy voting systems, state organizations that certify a system prior to procurement by a local jurisdiction, and public interest organizations that have an interest in voting systems and voting systems standards.

- Section 2 describes the functional capabilities required of voting systems.
- Sections 3 through 6 describe specific performance standards for election system hardware, software, telecommunications and security, respectively.
- Sections 7 and 8 describe practices for quality assurance and configuration management, respectively, to be used by vendors, and required information about vendor practices that will be reviewed in concert with system qualification and certification test processes and system purchase decisions.
- Section 9 provides an overview of the test and measurement process used by test authorities for qualification and re-qualification of voting systems.
- Appendix A provides a glossary of important terms used in Volume I.
- Appendix B lists the publications that were used for guidance in the preparation of the Standards. These publications contain information that is useful in interpreting and complying with the requirements of the Standards.
- Appendix C addresses issues of usability of voting systems, commonly referred to as ''human factors.'' This appendix does not represent mandates that voting systems will be tested against, but rather contain recommendations and best practices on usability issues designed to provide vendors and election officials with guidance on designing and procuring systems that are easy and intuitive to use by voters.

Volume II, Voting System Qualification Testing Standards describes the standards for the technical information submitted by the vendor to support testing; the development of test plans by the ITA for initial system testing and testing of system modifications; the conduct of system qualification tests by the ITA; and the test reports generated by the ITA. This volume complements the content of Volume I and is intended primarily for use by ITAs, state organizations that certify a system, and vendors.

Volume I, Section 2

Table of Contents

Functional Capabilities

2.1 Scope

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

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

♦ *Overall 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.

♦ *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 or ballot pages, the installation of ballots and ballot counting software (including firmware), and system and equipment tests.

♦ *Voting Capabilities:* These functional capabilities include all operations conducted at the polling place by voters and officials including the generation of status messages.

♦ *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.

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

2.2 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:

- Security;
- Accuracy;
- Error recovery;
- Integrity;
- System auditability;
- Election management system;
- Accessibility:
- Vote tabulating;
- Ballot counters; and
- Data Retention.

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

2.2.1 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 to protect against tampering during system repair, or interventions in system operations, in response to system failure.

e. Provide security provisions that are compatible with the procedures and administrative tasks involved in equipment preparation, testing, and operation.

f. If access to a system function is to be restricted or controlled, the system shall incorporate a means of implementing this capability.

g. Provide documentation of mandatory administrative procedures for effective system security.

2.2.2 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 3 provides additional information on susceptibility requirements.

2.2.2.1 Common Standards

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 be able to 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; and

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.

2.2.2.2 DRE System Standards

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.

2.2.3 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; and

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.

2.2.4 Integrity

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

2.2.4.1 Common Standards

To ensure system integrity, all systems shall:

a. Protect, by a means compatible with these Standards, against a single point of failure that would prevent further voting at the polling place;

b. Protect against the interruption of electronic 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; and

j. Include built-in measurement, self-test, and diagnostic software and hardware for detecting and reporting the system's status and degree of operability.

2.2.4.2 DRE Systems Standards

In addition to the common standards, DRE systems shall:

a. 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; and

b. Provide a capability to retrieve ballot images in a form readable by humans.

2.2.5 System Audit

This section describes the context and purpose of voting system audits and sets forth specific functional requirements. Additional technical audit requirements are set forth in Section 4.

2.2.5.1 System Audit Purpose and Context

Election audit trails provide the supporting documentation for verifying the correctness 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.

The following audit trail 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 sections 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 4 of the Standards.

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 that ITAs 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 (TDP).

Documentation of items such as paper ballots delivered and 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. Future volumes of the Standards will address these and other system operations practices. In the interim, useful guidance is provided by the *Innovations in Election Administration #10, Ballot Security and Accountability,* available from the FEC's Office of Election Administration.

2.2.5.2 Operational Requirements

Audit records shall be prepared for all phases of elections 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 in the following sections.

2.2.5.2.1 Time, Sequence, and Preservation of Audit Records

The timing and sequence of audit record entries is as important as the data contained in the record. All voting systems shall meet the following requirements for time, sequence and preservation of audit records:

a. 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.

b. 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.

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

d. 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.

e. 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.

f. 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.

g. 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:

(1) The generation of audit trail records does not interfere with the production of output reports;

(2) The entries can be identified so as to facilitate their recognition, segregation, and retention; and

(3) The audit record entries are kept physically secure.

2.2.5.2.2 Error Messages

All voting systems shall meet the following requirements for error messages:

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

b. All error messages requiring intervention by an operator or precinct official shall be displayed or printed unambiguously in easily understood language text, or by means of other suitable visual indicators;

c. When the 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 unit device. This is intended to reduce inappropriate reactions to error conditions, and to allow for ready and effective problem correction;

d. All error messages for which correction impacts vote recording or vote processing shall be written in a manner that is understandable to an election official who possesses training on system use and operation, but does not possess technical training on system servicing and repair;

e. The message cue for all systems shall clearly state the action to be performed in the event that voter or operator response is required;

f. System design shall ensure that erroneous responses will not lead to irreversible error; and

g. Nested error conditions shall be corrected in a controlled sequence such that system status shall be restored to the initial state existing before the first error occurred.

2.2.5.2.3 Status Messages

The Standards 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 system shall display and report critical status messages using unambiguous indicators or English language text. The system need not display non-critical status messages at the time of occurrence. 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.

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

2.2.5.3 COTS General Purpose Computer System Requirements

Further requirements must be applied to COTS 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 (or ''PCs''), including the many varieties of UNIX and Linux, and those offered by Microsoft and Apple. Election software running on these COTS 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.

2.2.6 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:

a. Define political subdivision boundaries and multiple election districts as indicated in the system documentation;

b. Identify contests, candidates, and issues

c. Define ballot formats and appropriate voting options;

d. Generate ballots and election-specific programs for vote recording and vote counting equipment;

e. Install ballots and election-specific programs;

f. Test that ballots and programs have been properly prepared and installed;

g. Accumulate vote totals at multiple reporting levels as indicated in the system documentation;

h. Generate the post-voting reports required by Section 2.5; and

i. Process and produce audit reports of the data indicated in Section 4.5.

2.2.7 Human Factors

The importance of human factors 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 special difficulties in 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 race or decide on abstrusely worded referenda.
- Voting is performed infrequently, so learning and familiarity are lower than for more frequent tasks, such as use of an ATM.
- Jurisdictions may change voting equipment, thus obviating whatever familiarity the voter might have acquired.
- Once the voting session has been completed by the voter, there is never a chance for later correction.
- Voting must be accessible to all eligible citizens, whatever their age, physical abilities, language skills, or experience with technology.

The challenge, then, is to provide a voting system and voting environment that all voters can use comfortably, efficiently, and with justified

confidence that they have cast their votes correctly. The requirements within this section are intended to serve that goal.

Although there are many detailed requirements, three broad principles motivate this section on human factors:

1. All Eligible and Potentially Eligible Voters Shall Have Access to the Voting Process Without Discrimination.

The voting process shall allow eligible voters of whatever age, condition, or background to be able to go through the entire voting process with the same degree of independence, privacy, and confidence, insofar as technology will allow. Note that the voting process includes access to the polling place, instructions on how to vote, initiating the voting session, choosing candidates, getting help as needed, review of the ballot, VVPAT, if applicable, and final submission of the ballot.

2. Each Cast Ballot Shall Capture the Intent of the Voter Who Cast That Ballot.

Voters have the right to have the ballot presented to them in a manner that is clear and usable. Voters should encounter no difficulty or confusion in recording their choices.

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, with or 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. The process must also preclude the voter from disclosing the content of the ballot to anyone else.

All the requirements within Section 2.2.7 have the purpose of improving the quality of interaction between voters and voting systems.

- Requirements that are likely to be relevant only to those with some disability are listed under Section 2.2.7.1, although they may also assist those not usually described as having a disability, e.g. voters with poor eyesight or somewhat limited dexterity.
- Requirements that are likely to be relevant only to those with limited English proficiency are listed in Section 2.2.7.2.
- Finally, requirements for general usability make up Section 2.2.7.3 and those for privacy, Section 2.2.7.4.

Certain abbreviations and terms are used extensively throughout Section 2.2.7:

- CIF: Common Industry Format: Refers to the format described in ANSI/INCITS 354–2001 ''Common Industry Format (CIF) for Usability Test Reports.''
- Acc-VS: Accessible Voting Station—the voting station equipped for individuals with disabilities referred to in HAVA 301(a)(3)(B).
- ATI: Audio-Tactile Interface—a voter interface designed so as 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.
- ALVS: Alternative Language Voting Station—a voting station designed to be usable by voters who have limited English proficiency.

This section also uses common terms as defined in the updated Glossary. Note in particular, the distinctions among ''voting system,'' ''voting station,'' and ''voting process.''

1. 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 Station So Equipped Is Referred to Herein as an Accessible Voting Station (Acc-VS)

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 within Section 2.2.7.1 are intended to address this mandate. Ideally every voter would be able to vote independently and privately. As a practical matter, there may be a small number of voters whose disabilities are so severe that they will need personal assistance. Nonetheless, the requirements of this section are meant to make the voting system directly accessible to as many voters as possible.

Note that this section does not replace requirements of other sections, but adds to them. In particular, the requirements of Section 2.2.7.3 on usability apply either to all voting stations or, in some cases, to all DRE voting stations; many of these requirements support accessibility as well as general usability.

Certain accessibility features that are likely to be useful to a wide range of voters are required on all voting stations, not just the Acc-VS. Finally, note that the Acc-VS is not necessarily a full-fledged DRE; for instance, an implementation may provide an ATI that generates an optiscan ballot.

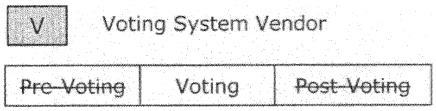
The outline for Section 2.2.7.1 is:

2.2.7.1 Accessibility
2.2.7.1.1 Voters with Disabilities—General
2.2.7.1.2 Vision
2.2.7.1.2.1 Partial Vision
2.2.7.1.2.2 Blind
2.2.7.1.3 Dexterity
2.2.7.1.4 Mobility
2.2.7.1.5 Hearing
2.2.7.1.6 Speech
2.2.7.1.7 Cognitive

1. The Voting Process Shall Incorporate Features That Are Applicable to Several Types of Disability

Discussion: These features span the disability categories within requirement #2.2.7.1 (e.g. vision, dexterity).

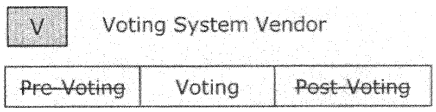
1.1 When the Provision of Accessibility Involves an Alternative Format for Ballot Presentation, Then All the Other Information Presented to Voters in the Case of Non-Disabled English-Literate Voters (Including Instructions, Warnings, Messages, and Ballot Choices) Shall Also Be Presented in That Alternative Format



Discussion: This is a general principle to be followed for any alternative format presentation. Two particular cases, (a) audio formats and (b) non-English formats, are the subject of specific requirements in later sections.

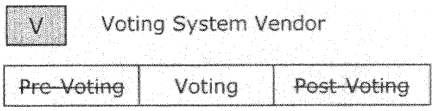
[Best Practice for Voting Officials] When the provision of accessibility involves an alternative format for ballot presentation, then all the other information presented to voters in the case of non-disabled English-literate voters (including instructions, warnings, messages, and ballot choices) is also presented in that alternative format.

1.2 An Acc-VS Shall Provide Direct Accessibility Such That Voters' Personal Assistive Devices Are Not Required for Voting



Discussion: Voters are not to be obliged to supply any special equipment in order to vote. This requirement does not preclude the Acc-VS from providing interfaces to assistive technology.

1.3 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 were used for identification, there would have to be another mechanism for voters without usable fingerprints.

[Best Practice for Voting Officials] When the primary means of voter identification or authentication uses biometric measures that require a voter to possess particular biological characteristics, the voting process provides a secondary means that does not depend on those characteristics.

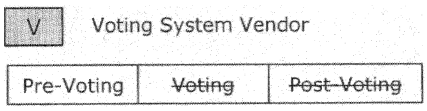
[Best Practice for Voting Officials] Polling places are subject to the appropriate guidelines of the Americans with Disabilities Act (ADA) of 1990 and of the Architectural Barriers Act (ABA) of 1968. This requirement does not stem from HAVA, but rather is a reminder of other legal obligations. For more details, see *http://www.access-board.gov/ada-aba.htm* and *http://www.usdoj.gov/crt/ada/votingck.htm*.

2. 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 station.

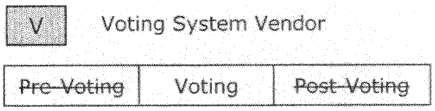
2.1 The Acc-VS Shall Be Accessible to Voters With Partial Vision

2.1.1 The Vendor Should Conduct Summative Usability Tests on the Acc-VS Using Partially Sighted Subjects and Report the Test Results to the Appropriate Testing Authority According to the Common Industry Format (CIF)



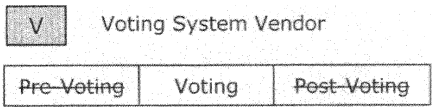
Discussion: This requirement is meant to encourage Acc-VS designers to conduct some realistic usability tests on the final product. For now, it is purely a documentation recommendation. Future versions of the VVSG will include requirements for usability testing to be conducted by the testing authority, with specific performance benchmarks.

2.1.2 The Acc-VS and Any 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 or Poll Worker



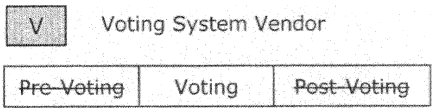
Discussion: While larger font sizes may assist most voters with poor vision, certain disabilities such as tunnel vision are best addressed by smaller font sizes. It is anticipated that future versions of the VVSG will require font size to be under the independent control of the voter.

2.1.3 All Voting Stations Using Paper Ballots Should Make Provisions for Voters With Poor Reading Vision



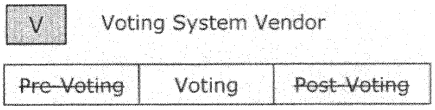
Discussion: Possible solutions include: (a) providing paper ballots in at least two font sizes, 3.0–4.0 mm and 6.3–9.0 mm and (b) providing a magnifying device.

2.1.4 An Acc-VS and Any Voting Station With a Black-and-White-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



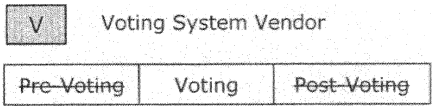
Discussion: It is anticipated that future versions of the VVSG will require contrast to be under the independent control of the voter.

2.1.5 An Acc-Vs With a Color Electronic Image Display Shall Allow the Voter or Poll Worker To Adjust the Color or the Figure-to-Ground Ambient Contrast Ratio



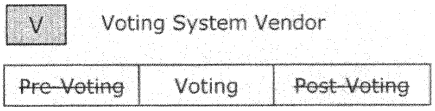
Discussion: See NASED Technical Guide #1 for examples of how a voting station may meet this requirement by offering a limited number of discrete choices. In particular, it is not required that the station offer a continuous range of color or contrast values.

2.1.6 On All Voting Stations, the Default Color Coding Shall Maximize Correct Perception by Voters and Operators With Color Blindness



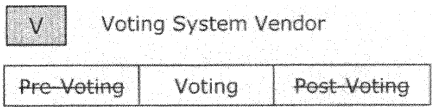
[Best Practice for Voting Officials] On all voting stations, the default color coding maximizes correct perception by voters and operators with color blindness.

2.1.7 On All Voting Stations, Color Coding Shall Not Be Used as the Sole Means of Conveying Information, Indicating an Action, Prompting a Response, or Distinguishing a Visual Element



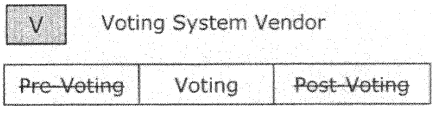
Discussion: This implies that although color can be used for emphasis, some other non-color mode must also be used to convey the information, such as a shape or text style. For example, red can be enclosed in an octagon shape.

2.1.8 Buttons and Controls on All Voting Stations Should Be Distinguishable by Both Shape and Color



Discussion: The redundant cues have been found to be helpful to those with partial vision.

2.1.9 Any Voting Station Using an Electronic Image Display Should Also Provide Synchronized Audio Output To Convey the Same Information as That on the Screen

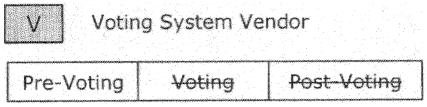


Discussion: Synchronized presentation of information in both visual and aural modes is a recommendation in this version of the VVSG, but it is anticipated that this will become a requirement in future versions.

2.2 The Acc-VS Shall Be Accessible to Voters Who Are Blind

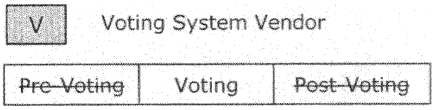
Discussion: Of course, many of the features under this requirement are also useful for voters with partial vision (see requirement # 2.2.7.1.2.1) and for voters who cannot read English for other reasons (see requirement # 2.2.7.2).

2.2.1 The Vendor Should Conduct Summative Usability Tests on the Acc-Vs Using Subjects Who Are Blind and Report the Test Results to the Appropriate Testing Authority According to the Common Industry Format (CIF)



Discussion: This requirement is meant to encourage Acc-VS designers to conduct some realistic usability tests on the final product. For now, it is purely a documentation recommendation. Future versions of the VVSG will include requirements for usability testing to be conducted by the testing authority, with specific performance benchmarks.

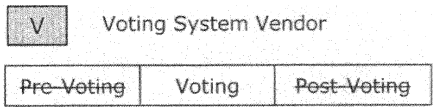
2.2.2 The Acc-VS Shall Provide an Audio-Tactile Interface (ATI) That Supports the Full Functionality of a Normal Ballot Interface, as Specified in Section 2.4



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

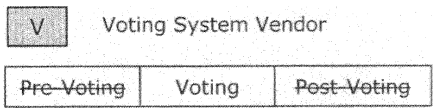
- Instructions and feedback on initial activation of the ballot (such as insertion of a smart card), if this is normally performed by the voter on comparable voting stations,
- Instructions and feedback to the voter on how to operate the Acc-VS, including settings and options (e.g. volume control, repetition),
- Instructions and feedback for navigation of the ballot,
- Instructions and feedback for voter selections in races and referenda, including write-in candidates,
- Instructions and feedback on confirming and changing selections, and
- Instructions and feedback on final submission of ballot.

2.2.2.1 The ATI of the Acc-VS Shall Provide the Same Capabilities To Vote and Cast a Ballot as Are Provided by the Other Voting Stations or by the Visual Interface of the Acc-VS. Therefore, Functional Features That Exceed the Requirements of Section 2.4 Must Be Provided on a Non-Discriminatory Basis

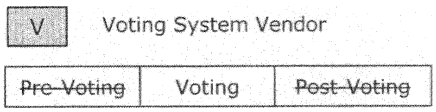


Discussion: For example, if a ''normal'' ballot supports voting a straight party ticket and then changing the choice in a single race, so must the ATI. This requirement is a special case of the more general requirement # 2.2.7.1.1.1.

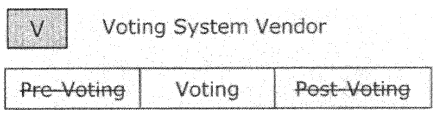
2.2.2.2 The ATI Shall Allow the Voter To Have Any Information Provided by the System Repeated



2.2.2.3 The ATI Shall Allow the Voter To Pause and Resume the Audio Presentation

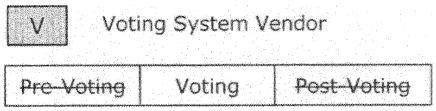


2.2.2.4 The ATI Shall Allow the Voter To Skip to the Next Contest or Return to Previous Contests



Discussion: This is analogous to the ability of sighted voters to move on to the next race once they have made a selection or to abstain from voting on a contest.

2.2.2.5 The ATI Should Allow the Voter To Skip Over the Reading of a Referendum so as To Be Able To Vote on It Immediately

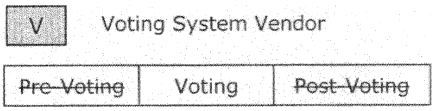


Discussion: This is analogous to the ability of sighted voters to skip over the wording of a referendum on which they have already made a decision prior to the voting session (e.g. ''Vote yes on proposition #123''). It is anticipated that this recommendation will become a requirement in future versions of the VVSG.

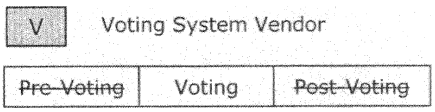
2.2.3 All Voting Stations That Provide Audio Presentation of the Ballot Shall Conform to the Following Sub-Requirements

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

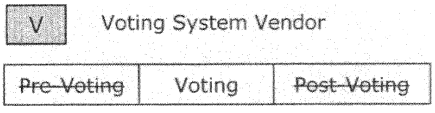
2.2.3.1 The Ati Shall Provide Its Audio Signal Through an Industry Standard Connector for Private Listening Using a 3.5Mm Stereo Headphone Jack To Allow Voters To Use Their Own Audio Assistive Devices



2.2.3.2 When a Voting Station Utilizes a Telephone Style Handset/Headset 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

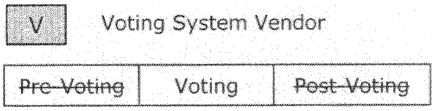


2.2.3.3 No Voting Station Shall Cause Electromagnetic Interference With Assistive Hearing Devices That Would Substantially Degrade the Performance of Those Devices. The Station, Considered as a Wireless Device (WD) Shall Achieve at Least a Category T4 Rating as Defined by American National Standard for Methods of Measurement of Compatibility Between Wireless Communications Devices and Hearing Aids, ANSI C63.19



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

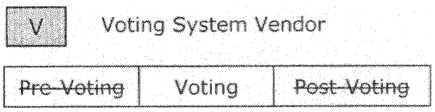
2.2.3.4 A Sanitized Headphone or Handset Should Be Made Available to Each Voter



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

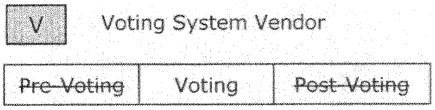
[Best Practice for Voting Officials] A sanitized headphone or handset is made available to each voter.

2.2.3.5 The Voting Station Shall Set the Initial Volume for Each Voter Between 40 and 50 dB SPL

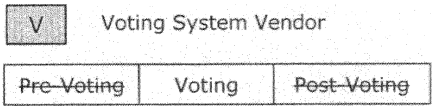


Discussion: A voter does not ''inherit'' the volume as set by the previous user of the voting station.

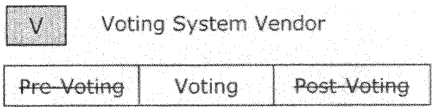
2.2.3.6 The Voting Station Shall Provide a Volume Control With an Adjustable Amplification From a Minimum of 20dB SPL Up to a Maximum of 105 dB SPL, in Increments No Greater Than 20dB



2.2.3.7 The Audio System Shall Be Able To Reproduce Frequencies Over the Audible Speech Range Of 315 Hz To 10KHz

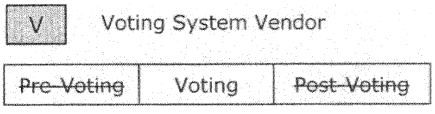


2.2.3.8 The Audio System Should Provide Information Via Recorded Human Speech, Rather Than Synthesized Speech



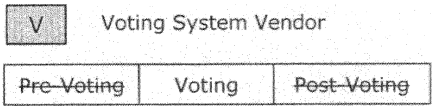
Discussion: Most users prefer real speech over synthesized speech.

2.2.3.9 The Audio System Should Allow Voters To Control, Within Reasonable Limits, the Rate of Speech



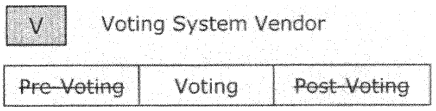
Discussion: Many blind voters are accustomed to interacting with accelerated speech.

2.2.4 If the Normal Procedure Is To Have Voters Initialize the Activation of the Ballot, the Acc-Vs 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.

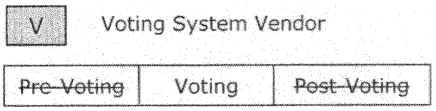
2.2.5 If the Normal Procedure Is for Voters To Submit Their Own Ballots, Then the Voting Process Should Provide Features That Enable Voters Who Are Blind To Perform This Submission



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

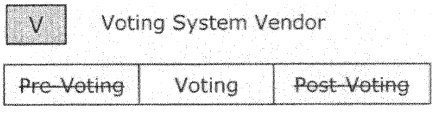
[Best Practice for Voting Officials] If the normal procedure is for voters to submit their own ballots, then the voting process provides features that enable voters who are blind to perform this submission.

2.2.6 If the Normal Procedure Includes VVPAT, the Acc-VS Should Provide Features That Enable Voters Who Are Blind To Perform This Verification

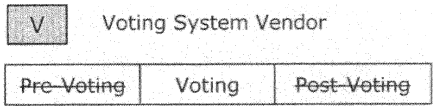


Discussion: For example, the Acc-VS might provide an automated reader for the paper record that converts the contents of the paper into audio output. It is anticipated that this recommendation will become a requirement in future versions of the VVSG.

2.2.7 All Mechanically Operated Controls or Keys on an Acc-VS Shall Be Tactilely Discernible Without Activating Those Controls or Keys

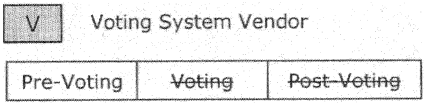


2.2.8 On an Acc-VS, the Status of All Locking or Toggle Controls or Keys (Such as the ''Shift'' Key) Shall Be Visually Discernible, and Discernible Either Through Touch or Sound



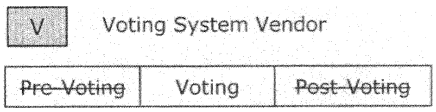
3. The Voting Process Shall Be Accessible to Voters Who Lack Fine Motor Control or the Use of Their Hands

3.1 The Vendor Should Conduct Summative Usability Tests on the Acc-VS With Subjects Lacking Fine Motor Control and Report the Test Results to the Appropriate Testing Authority According to the Common Industry Format (CIF)



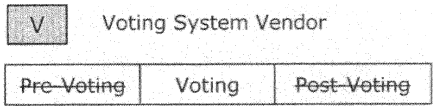
Discussion: This requirement is meant to encourage Acc-VS designers to conduct some realistic usability tests on the final product. For now, it is purely a documentation recommendation. Future versions of the VVSG will include requirements for usability testing to be conducted by the testing authority with specific performance benchmarks.

3.2 All Keys and Controls on the Acc-VS Shall Be Operable With One Hand and Shall Not Require Tight Grasping, Pinching, or Twisting of the Wrist. The Force Required To Activate Controls and Keys Shall Be No Greater 5 lbs. (22.2 N)



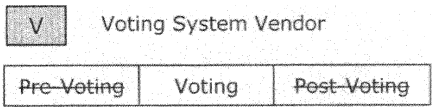
Discussion: Controls are to be operable without excessive force.

3.3 The Acc-VS Controls Shall Not Require Direct Bodily Contact or for the Body To Be Part of Any Electrical Circuit



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

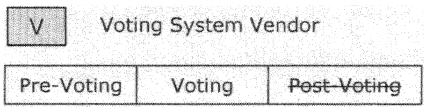
3.4 The Acc-VS Should Provide a Mechanism To Enable Non-Manual Input That Is Functionally Equivalent to Tactile Input



Discussion: This recommendation ensures that the Acc-VS is operable by individuals who do not have the use of their hands. All the functionality of the Acc-VS (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 the input mechanism if it is provided by the Acc-VS.

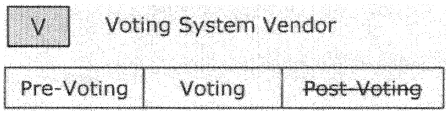
4. The Voting Process Shall Be Accessible to Voters Who Use Mobility Aids, Including Wheelchairs

4.1 The Acc-VS 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



[Best Practice for Voting Officials] The Acc-VS provides 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 is level with no slope exceeding 1:48 and positioned for a forward approach or a parallel approach.

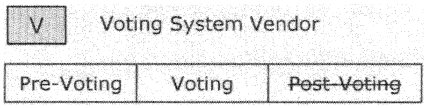
4.2 All Controls, Keys, Audio Jacks and Any Other Part of the Acc-VS Necessary for the Voter To Operate the Voting System Shall Be Within Reach as Specified Under the Following Sub-Requirements



Discussion: All dimensions are given in inches. To convert to millimeters, multiply by 25.4 and then round to the nearest multiple of 5. Note that these sub-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. All the sub-requirements inherit the ''responsible entity'' and ''process'' properties.

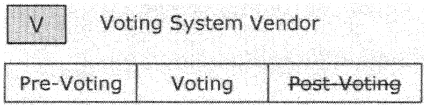
[Best Practice for Voting Officials] All controls, keys, audio jacks and any other part of the Acc-VS necessary for the voter to operate the voting system are within the reach regions as specified in the VVSG Volume I, Section 2.2.7.1.4.3.

4.2.1 If the Acc-VS Has a Forward Approach With No Forward Reach Obstruction Then the High Reach Shall Be 48 Inches Maximum and the Low Reach Shall Be 15 Inches Minimum. See Figure 2.2.7.1–1

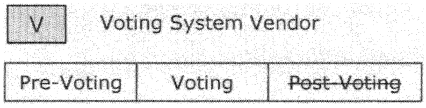


4.2.2 If the Acc-VS Has a Forward Approach With a Forward Reach Obstruction, the Following Sub-Requirements Apply. See Figure 2.2.7.1–2

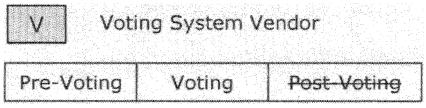
4.2.2.1 The Forward Obstruction Shall Be No Greater Than 25 Inches in Depth, Its Top No Higher Than 34 Inches and Its Bottom Surface No Lower Than 27 Inches



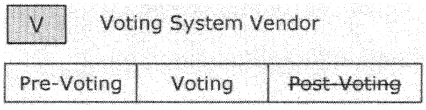
4.2.2.2 If the Obstruction Is No More Than 20 Inches in Depth, Then the Maximum High Reach Shall Be 48 Inches, Otherwise It Shall Be 44 Inches



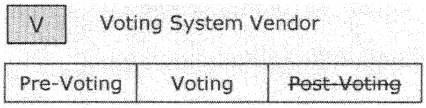
4.2.2.3 Space Under the Obstruction Between the Finish Floor or Ground and 9 Inches (230 mm) Above the Finish Floor or Ground Shall Be Considered Toe Clearance and Shall Comply With the Following Sub-Requirements



A. Toe clearance shall extend 25 inches (635 mm) maximum under the obstruction.

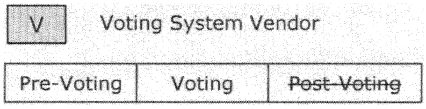


B. The minimum toe clearance under the obstruction shall be either 17 inches (430 mm) or the depth required to reach over the obstruction to operate the Acc-VS, whichever is greater.



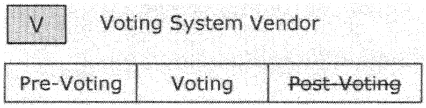
C. Toe clearance shall be 30 inches (760 mm) wide minimum.

Voting System Vendor

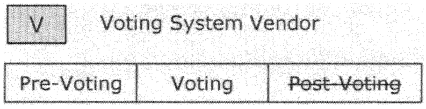


4.2.2.4 Space Under the Obstruction Between 9 inches (230 mm) and 27 Inches (685 mm) Above the Finish Floor or Ground Shall Be Considered Knee Clearance and Shall Comply With the Following Sub-Requirements

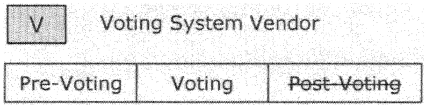
A. Knee clearance shall extend 25 inches (635 mm) maximum under the obstruction at 9 inches (230 mm) above the finish floor or ground.



B. 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.

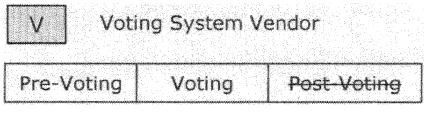


C. Between 9 inches (230 mm) and 27 inches (685 mm) above the finish floor or ground, the knee clearance shall be permitted to reduce at a rate of 1 inch (25 mm) in depth for each 6 inches (150 mm) in height.

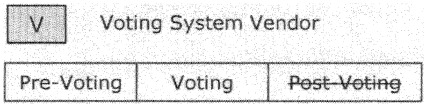


Discussion: It follows that the minimum knee clearance at 27 inches above the finish floor or ground shall be 3 inches less than the minimum knee clearance at 9 inches above the floor.

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

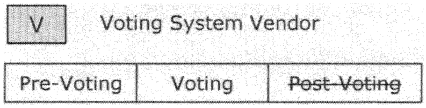


4.2.3 If the Acc-VS Has a Parallel Approach With No Side Reach Obstruction Then the Maximum High Reach Shall be 48 Inches and the Minimum Low Reach Shall be 15 Inches. See Figure 2.2.7.1–3

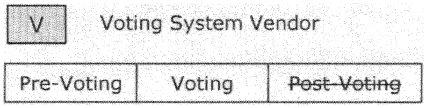


4.2.4 If the Acc-VS Has a Parallel Approach With a Side Reach Obstruction, the Following Sub-Requirements Apply. See Figure 2.2.7.1–4

4.2.4.1 The Side Obstruction Shall Be No Greater Than 24 Inches in Depth and Its Top No Higher Than 34 Inches

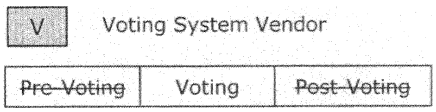


4.2.4.2 If the Obstruction Is No More Than 10 inches in Depth, Then the Maximum High Reach Shall Be 48 Inches, Otherwise It Shall Be 46 Inches



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

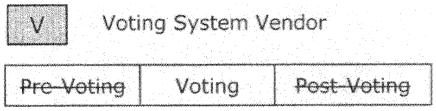
4.2.5 All Labels, Displays, Controls, Keys, Audio Jacks, and Any Other Part of the Acc-VS Necessary for the Voter To Operate the Voting System Shall Be Easily Legible and Visible to a Voter in a Wheelchair With Normal Eyesight (No Worse Than 20/40, Corrected) Who Is in an Appropriate Position and Orientation with Respect to the Acc-VS



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

5. The Voting Process Shall Be Accessible to Voters With Hearing Disabilities

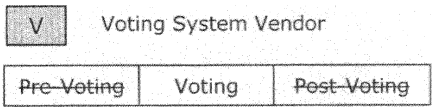
5.1 The Acc-VS Shall Incorporate the Features Listed Under Requirement # 2.2.7.1.2.2.3 (Audio Presentation) To Provide Accessibility to Voters With Hearing Disabilities



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

[Best Practice for Voting Officials] The Acc-VS incorporates the features listed in the VVSG Volume I, Section 2.2.7.1.2.2.3 (audio presentation) to provide accessibility to voters with hearing disabilities.

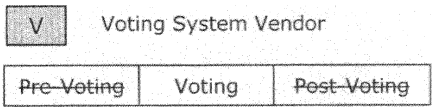
5.2 If a Voting Station Provides Sound Cues as a Method To Alert the Voter, the Tone Shall Be Accompanied by a Visual Cue



Discussion: For instance, the station 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.

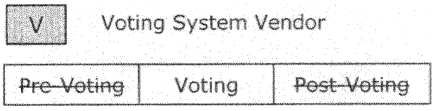
6. The Voting Process Shall Be Accessible to Voters With Speech Disabilities

6.1 No Voting Station Shall Require Voter Speech for its Operation



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

7. 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. Section 2.2.7.1.2.1.9, the synchronization of audio with the screen in a DRE, is helpful for some cognitive disabilities such as dyslexia. Section 2.2.7.3.3 also contains some relevant guidelines.

[Best Practice for Voting Officials] The voting process is made accessible to voters with cognitive disabilities.

Figures for Accessibility

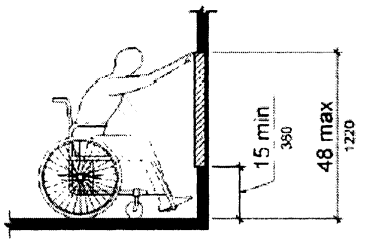


Figure 2.2.7.1-1
Unobstructed forward reach

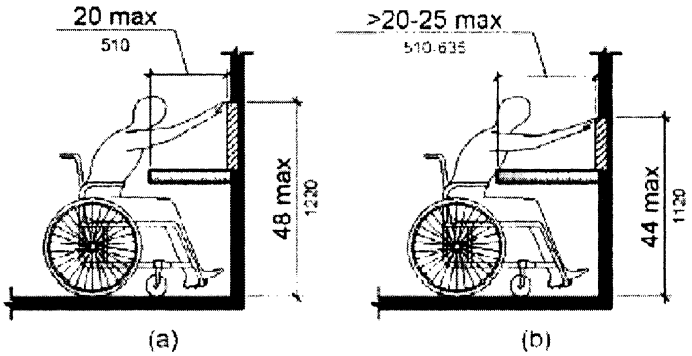


Figure 2.2.7.1-2
Obstructed forward reach
(a) for an obstruction depth of up to 20 inches (508 mm)
(b) for an obstruction depth of up to 25 inches (635 mm)

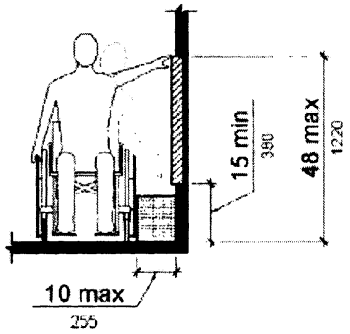


Figure 2.2.7.1-3
Unobstructed side reach with an allowable obstruction less than 10 inches (254 mm) deep.

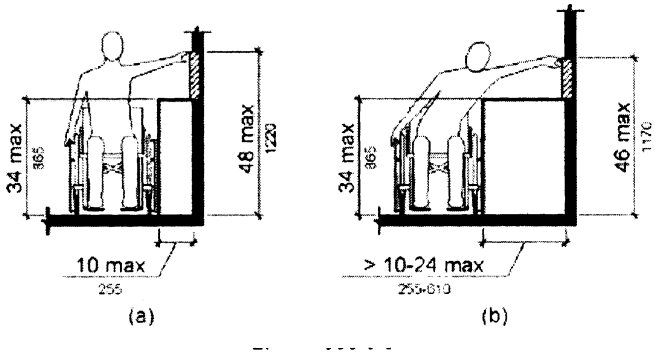


Figure 2.2.7.1-4
Obstructed side reach
(a) for an obstruction depth of up to 10 inches (254 mm)
(b) for an obstruction depth of up to 24 inches (610 mm)

2. The Voting Process Shall Be Accessible to Voters Who Are Not Fully Literate in English. This Requirement May Be Satisfied by Providing Voting Stations in a Polling Place That Accommodate Those Without a Full Command of English. See HAVA 301 (a)(4) and 241 (b)(5). Such a Facility is Referred to Herein as an Alternative Language Voting Station (ALVS)

HAVA Section 301 (a)(4) reads:

ALTERNATIVE LANGUAGE ACCESSIBILITY.—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).

The requirements within Section 2.2.7.2 are intended to address this mandate. 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 citizens.

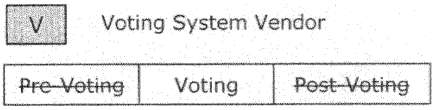
Note that the provision of an audio interface for people with visual disabilities as described in Section 2.2.7.1 may also assist voters who speak English, but are unable to read it.

The outline for section 2.2.7.2 is:

2.2.7.2. Alternative Languages
2.2.7.2.1 Complete Information

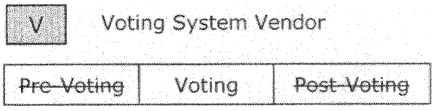
2.2.7.2.2 Spelling of Names
2.2.7.2.3 Literate Voters
2.2.7.2.4 Illiterate Voters

1. All the Information Presented in the Normal Case of English-literate Voters (Including Instructions, Warnings, Messages, and Ballot Choices) Shall Also Be Presented by the ALVS, Whether the Language Is Written or Spoken



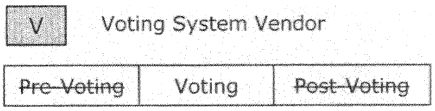
Discussion: This is in keeping with general requirement # 2.2.7.1.1.1.

2. Regardless of the Language, Candidate Names Shall Be Displayed or Pronounced in English on All Ballots. For Written Languages That Do Not Use Roman Characters (e.g. Chinese, Japanese, Korean, Arabic), the Ballot Shall Include Transliteration of Candidate Names Into the Relevant Language

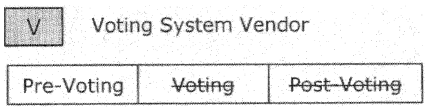


[Best Practice for Voting Officials] Regardless of the language, candidate names are displayed or pronounced in English on all ballots. For written languages that do not use Roman characters (e.g., Chinese, Japanese, Korean, Arabic), the ballot includes transliteration of candidate names into the relevant language.

3. For Literate Voters, the ALVS Shall Provide Printed or Displayed Instructions, Messages, and Ballots in Their Preferred Language, Consistent With State and Federal Law

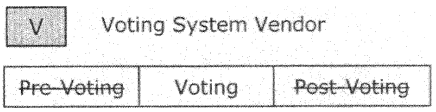


3.1 The Vendor Should Conduct Summative Usability Tests on the ALVS With Literate Subjects Who Neither Speak Nor Read English and Report the Test Results According to the Common Industry Format (CIF)



Discussion: This requirement is meant to encourage Acc-VS designers to conduct some realistic usability tests on the final product. For now, it is purely a documentation recommendation. Future versions of the VVSG will include requirements for usability testing to be conducted by the testing authority, with specific performance benchmarks.

4. For Illiterate Voters, the ALVS Shall Provide Spoken Instructions and Ballots in the Preferred Language of the Voter, Consistent With State and Federal Law. The Requirements and Sub-Requirements of # 2.2.7.1.2.2.2 (Acc-VS/ATI) Shall Apply to This Mode of Interaction



Discussion: Note that some languages have no widely accepted written form.

3. The Voting Process Shall Provide a High Level of Usability to the Voters. Accordingly, Voters Shall Be Able to Negotiate the Process Effectively, Efficiently, and Comfortably

Discussion: The first Voting System Standards codified in HAVA relate to the interaction between the voter and the voting system. HAVA Section 301 begins:

SEC. 301. VOTING SYSTEMS STANDARDS.

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.''

The requirements of this section supplement these basic HAVA mandates and also HAVA's support for improved usability (see Section 243 and Section 221(e)(2)(D)).

Voting and Usability

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 users are the voters (but also poll workers), the product is the voting system, and the task is the correct representation of one's choices in the election. Additional requirements for task performance are independence and privacy: the voter should normally be able to complete the voting task without assistance from others (although the voting system itself may offer help), and the voter's choices should be private (see Section 2.2.7.4). Aside from its intrinsic undesirability, 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 ''bottom-line'' metrics for usability are:

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

These criteria define the core of good voting system usability. The purpose of the detailed requirements listed below is to help voting systems meet the core criteria.

Methodology for Requirements

It is the intention of the TGDC that in forthcoming versions of the VVSG, 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 voters' intentions), 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 somewhat 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.

This is not to say that an extensive set of design guidelines is without value. But we wish to distinguish between good advice to be considered by developers and strict requirements that will be enforced by a regime of formal testing. For more detail on the issue of design vs. performance standards, see Sections 2.3 and 6.1 et al. of NIST Special Publication 500–256: Improving the Usability and Accessibility of Voting Systems and Products (*http://vote.nist.gov/ Final%20Human%20Factors%20 Report%20% 205–04.pdf*).

General Issues for the Usability Requirements

As mentioned in Section 2.2.7.1, many of the guidelines in this section enhance accessibility as well as general usability.

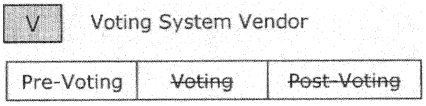
The scope of usability includes the entire voting process, although the emphasis herein is on the interface between the voter and the voting station.

The requirements in this sub-section generally assume a visual-tactile interface, but also see requirements in Sections 2.2.7.1 and Section 2.2.7.2 for alternative formats, including audio.

The outline for Section 2.2.7.3 is:

2.2.7.3 Usability
2.2.7.3.1 Usability Testing by Vendor
2.2.7.3.2 Functional Capabilities
2.2.7.3.3 Cognitive Issues
2.2.7.3.4 Perceptual Issues
2.2.7.3.5 Interaction Issues

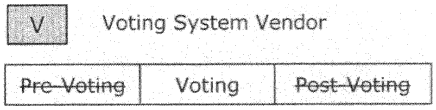
1. The Vendor Should Conduct Summative Usability Tests on the Voting System Using Subjects Representative of the General Population and Report the Test Results to the Appropriate Testing Authority According to the Common Industry Format (CIF)



Discussion: This requirement is meant to encourage Acc-VS designers to conduct some realistic usability tests on the final product. For now, it is purely a documentation recommendation. Future versions of the VVSG will include requirements for usability testing to be conducted by the testing authority, with specific performance benchmarks.

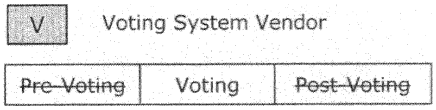
2. The Voting Process Shall Provide Certain Functional Capabilities To Support Voter Usability

2.1 As Mandated by HAVA 301(a)(1)(A), the Voting System Shall Support a Process That Allows the Voter To Review His or Her Completed Ballot Before Final Submission in Order To Verify That it Correctly Represents the Intended Vote and To Correct the Ballot if Mistakes Are Detected



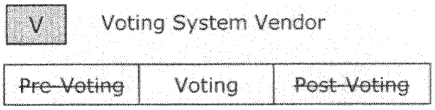
Discussion: Note that this review and correction may be achieved by procedural means (e.g. in the case of paper ballots), as well as technical (see HAVA 301(a)(1)(B)). This requirement is a brief paraphrase of the HAVA language but of course the statutory language is determinative.

2.2 As Mandated by HAVA 301(a)(1)(A), the Voting System Shall Support a Process That Notifies the Voter if He or She Has Attempted To Vote for More Candidates Than the Maximum Permitted in a Given Race and That Provides the Voter With the Opportunity To Correct the Ballot Before Final Submission



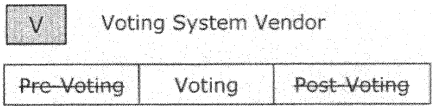
Discussion: Note that this notification and correction may be achieved by procedural means (e.g. in the case of paper ballots), as well as technical (see HAVA 301(a)(1)(B)). This requirement is a brief paraphrase of the HAVA language but of course the statutory language is determinative.

2.3 DRE Voting Stations Shall Allow the Voter To Change a Vote Within a Race Before Advancing to the Next Race



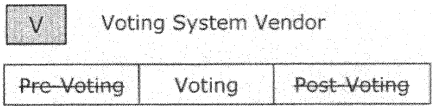
Discussion: The point here is that voters using a DRE should not have to wait for the final ballot review in order to change a vote.

2.4 The Voting System Shall Support a Process That Notifies the Voter if He or She Has Attempted To Vote for Fewer Candidates Than the Maximum Permitted in a Given Race and That Provides the Voter With the Opportunity To Change the Ballot Before Final Submission. The Process Shall Also Notify the Voter That Such an ''Undervote'' Is Permitted and Shall Accept a Ballot if the Voter so Chooses



Discussion: Note that this notification and correction may be achieved by procedural means (e.g. in the case of paper ballots), as well as technical (see HAVA 301(a)(1)(B)).

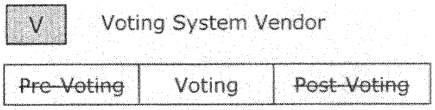
2.5 DRE Voting Stations Should Provide Navigation Controls That Allow the Voter To Advance to the Next Race or Go Back to the Previous Race Before Completing a Vote on the Race or Races Currently Being Presented (Whether Visually or Aurally)



Discussion: For example, the voter should not be forced to proceed sequentially through all the races and/or candidates before going back to check the status of a previous race.

3. The Voting Process Shall Be Designed To Minimize Cognitive Difficulties for the Voter

3.1 Consistent With Election Law, the Voting System Should Support a Process That Does Not Introduce Any Bias for or Against Any of the Choices To Be Made by the Voter. In Both Visual and Aural Formats, Candidates and Choices Shall Be Presented in an Equivalent Manner

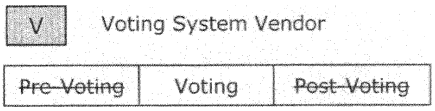


Discussion: Certain differences in presentation are unavoidable, such as the order in which candidates are listed, and write-in candidates are inherently more difficult to vote for. But comparable characteristics such as font size or voice volume and speed must be the same for all choices.

3.2 The Voting System or Related Materials Shall Provide Clear Instructions and Assistance so as To Allow Voters To Successfully Execute and Cast Their Ballots Independently

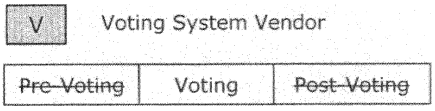
Discussion: Voters should not routinely need to ask for human assistance.

3.2.1 Voting Stations 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 at the station if confused. DRE voting stations may provide this with a distinctive ''help'' button. Any type of voting station may provide written instructions that are available and separate from the ballot. Note special requirements for the Acc-VS in requirement # 2.2.7.1.2.2.2 (Acc-VS/ATI).

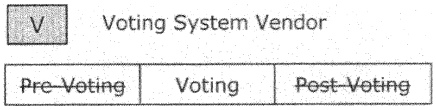
3.2.2 The Voting Station Shall Provide Instructions for All Its Valid Operations



Discussion: If an operation is available to the voter, it must be documented. Examples include how to change a vote, how to navigate among races, how to cast a party-line vote, and how to cast a write-in vote.

3.3 The Voting System Shall Provide the Capability To Design a Ballot for Maximum Clarity and Comprehension

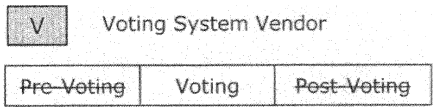
3.3.1 The Voting Station Should Not Visually Present a Single Race Spread Over Two Pages or Two Columns



Discussion: Such a visual separation poses the risk that the voter will perceive the race as two races. Of course, if a race has a very large number of candidates, it may be infeasible to observe this guideline.

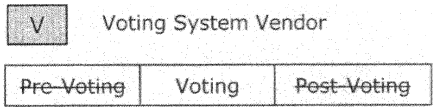
[Best Practice for Voting Officials] The voting station does not visually present a single race spread over two pages or two columns.

3.3.2 The Ballot Shall Clearly Indicate the Maximum Number of Candidates for Which One Can Vote Within a Single Race



[Best Practice for Voting Officials] The ballot clearly indicates the maximum number of candidates for which one can vote within a single race.

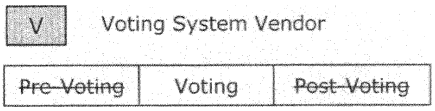
3.3.3 There Shall Be a Consistent Relationship Between the Name of a Candidate and the Mechanism Used to Vote for That Candidate



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 candidate's names.

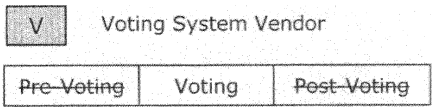
[Best Practice for Voting Officials] The ballot presents the relationship between the name of a candidate and the mechanism used to vote for that candidate in a consistent manner.

3.4 Warnings and Alerts Issued by the Voting Station 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 Failed in Some Way



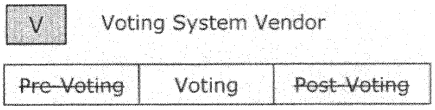
Discussion: In case of an equipment failure, the only action available to the voter might be to get assistance from a poll worker.

3.5 The Use of Color by the Voting Station 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



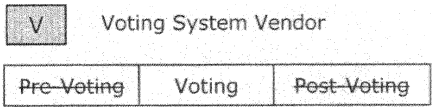
4. The Voting Process Shall Be Designed to Minimize Perceptual Difficulties for the Voter

4.1 No Display Screen of a Voting Station Shall Flicker With a Frequency Between 2 Hz and 55 Hz



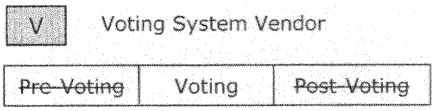
Discussion: Aside from usability concerns, this requirement protects voters with epilepsy.

4.2 Any Aspect of the Voting Station 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



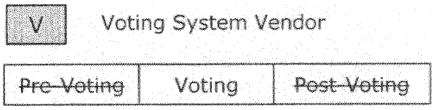
Discussion: This implies that the voting station presents the same initial appearance to every voter (excluding, of course, substantive differences in the ballot content due to residence or party of the voter).

4.3 If Any Aspect of a Voting Station is Adjustable by the Voter, There Should Be a Mechanism to Reset All Such Aspects to Their Default Values

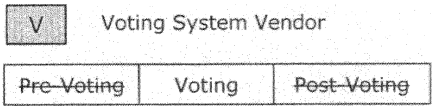


Discussion: The purpose is to allow a voter who has adjusted the station into an undesirable state to reset all the aspects so as to get a fresh start.

4.4 The Minimum Font Size for All Text Intended for the Voter During the Voting Session Shall Be 3.0mm (Measured as the Height of a Capital Letter)

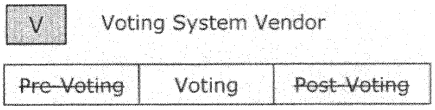


4.5 All Text Intended for the Voter During the Voting Session Should Be Presented in a Sans Serif Font



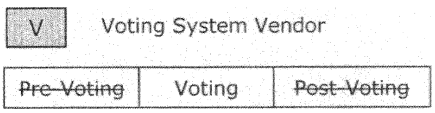
Discussion: Experimentation has shown that users prefer such a font and the legibility of serif and sans serif fonts is equivalent.

4.6 The Minimum Figure-to-Ground Ambient Contrast Ratio for All Text and Informational Graphics (Including Icons) Intended for the Voter Shall Be 3:1



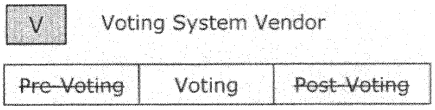
5. The Voting Process Shall Be Designed to Minimize Interaction Difficulties for the Voter

5.1 Voting Stations With Electronic Image Displays Shall Not Require Page Scrolling by the Voter

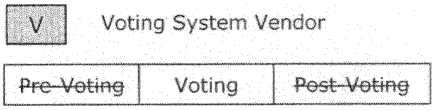


Discussion: This is not an intuitive operation for those unfamiliar with the use of computers. Even those experienced with computers often do not notice a scroll bar and miss information below the page. DREs may require voters to move to the next or previous ''page.''

5.2 The Voting Station Shall Provide Unambiguous Feedback Regarding the Voter's Selection, Such as Displaying a Checkmark Beside the Selected Option or Conspicuously Changing Its Appearance

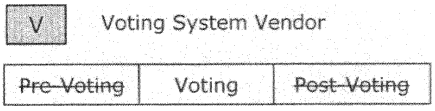


5.3 If the Voting Station Requires a Response by a Voter Within a Specific Period of Time, It Shall Issue an Alert at Least 20 Seconds Before This Time Period Has Expired and Provide a Means by Which the Voter May Receive Additional Time

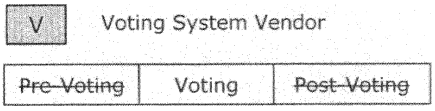


5.4 Input Mechanisms Shall Be Designed so as to Minimize Accidental Activation (Also, See Requirement # 2.2.7.1.2.2.7 on Tactile Discernability)

5.4.1 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



5.4.2 No Key or Control on a Voting Station Shall Have a Repeat Feature Enabled



Discussion: This is to preclude accidental activation.

4. The Voting Process Shall Preclude Anyone Else From Determining the Content of a Voter's Ballot, With or Without the Voter's Cooperation

Discussion: Voter privacy is strongly supported by HAVA—see Sections 221(e)(2)(C) and 301(a)(1). In this subsection, we address only privacy concerns in relation to human factors issues, but not with respect to the processing of cast ballots.

Although elections in American history have sometimes been public (and certain ''town-hall'' questions are still voted openly), the use of the secret ballot for political office is now universal.

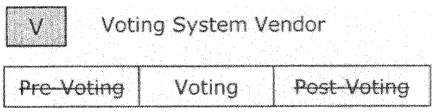
Privacy in this context, including the property of the voter being unable to disclose his or her vote, ensures that the voter can make choices based solely on his or her own preferences without intimidation or inhibition. Among other practices, this forbids the issuance of a receipt to the voter that would provide proof to another how he or she voted.

The outline for Section 2.2.7.4 is:

2.2.7.4 Privacy
2.2.7.4.1 Privacy at the polling place
2.2.7.4.2 No preservation of alternative formats
2.2.7.4.3 Absentee Balloting

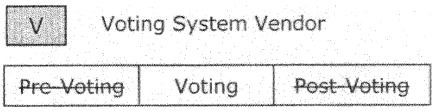
1. The Voting Station and Polling Place Shall Be Configured so as to Prevent Others From Learning the Contents of a Voter's Ballot

1.1 The Ballot and Any Input Controls Shall Be Visible Only to the Voter During the Voting Session and Ballot Submission



[Best Practice for Voting Officials] The ballot and any input controls are visible only to the voter during the voting session and ballot submission. Poll workers need to take into account such factors as visual barriers, windows, permitted waiting areas for other voters, and procedures for ballot submission when not performed at the voting station, e.g. submission of optiscan ballots to a central reader.

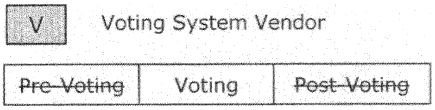
1.2 The Audio Interface Shall Be Audible Only to the Voter



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.

[Best Practice for Voting Officials] The audio interface is audible only to the voter.

1.3 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

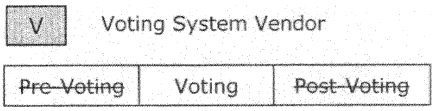


Discussion: This requirement is a brief paraphrase of the HAVA language but of course the statutory language is determinative.

[Best Practice for Voting Officials] As mandated by HAVA 301(a)(1)(C), the voting system notifies the voter of an attempted overvote in a way that preserves the privacy of the voter and the confidentiality of the ballot.

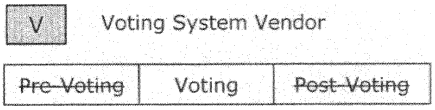
2. Voter Anonymity Shall Be Maintained for Alternative Format Ballot Presentation

2.1 No Information Shall Be Kept Within a Non-Paper-Based Cast Vote Record That Identifies Any Accessibility Feature(s) Used by a Voter



Discussion: Large-print paper ballots unavoidably preserve such information.

2.1.1 No Information Shall Be Kept Within a Non-Paper-Based Cast Vote Record That Identifies Any Alternative Language Feature(s) Used by a Voter



Discussion: Non-English paper ballots unavoidably preserve such information.

[Best Practice for Voting Officials] Appropriate procedures are needed to ensure that absentee balloting enable the voter to preserve privacy. There is no practical means to prevent a voter from revealing an absentee paper ballot to others. But the procedures should ensure that if a voter chooses to maintain privacy, it is not violated at a later stage, in particular when the ballot is received by voting officials.

2.2.8 Vote Tabulating Program

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

2.2.8.1 Functions

The vote tabulating program software resident in each voting device, 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; and

d. Accommodate variations in ballot counting logic.

2.2.8.2 Voting Variations

There are significant variations among the election laws of the 50 states with respect to permissible ballot contents, voting options, and the associated ballot counting logic. The TDP accompanying the system shall specifically identify which of the following items can and cannot be supported by the system, as well as how the system can implement the items supported:

a. Closed primaries;

b. Open primaries;

c. Partisan offices;

d. Non-partisan offices;

e. Write-in voting;

f. Primary presidential delegation nominations;

g. Ballot rotation;

h. Straight party voting;

i. Cross-party endorsement;

j. Split precincts;

k. Vote for N of M;

l. Recall issues, with options;

m. Cumulative voting;

n. Ranked order voting; and

o. Provisional or challenged ballots.

2.2.9 Ballot Counter

For all voting systems, each device 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; and

e. Is visible to designated election officials.

2.2.10 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 Standards. Section 5 of the Standards 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 a voting machine the content and appearance of the ballots to be used in an election;
- *Vote Transmission to Central Site:* For 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; and
- *List of Voters:* A listing of the individual voters who have cast ballots in a specific election.

2.2.9 Data Retention

United States Code Title 42, Sections 1974 through 1974e, states 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 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 4.5 of the Standards 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 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, authenticatable 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 device 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 device or system.

2.3 Pre-Voting Functions

This section 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; and
- 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.

2.3.1 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 for ballot preparation;
- Ballot formatting; and
- Ballot production.

2.3.1.1 General Capabilities

All systems shall provide the general capabilities for ballot preparation.

2.3.1.1.1 Common Standards

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:

(1) Offices and their associated labels and instructions;

(2) Candidate names and their associated labels; and

(3) 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 races by party affiliation;

e. Generating ballots that contain identifying codes or marks uniquely associated with each format; and

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.

2.3.1.1.2 Paper-Based System Standards

In addition to the common standards, paper-based systems shall meet the following standards applicable to the technology used:

a. Enable voters to make selections by punching a hole or by making a mark in areas designated for this purpose upon each ballot card or sheet;

b. For punchcard systems, ensure that the vote response fields can be properly aligned with punching devices used to record votes; and

c. For marksense systems, ensure that the timing marks align properly with the vote response fields.

2.3.1.2 Ballot Formatting

Ballot formatting is the process by which election officials or their designees use election databases and vendor 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 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; and

g. Modification by authorized persons of a previously defined ballot format for use in a subsequent election.

2.3.1.3 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.

2.3.1.3.1 Common Standards

The voting system shall provide a means of printing or otherwise generating a ballot display that can be installed in all system voting devices for which it is intended. All systems shall provide a capability to ensure:

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; and

c. The ballot conforms to vendor specifications for type of paper stock, weight, size, shape, size and location of punch or 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.

2.3.1.3.2 Paper-Based System Standards

In addition to the common standards, 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).

2.3.2 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; and

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.

2.3.3 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 a programmable memory devices and for indicating errors; and

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.

2.3.4 Readiness Testing

Election personnel conduct equipment and system readiness tests prior to the start of an election to ensure that the voting system functions properly, to confirm that system equipment has been properly integrated, and to obtain equipment status reports.

2.3.4.1 Common Standards

All systems shall provide the capabilities to:

a. Verify that voting machines or vote recording and data processing equipment, precinct count equipment, and central count equipment are 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 system equipment;

d. Verify that hardware and software function correctly;

e. Generate consolidated data reports at the polling place and higher jurisdictional levels; and

f. Segregating 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 devices to simulate operator and voter functions may be used for these tests provided that the following standards are met:

a. These elements shall be capable of being tested separately, and shall be proven to be reliable verification tools prior to their use; and

b. 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.

2.3.4.2 Paper-Based Systems

Paper-based systems shall:

a. Support conversion testing that uses all potential ballot positions as active positions; and

b. Support conversion testing of ballots with active position density for systems without pre-designated ballot positions.

2.3.5 Verification at the Polling Place

Election officials perform verification at the polling place to ensure that all voting systems and equipment function properly before and during an election. All 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; and

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:

a. Confirmation that there are no hardware or software failures; and

b. Confirm 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 places, 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.

2.3.6 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); and

c. Other information needed to ensure the readiness of the equipment and to accommodate administrative reporting requirements.

2.4 Voting Functions

All systems shall support:

- Opening the polls; and
- Casting a ballot.

Additionally, all DRE systems shall support:

- Activating the ballot.
- Augmenting the election counter; and
- Augmenting the life-cycle counter.

2.4.1 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.

2.4.1.1 Opening the Polling Place (Precinct Count Systems)

To allow voting devices to be activated for voting, the system shall provide:

a. An internal test or diagnostic capability to verify that all of the polling place tests specified in Section 2.3.5 have been successfully completed; and

b. Automatic disabling any device that has not been tested until it has been tested.

2.4.1.2 Paper-Based System Standards

The standards for opening the polling place for paper-based systems consist of common standards and additional standards that apply to precinct count paper-based systems.

2.4.1.2.1 All Paper-Based Systems

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

a. A means of verifying that ballot punching or marking devices are properly prepared and ready to use;

b. A voting booth or similar facility, in which the voter may punch or mark the ballot in privacy; and

c. Secure receptacles for holding voted ballots.

2.4.1.2.2 Precinct Count Paper-Based Systems

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

a. Activating the ballot counting device;

b. Verifying that the device has been correctly activated and is functioning properly; and

c. Identifying device failure and corrective action needed.

2.4.1.3 DRE System Standards

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; and

d. A means of identifying system failure and any corrective action needed.

2.4.2 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; and

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; and

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

2.4.3 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 Section 2.2.7 of the Standards.

2.4.3.1 Common Standards

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 graceful 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; and

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.

2.4.3.2 Paper-Based Systems Standards

The standards for casting a ballot for paper-based systems consist of common standards and additional standards that apply to precinct count paper-based systems.

2.4.3.2.1 All Paper-Based Systems

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 punch or 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); and

d. Protect the secrecy of the vote throughout the process.

2.4.3.2.2 Precinct Count Paper-Based Systems

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

a. Provide feedback to the voter that identifies specific contests or ballot issues for which an overvote or undervote is detected;

b. Allow the voter, at the voter's choice, to vote a new ballot or submit the ballot 'as is' without correction; and

c. Allow an authorized election official to turn off the capabilities defined in 'a' and 'b' above.

2.4.3.3 DRE Systems Standards

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 in a contest;

f. Prevent the voter from overvoting;

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

h. 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;

i. 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;

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

k. 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;

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

m. Ensure that the votes stored accurately represent the actual votes cast;

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

o. Provide a capability to retrieve ballot images in a form readable by humans (in accordance with the requirements of Section 2.2.2.2 and 2.2.4.2);

p. Increment the proper ballot position registers or counters;

q. Protect the secrecy of the vote throughout the voting process;

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

s. Provide the ability for election officials to submit test ballots for use in verifying the end-to-end integrity of the system; and

t. Isolate test ballots such that they are accounted for accurately in vote counts and are not reflect in official vote counts for specific candidates or measures.

2.5 Post-Voting Functions

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

2.5.1 Closing the Polling Place (Precinct Count)

These standards for closing the polling place are specific to precinct count systems. The system shall provide the means for:

a. Preventing the further casting of ballots once the polling place has 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; and

e. Precluding the unauthorized reopening of the polls once the poll closing has been completed for that election.

2.5.2 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).

2.5.3 Producing Reports

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

2.5.3.1 Common Standards

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 Section 4.5 in the form of printed reports, or in electronic memory for printing centrally; and

g. Prevent data from being altered or destroyed by report generation, or by the transmission of results over telecommunications lines.

2.5.3.2 Precinct Count Systems

In addition to the common reporting requirements, all precinct count voting systems shall:

a. Prevent the printing of reports and the unauthorized extraction of data prior to the official close of the polling place;

b. Provide a means to extract information from a transportable programmable memory device or data storage medium for vote consolidation;

c. 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; and

d. Prevent data in transportable memory from being altered or destroyed by report generation, or by the transmission of results over telecommunications lines.

2.5.4 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; and

c. Clearly indicate on each report or file that the results it contains are unofficial.

2.6 Maintenance, Transportation, and Storage

All systems shall be designed and manufactured to facilitate preventive and corrective maintenance, conforming to the hardware standards described in Section 3.

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 Section 3; and

b. Function without degradation in capabilities after storage between elections, as demonstrated by meeting the performance standards described in Section 3.

Volume I, Section 3

Table of Contents

3 Hardware Standards

3.1 Scope

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 punching and 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; and
- 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 4 of the Standards.

3.1.1 Hardware Sources

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

a. Hardware provided by the voting system vendor and its suppliers;

b. Hardware furnished by an external provider (for example, providers of commercial off-the-shelf (COTS) machines and devices) where the hardware may be used in any way during voting system operation; and

c. Hardware provided by the voting jurisdiction.

3.1.2 Organization of this Section

The standards presented in this section are organized as follows:

- Performance Requirements: These requirements address the combined operational capabilities of the voting system's hardware and software across a broad range of parameters;
- Physical Requirements: These requirements address the size, weight and transportability of the voting system; and
- 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.

3.2 Performance Requirements

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

a. Accuracy requirements, where requirements are specified for distinct processing functions of paper-based and DRE systems;

b. Environmental requirements, where no distinction is made between requirements for paper-based and DRE systems, but requirements for precinct and central count are described;

c. Vote data management requirements, where no differentiation is made between requirements for paper-based and DRE systems;

d. Vote recording requirements, where separate and distinct requirements are delineated for paper-based and DRE systems;

e. Conversion requirements, which apply only to paper-based systems;

f. Processing requirements, where separate and distinct requirements are delineated for paper-based and DRE systems; and

g. 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.

3.2.1 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 such 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 systems:

(1) Scanning ballot positions on paper ballots to detect selections for individual candidates and contests;

(2) Conversion of selections detected on paper ballots into digital data;

b. For all DRE systems:

(1) Recording the voter selections of candidates and contests into voting data storage; and

(2) Independently from voting data storage, recording voter selections of candidates and contests into ballot image storage.

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; and

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.

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 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.

3.2.2 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; and
- 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 Standards. 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 Standards.

The TDP 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.

3.2.2.1 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.

3.2.2.2 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.

3.2.2.3 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 system but that are used to support its storage, transportation, or operation, shall comply with the design and safety requirements of Subsection 3.4.8.

3.2.2.4 Electrical Supply

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

a. Precinct count systems shall operate with the electrical supply ordinarily found in polling places (120vac/60hz/1);

b. Central count systems shall operate with the electrical supply ordinarily found in central tabulation facilities or computer room facilities (120vac/60hz/1, 208vac/60hz/3, or 240vac/60hz/2); and

c. All systems 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 system shall retain the contents of all memories intact.

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

3.2.2.5 Electrical Power Disturbance

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:

a. Surges of 30% dip @10 ms;

b. Surges of 60% dip @100 ms & 1 sec;

c. Surges of >95% interrupt @5 sec;

d. Surges of ±15% line variations of nominal line voltage; and

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.

3.2.2.6 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 AC & DC external power lines;

b. ±1 kV all external wires >3m no control; and

c. ±2 kV all external wires control.

3.2.2.7 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. ±.5 kV DC line to line >10m;
d. ±.5 kV DC line to earth >10m; and
e. ±1 kV I/O sig/control >30m.

3.2.2.8 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.

3.2.2.9 Electromagnetic Radiation

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.

3.2.2.10 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.

3.2.2.11 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 AC & DC power; and
b. 10V, 20 sig/control >3m.

3.2.2.12 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.

3.2.2.13 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.

3.2.2.14 Environmental Control—Transit and Storage

Equipment used for vote casting, or for counting votes in a precinct count system, shall meet 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; and

d. Uncontrolled humidity equivalent to the procedure of MIL–STD–810D, Method 507.2, Procedure I—Natural Hot—Humid.

3.2.2.15 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 5 of the Standards and the Security requirements described in Section 6.

3.2.3 Election Management System (EMS) Requirements

The 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.

3.2.3.1 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; and

g. Log corrected data errors by the system.

3.2.3.2 Memory Stability

Electronic system memory devices, used to retain election management data, shall have demonstrated error-free data retention for a period of 22 months.

3.2.4 Vote Recording Requirements

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

3.2.4.1 Common Standards

All 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 makes provision for, the installation of, the voting device;

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; and

d. Be capable of meeting the accessibility requirements of Section 2.2.7.1.

3.2.4.2 Paper-Based Recording Standards

The paper-based recording requirements govern:

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

3.2.4.2.1 Paper Ballot Standards

Paper ballots used by paper-based voting systems shall meet the following standards:

a. Punches or marks that identify the unique ballot format, in accordance with Section 2.3.1.1.1.c., shall be

outside the area in which votes are recorded, so as to minimize the likelihood that these punches or marks will be mistaken for vote responses and the likelihood that recorded votes will obliterate these punches or marks;

b. If printed or punched 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; and

c. 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.

3.2.4.2.2 Punching Devices

Punching devices used by voting systems shall:

a. Be suitable for the type of ballot card specified;

b. Facilitate the clear and accurate recording of each vote intended by the voter;

c. Be designed to avoid excessive damage to vote recorder components; and

d. Incorporate features to ensure that the chad (debris) is completely removed, without damage to other parts of the ballot card.

3.2.4.2.3 Marking Devices

The TDP shall specify marking devices (such as pens or pencils) that, if used to make the prescribed form of mark, produce readable marked ballots such that the system meets the performance requirements for accuracy specified previously. These specifications shall identify:

a. Specific characteristics of marking devices that affect readability of marked ballots;

b. Performance capabilities with regard to each characteristic; and

c. For marking devices manufactured by multiple external sources, a listing of sources and model numbers that are compatible with the system.

3.2.4.2.4 Frames or Fixtures for Punchcard Ballots

The frame or fixture for punchcards shall:

a. Hold the ballot card securely in its proper location and orientation for voting;

b. When contests are not printed directly on the ballot card or sheet, incorporate an assembly of ballot label pages that identify the offices and issues corresponding to the proper ballot format for the polling place where it is used and that are aligned with the voting fields assigned to them; and

c. Incorporate a template to preclude perforation of the card except in the specified voting fields; a mask to allow punches only in fields designated by the format of the ballot; and a backing plate for the capture and removal of chad. This requirement may be satisfied by equipment of a different design as long it achieves the same result as the Standards with regard to:

(1) Positioning the card;

(2) Association of ballot label information with corresponding punch fields;

(3) Enabling of only those voting fields that correspond to the format of the ballot; and

(4) Punching the fields and the positive removal of chad.

3.2.4.2.5 Frames or Fixtures for Printed Ballots

A frame or fixture for printed ballot cards is optional. However, if such a device is provided, it shall:

a. Be of any size and shape consistent with its intended use;

b. Position the card properly;

c. Hold the ballot card securely in its proper location and orientation for voting; and

d. Comply with the requirements for design and construction contained in Section 3.4.

3.2.4.2.6 Ballot Boxes and Ballot Transfer Boxes

Ballot boxes and ballot transfer boxes, which serve as secure containers for the storage and transportation of voted ballots, shall:

a. Be of any size, shape, and weight commensurate with their intended use;

b. Incorporate locks or seals, the specifications of which are described in the system documentation;

c. Provide specific points where ballots are inserted, with all other points on the box constructed in a manner that prevents ballot insertion; and

d. 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.

3.2.4.3 DRE Systems Recording Requirements

The DRE systems 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.

3.2.4.3.1 Activity Indicator

DRE systems shall include an audible or visible activity indicator providing the status of each voting device. This indicator shall:

a. Indicate whether the device has been activated for voting; and

b. Indicate whether the device is in use.

3.2.4.3.2 DRE System Vote Recording

To ensure vote recording accuracy and integrity while protecting the anonymity of the voter, all DRE systems shall:

a. 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;

b. Incorporate redundant memories to detect and allow correction of errors caused by the failure of any of the individual memories;

c. Provide at least two processes that record the voter's selections that:

(1) To the extent possible, are isolated from each other;

(2) Designate one process and associated storage location as the main vote detection, interpretation, processing and reporting path; and

(3) 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.

d. Provide a capability to retrieve ballot images in a form readable by humans; and

e. Ensure that all processing and storage protects the anonymity of the voter.

3.2.4.3.3 Recording Accuracy

DRE systems shall meet the following requirements for recording accurately each vote and ballot cast:

a. Detect every selection made by the voter;

b. Correctly add permissible selections to the memory components of the device;

c. Verify the correctness of the detection of the voter selections and the addition of the selections to memory;

d. Achieve an error rate not to exceed the requirement indicated in Section 3.2.1;

e. 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; and

f. Maintain a log of corrected data.

3.2.4.3.4 Recording Reliability

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 Section 3.4.3.

3.2.5 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 punches or 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.

3.2.5.1 Ballot Handling

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

3.2.5.1.1 Capacity (Central Count)

The capacity to convert the punches or 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.

3.2.5.1.2 Exception Handling (Central Count)

This requirement refers to the handling of ballots for a central count system when they are unreadable or when some condition is detected requiring that the cards be segregated from normally processed ballots for human review. In response to an unreadable ballot or a write-in vote all central count paper-based systems shall:

a. Outstack the ballot, or

b. Stop the ballot reader and display a message prompting the election official or designee to remove the ballot, or

c. Mark the ballot with an identifying mark to facilitate its later identification.

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 race. If enabled, these capabilities shall perform one of the above actions in response to the indicated condition.

3.2.5.1.3 Exception Handling (Precinct Count)

This requirement refers to the handling of ballots for a precinct count system when they are unreadable or when some condition is detected requiring that the cards be segregated from normally processed ballots for human review. All paper based precinct count systems shall:

a. In response to an unreadable or blank ballot, return the ballot and provide a message prompting the voter to examine the ballot;

b. 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;

c. In response to a ballot with an overvote the system shall:

(1) Provide a capability to identify an overvoted ballot;

(2) Return the ballot;

(3) Provide an indication prompting the voter to examine the ballot;

(4) Allow the voter to submit the ballot with the overvote; and

(5) Provide a means for an authorized election official to deactivate this capability entirely and by contest; and

d. In response to a ballot with an undervote the system shall:

(1) Provide a capability to identify an undervoted ballot;

(2) Return the ballot;

(3) Provide an indication prompting the voter to examine the ballot;

(4) Allow the voter to submit the ballot with the undervote; and

(5) Provide a means for an authorized election official to deactivate this capability.

3.2.5.1.4 Multiple Feed Prevention

Multiple feed refers to the situation arising when a ballot reader attempts to read more than one ballot at a time. The requirements govern the ability of a ballot reader to prevent multiple feed or to detect and provide an alarm indicating multiple feed.

a. 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.

b. The frequency of multiple feeds with ballots intended for use with the system shall not exceed 1 in 10,000.

3.2.5.2 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:

- Recognize vote punches or marks, or the absence thereof, for each possible selection on the ballot;
- Discriminate between valid punches or marks and extraneous perforations, smudges, and folds; and
- 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:

a. Detect punches or marks that conform to vendor specifications with an error rate not exceeding the requirement indicated in Section 3.2.1;

b. Ignore, and not record, extraneous perforations, smudges, and folds; and

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

3.2.6 Processing Requirements

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.

3.2.6.1 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.

3.2.6.1.1 Processing Accuracy

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:

a. 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;

b. 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;

c. The vote selection error rate shall include all errors from any source; and

d. The vote selection error rate shall not exceed the requirement indicated in Section 3.2.1.

3.2.6.1.2 Memory Stability

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).

3.2.6.2 DRE System Processing Requirements

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

3.2.6.2.1 Processing Speed

DRE voting systems shall meet the following requirements for processing speed:

a. Operate at a speed sufficient to respond to any operator and voter input without perceptible delay (no more than three seconds); and

b. 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.

3.2.6.2.2 Processing Accuracy

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 polling places have been closed. DRE voting systems shall:

a. Produce reports that are completely consistent, with no discrepancy among reports of voting device data produced at any level; and

b. 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.

3.2.6.2.3 Memory Stability

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.

3.2.7 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.

3.2.7.1 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 Section 3.2.2. Examples of removable storage media include: programmable read-only memory (PROM), random access memory (RAM) with battery backup, magnetic media, or optical media.

3.2.7.2 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; and

c. Alphanumeric entries generated as part of the audit record.

3.2.8 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 intermediate levels. These capabilities allow the system to:

a. Consolidate voting data from polling place data memory or transfer devices;

b. Report polling place summaries; and

c. 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.

3.2.8.1 Data File Management

All voting systems shall provide the capability to:

a. Integrate voting data files with ballot definition files;

b. Verify file compatibility; and

c. Edit and update files as required.

3.2.8.2 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.

3.3 Physical Characteristics

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

3.3.1 Size

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

3.3.2 Weight

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

3.3.3 Transport and Storage of Precinct Systems

All precinct systems shall:

a. Provide a means to safely and easily handle, transport, and install polling place equipment, such as wheels or a handle or handles; and

b. Be capable of using, or be provided with, a protective enclosure rendering the equipment capable of withstanding:

(1) Impact, shock and vibration loads accompanying surface and air transportation; and

(2) Stacking loads accompanying storage.

3.4 Design, Construction, and Maintenance Characteristics

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

3.4.1 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 TDP, an approved parts list; and

c. Exclude parts or components not included in the approved parts list.

3.4.2 Durability

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

3.4.3 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 consist 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:

a. Loss of one or more functions; or

b. Degradation of performance such that the device is unable to perform its intended function for longer than 10 seconds.

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

3.4.4 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; and
- 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 ITA. Although a more quantitative basis for assessing maintainability, such as the mean to repair the system is desirable, the qualification of a system is conducted before it is approved for sale and thus before a broader base of maintenance experience can be obtained.

3.4.4.1 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;

c. Presence of labels and alarms related to failures; and

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

3.4.4.2 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;

b. 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; and

g. Adjust, align, tune, or service components.

3.4.5 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:

(1) Recording voter selections (such as by ballot marking or punch); and

(2) Scanning the punches or marks on paper ballots and converting them into digital data;

b. For all DRE systems, recording and storing the voter's 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; and

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

$$Ai = (MTBF)/(MTBF + MTTR)$$

Mean Time to Repair (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 ninety nine 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 attribute.

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:

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

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

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

3.4.6 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; and

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.

3.4.7 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; and

b. Ensure that components provided by external suppliers are free from damage or defect that could make them unsatisfactory for their intended purpose.

3.4.8 Safety

All voting systems shall meet the following requirements for safety:

a. All voting systems and their components shall be designed so as 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; and

c. Equipment design for personnel safety shall be equal to or better than the appropriate requirements of the Occupational Safety and Health Act (OSHA), as identified in Title 29, part 1910, of the Code of Federal Regulations.

Volume I, Section 4

Table of Contents

4 Software Standards

4.1 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 standards 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 standards 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 Standards 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 qualification process.

4.1.1 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; and
- Software developed by the voting jurisdiction.

Compliance with the requirements of the software standards is assessed by several formal tests, including code examination. Unmodified software is not subject to code examination; however, source code generated by a package and embedded in software modules for compilation or interpretation shall be provided in human readable form to the ITA. The ITA 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 to the ITA, in the TDP, a

record of all user selections made during software installation. The vendor shall also submit a record of all configuration changes made to the software following its installation. The ITA shall confirm the propriety and correctness of these user selections and configuration changes.

4.1.2 Location and Control of Software and Hardware on Which it Operates

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); and
- 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 6 of the Standards.

4.1.3 Exclusions

Some voting systems use equipment, such as personal computers, that may be used for other purposes and have resident on the equipment general purpose software such as operating systems, programming language compilers, database management systems, and Web browsers. Such software is governed by the Standards unless:

- The software provides no support of voting system capabilities;
- The software is removable, disconnectable, or switchable such that it cannot function while voting system functions are enabled; and
- Procedures are provided that confirm that the software has been removed, disconnected, or switched.

4.2 Software Design and Coding Standards

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

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

4.2.1 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.

4.2.2 Software Integrity

Self-modifying, dynamically loaded, or interpreted code is prohibited, except under the security provisions outlined in section 6.4.e. This prohibition is to ensure that the software tested and approved during the qualification 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:

- Unbounded arrays or strings (includes buffers used to move data);
- Pointer variables; and
- Dynamic memory allocation and management.

4.2.3 Software Modularity and Programming

Voting system application software, including 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 concept 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 following rules:

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 ITA 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; and

[1] Some software languages and development environments use a different definition of module but this principle still applies.

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/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.

4.2.4 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);

b. 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;

c. 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); and

d. 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.

4.2.5 Naming Conventions

Voting system software shall use the following naming conventions:

a. Object, function, procedure, and variable names shall be chosen so as 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, verbs to represent functions, etc.;

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; and

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.

4.2.6 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 ITAs shall test for compliance; or

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

These standards 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.

4.2.7 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:

(1) The purpose of the unit and how it works;

(2) Other units called and the calling sequence;

(3) A description of input parameters and outputs;

(4) File references by name and method of access (read, write, modify, append, etc.);

(5) Global variables used; and

(6) 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; and

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

4.3 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 in which to resolve most contested elections and support other activities related to the reconstruction and investigation of a contested election; and

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.

4.4 Audit Record Data

Audit trails are essential to ensure the integrity of a voting system. Operational requirements for audit trails are described in Section 2.2.5.2 of the Standards. 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.

4.4.1 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 for an office or issue;

b. The combinations of voting patterns permitted or required by the jurisdiction;

c. The inclusion or exclusion of offices or issues 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's location;

e. Manual data maintained by election personnel;

f. Samples of all final ballot formats; and

g. Ballot preparation edit listings.

4.4.2 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 the polling place's 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; and

g. For systems that use a public network, provide a report of test ballots that includes:

(1) Number of ballots sent;

(2) When each ballot was sent;

(3) Machine from which each ballot was sent; and

(4) Specific votes or selections contained in the ballot.

4.4.3 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:

(1) The source and disposition of system interrupts resulting in entry into exception handling routines;

(2) All messages generated by exception handlers;

(3) The identification code and number of occurrences for each hardware and software error or failure;

(4) 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;

(5) Other exception events such as power failures, failure of critical hardware components, data transmission errors, or other type of operating anomaly;

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:

(1) Diagnostic and status messages upon startup;

(2) The ''zero totals'' check conducted before opening the polling place or counting a precinct centrally;

(3) For paper-based systems, the initiation or termination of card reader and communications equipment operation; and

(4) 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; and

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.

4.4.4 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 reports of them on a printer. 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); and

e. For paper-based systems only, the total number of ballots both processed and unprocessable; 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.

4.5 Vote Secrecy (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; and

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.

Volume I, Section 5

Table of Contents

5 Telecommunications

5.1 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 Standards, 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, perhaps 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 compliment the network security requirements found in Volume I Section 6, which include requirements for voter and administrator access, availability of network service, data confidentiality, and data integrity. Most importantly, security services will restrict access to local election system components from public resources, and these services will also restrict access to voting system data while it is in transit across public resources. (This is corollary to voting supervisors controlling local election systems and not assuming control over public resources.)

5.1.1 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:
- Standard landline;
- Wireless;
- Microwave;
- Very Small Aperture Terminal (VSAT);
- Integrated Services Digital Network (ISDN); and
- Digital Subscriber Line (DSL);

—High-speed telecommunications lines (public and private):
- FT–1, T–1, T–3;
- Frame Relay; and
- Private line;

—Cabling technologies:
- Universal Twisted Pair (UTP) cable (CAT 5 or higher);
- Ethernet hub/switch; and
- Wireless connections (Radio Frequency (RF) and Infrared);

—Communications routers;

—Modems, whether internal and external to personal computers, computer servers, and other voting system components (whether installed at the polling place or central count location);

—Modem drivers, dial-up networking software;

—Channel service units (CSU)/Data service units (DSU) (whether installed at the polling place or central count location); and

—Dial-up networking applications software.

5.1.2 Telecommunications Operations and Providers

This section applies to voting-related transmissions over public networks, such as those provided by regional telephone companies 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 settings supervised by election officials, such as polling places or central offices. These standards apply to:

- Components acquired by the jurisdiction for the purpose of voting, including components installed at the poll site or a central office (including central site facilities operated by vendors or contractors); and
- Components acquired by others (such as school systems, libraries, military installations and other public organizations) that are used at settings 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)

5.1.3 Data Transmissions

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; and
- *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 standards 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 indicated below:

- Polling places;
- Precinct count facilities; and
- Central count facilities (whether operated by the jurisdiction or a contractor).

5.2 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.

5.2.1 Accuracy

The telecommunications components of all voting systems shall meet the accuracy requirements of Section 3.2.1.

5.2.2 Durability

The telecommunications components of all voting systems shall meet the durability requirements of Section 3.4.2.

5.2.3 Reliability

The telecommunications components of all voting systems shall meet the reliability requirements of Section 3.4.3.

5.2.4 Maintainability

The telecommunications components of all voting systems shall meet the maintainability requirements of Section 3.4.4.

5.2.5 Availability

The telecommunications components of all voting systems shall meet the availability requirements of Section 3.4.5.

5.2.6 Integrity

For WANs using public telecommunications, boundary definition and implementation shall meet the following requirements.

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 (DSU/CSU) (though the precise technology may vary, being such things as cable modems or routers). Regardless of the technology used, the boundary point must ensure that everything on one side is locally configured and controlled while everything on the other side is controlled by an outside service provider; and

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 causing total loss of voting capabilities at any polling place.

5.2.7 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:

d. Notify the user of the successful or unsuccessful completion of the data transmission; and

e. In the event of unsuccessful transmission, notify the user of the action to be taken.

Volume I, Section 6

Table of Contents

6.0 Security

Section 6.0 addresses four new, specific aspects of voting systems security:

1. Independent Dual Verification Voting Systems: Definition and characteristics of voting systems that produce multiple records of votes. A future version of the VVSG will require that voting systems produce multiple records of ballots or receipts for auditing purposes (Section 6.0.1, Informative).

2. Security Requirements for Voter Verified Paper Audit Trails: Requirements for voter verified paper audit trails, if a State chooses to require them (Section 6.0.2, Normative).

3. Use of Wireless Networking in Voting Systems: Requirements for wireless networks and the data sent across wireless networks (Section 6.0.3, Normative).

4. Security Requirements for Software Distribution and Setup Validation of Voting System: Requirements for (a) the secure distribution of voting systems software and (b) for verifying that voting systems are operating with the correct software configuration (Section 6.0.4, Normative).

1. Security Overview (Informative)

This section is a discussion of independent verification systems followed by characteristics of independent verification systems which will be used as the basis for future requirements. The characteristics are preliminary and will be evolving with further research.

1. Independent Dual 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 choices whose handling requirements are reasonable. To meet this objective, there are many factors to consider in an electronic voting system's design, including:

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

Independent Dual Verification (IDV) systems have as their primary objective the production of ballot records that are capable of being used in audits in which their correctness can be audited to very high levels of precision. The primary security issues addressed by IDV systems are:

- Whether electronic voting systems are accurately recording ballot choices, and
- Whether the ballot record contents can be audited precisely post-election.

The threats addressed by IDV systems are those that could cause a voting system to inaccurately record the voter's intent or cause a voting system's records to become damaged, i.e., inserted, deleted, or changed. These threats could occur via any number of means including accidental damage or various forms of fraud. 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.

1.1 Independent Dual Verification Systems: Improved Accuracy in Audits

Independent Verification is the top-level categorization for electronic voting systems that produce multiple records of ballot choices whose contents are capable of being audited to high levels 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 the voter's choices 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 the voter's choices and then copies it to some write-once media.
- The voter must be able to verify that both records are correct, e.g., verify his or her choices on the voting system's display and also verify the second record of choices stored on the write-once media.
- The verification processes for the two verifications 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 different systems produced by different vendors.
- 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 by using an electronic voting system, 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 above, 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 up on 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.

1.2 Issues in Handling Multiple Records Produced by Independent Dual Verification Systems

There are several fundamental questions that need to be addressed when designing the structure and selecting the physical characteristics of IDV systems 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, and
- 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.

As a consequence, 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, such as the following:

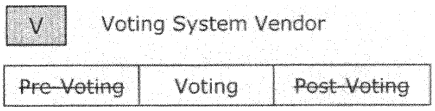
- Associating unique identifiers with corresponding records, e.g., an individual paper record sharing a unique identifier with its corresponding electronic record,
- Including an identification of the specific voting system that produced the records, such as a serial number identifier or by having the voting system digitally sign the records using public key cryptography,
- 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, and
- Structuring the records in open, publicly documented formats that can be readily analyzed on different computing platforms.

The ease or relative difficulty with which some types of records must be handled is also a determining factor in the practical capability to conduct precise audits, given that some types of records are better suited to different types of 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 voters or poll workers and thus be more susceptible to damage or loss. 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.

2. Core Characteristics for Independent Verification Systems

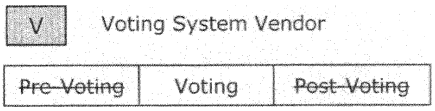
This section contains a preliminary set of characteristics for IDV systems. These characteristics are fundamental in nature and apply to all categories of IDV systems. They will form the basis for future requirements for independent verification systems.

2.1 An Independent Dual Verification Voting System Produces Two Distinct Sets of Records of Ballot Choices Via Interactions With the Voter Such That One Set of Records Can be Compared Against the Other to Check Their Equality of Content



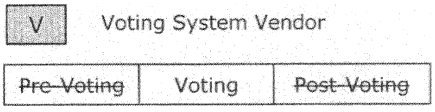
Discussion: This is the fundamental core definition for IDV systems. The records can be checked against one another to determine whether or not the voter's choices were correctly recorded.

2.1.1 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



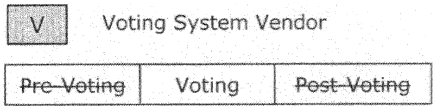
Discussion: Direct Verification involves using human senses, e.g., directly verifying a paper record via one's eyesight. Indirect Verification involves using an intermediary to perform the verification, e.g., verifying an electronic ballot image at the voting system.

2.1.2 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



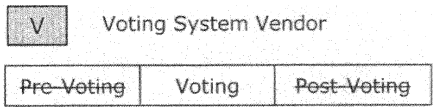
Discussion: The records must be stored on different media and handled independently of each other, so that no one process could compromise all records. If an attack can alter one record, it should still be very difficult to alter the other record.

2.1.2.1 At Least One Record Is Highly Resistant to Damage or Alteration and Should be Capable of Long-Term Storage



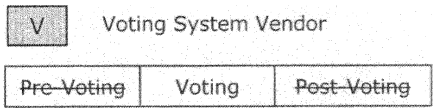
Discussion: At least one of the records should be difficult to alter or damage so that it could be used in case the counted records are damaged or lost.

2.1.3 The Processes of Verification for the Multiple Records do not all Depend for Their Integrity on the Same Device, Software Module, or System, and are Sufficiently Separate Such That Each Record Provides Evidence of the Voter's Choices Independently of Its Other Corresponding Record



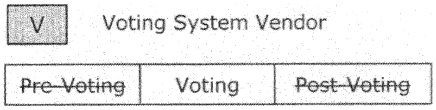
Discussion: For example, the verification of an electronic record on a DRE is not sufficiently separate from the verification of an electronic record located on a token but performed by the same DRE as the verification for the first record. Verification of the paper record by one's senses is sufficiently separate in this case.

2.1.4 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



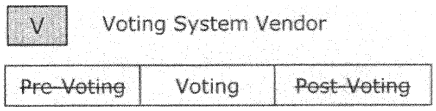
Discussion: For example, an electronic record can be used in an efficient counting process. A second paper record can be used to verify the accuracy of the electronic record; however its suitability for efficient counting is less clear. If a paper record can be used in an automated scan process, it may be more suitable.

2.1.5 The Records Within a Set are Linked to Their Corresponding Records in the Other Set by Including a Unique Identifier Within Each Record That Can Be Used to Identify the Record's Corresponding Record in the Other Set



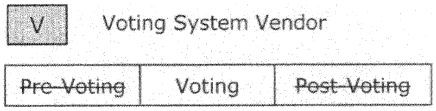
Discussion: The identifier should serve the purpose of uniquely identify the record so as to identify duplicates and/or for cross-checking two record types.

2.1.6 Each Record Includes an Identification of the Voting Site/Precinct

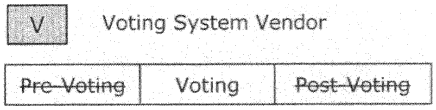


Discussion: If the voting site and precinct are different, both should be included.

2.1.7 The Records Include Information Identifying Whether the Balloting is Provisional, Early, or on Election Day, and Information That Identifies the Ballot Style In Use

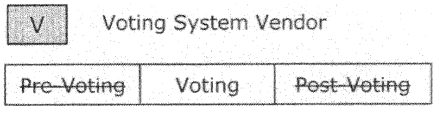


2.1.8 The Records Include a Voting Session Identifier that is Generated When The Voting Station is Placed in Voting Mode and That Can Be Used to Identify The Records as Being Created During That Voting Session



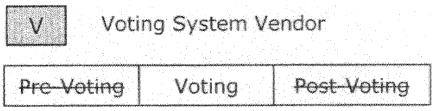
Discussion: If there are several voting sessions on the same voting station on the same day, the voting session identifiers must be different. They should be generated from a random number generator.

2.1.9 The Records Include An Identifier of The Voting System that is Unique To that Style of Voting Systems



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

2.1.10 The cryptographic Software in Independent Verification Voting Systems is Approved by The U.S. Government's Cryptographic Module Validation Program (CMVP) as Applicable



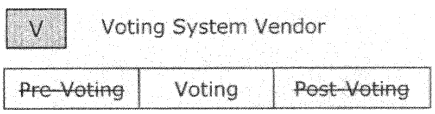
Discussion: The voting systems may use cryptographic software for a number of different purposes, including calculating checksums, encrypting records, authentication, generating random numbers, and for digital signatures. This software should be reviewed and approved by the Cryptographic Module Validation Program. 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.*

2. Requirements for Voter Verified Paper Audit Trails (Normative)

This section contains requirements for Voter Verified Paper Audit Trail (VVPAT) voting systems. VVPAT is not mandatory. These requirements apply only to voting systems that include a VVPAT component and are consistent with the definition of Independent Dual Verification (IDV) systems from Section 6.0.1. Requirements for usability, accessibility, and privacy from Volume I, Section 2.2.7 apply to VVPAT. The requirements in this section apply only to VVPAT systems; the requirements do not apply to other types of voting systems and are not intended to in any way restrict use or operation of other types of voting systems.

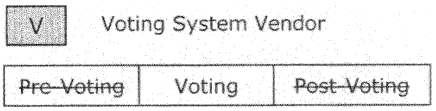
1. Display and Print a Paper Record

1.1 The Voting Station Shall Print and Display a Paper Record of the Voter's Ballot Choices Prior to the Voter Making the Ballot Choices Final



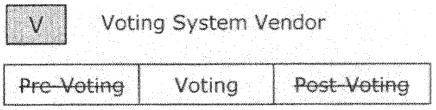
Discussion: This is the basic requirement for VVPAT capability. It requires that the paper record be created as a distinct representation of the voter's ballot choices. It requires that the paper record contain the same information as contained in the electronic record and be suitable for use in verifications and recounts of the election and of the voting station's electronic records. Thus, either the paper or electronic record could be used as the ballot of record for the election.

1.1.1 The Paper Record Shall Constitute A Complete Record of Ballot Choices That Can Be Used To Assess The Accuracy of The Voting Station's Electronic Record, To Verify The Election Results, And In Full Recounts.



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

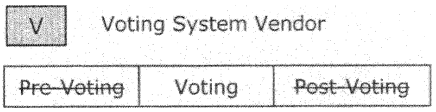
1.1.2 The Paper Record Shall Contain All Information Stored in the Electronic Record



Discussion: The electronic record cannot hide any information related to ballot choices; all information relating to ballot choices 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.

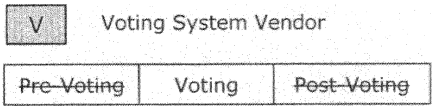
2. VVPAT Voting Station Usability

2.1 All Usability Requirements From Volume I, Section 2.2.7 Shall Apply to Voting Stations With VVPAT



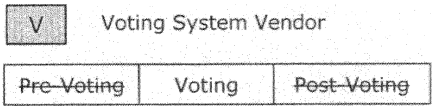
Discussion: The requirements in this section are in addition to those requirements from Section 2.2.7. They require that the paper record be formatted and displayed so that the voter is able to verify his or her votes with maximum reasonable ease and satisfaction, and that instructions be provided to the voter to handle all relevant aspects of the voter verification.

2.1.1 The Voting Station 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, (a) 3.0–4.0 mm and (b) 6.3–9.0 mm, Under Control of the Voter or Poll Worker

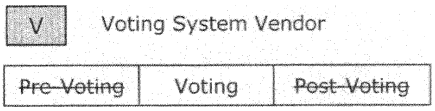


Discussion: In keeping with requirements in Section 2.2.7, the paper record should use the same font sizes as displayed by the voting station, but at least be capable of 3.0 mm. While larger font sizes may assist most voters with poor vision, certain disabilities such as tunnel vision are best addressed by smaller font sizes.

2.1.2 The Paper and Electronic Records Shall Be Presented so as to Allow for Easy, Simultaneous Comparison

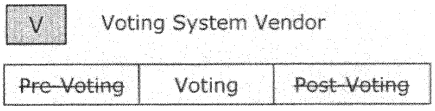


2.1.2.1 The Paper and Electronic Records Shall Be Positioned so That the Voter Can, at the Same Posture, Easily Read and Compare the Two Records



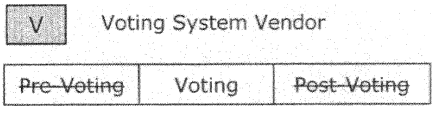
Discussion: The voter should not have to shift positions when comparing the records.

2.1.2.2 If The Paper Record Cannot Be Displayed in Its Entirety, a Means Shall Be Provided to Allow the Voter to View the Entire Ballot

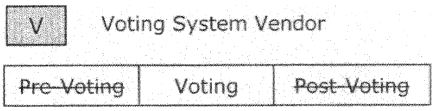


Discussion: Possible solutions include scrolling the paper or printing a new sheet of paper.

2.1.2.3 If the Paper Record Cannot Be Displayed in Its Entirety on a Single Page, Each Page of the Record Shall Be Numbered and the Last Page Shall Be Clearly Distinguished



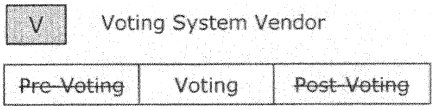
2.1.3 The Instructions for Performing the Verification Process Shall Be Made Available to the Voter in A Location on the Voting Station



Discussion: All instructions need to meet the accessibility requirements contained in Section 2.2.7.

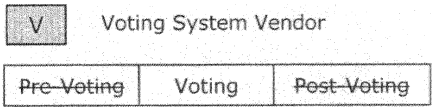
3. VVPAT Voting Station Accessibility

3.1 All Accessibility Requirements From Section 2.2.7 Shall Apply to Voting Stations With VVPAT



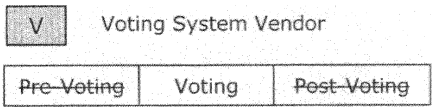
Discussion: Requirements in this section are in addition to the accessibility and alternative language requirements from Section 2.2.7. They make explicit that an accessible vote verification procedure for voters be provided at voting sites, including voters with disabilities, limited English proficiency (LEP), and voters with Native American and Alaska Native languages that are not written.

3.1.1 The Voting Station Shall Display, Print, and Store a Paper Record in any of the Alternative Languages Chosen for Making Ballot Selections



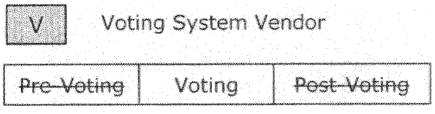
Discussion: For the purposes of voter privacy, it must not be possible to identify voters based on their use of alternative languages. Requirement 6.0.2.5.1.3 addresses this issue.

3.1.1.1 For the Purposes of Verification, Candidate Names on the Records Shall Be in English



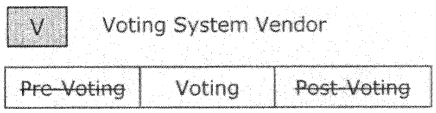
Discussion: This requirement is included to assist manual auditing of the paper records.

3.1.1.2 Other Markings Not Related to Ballot Selection on The Paper Record Shall Be In English



Discussion: Other markings may include designations of the precinct and the election.

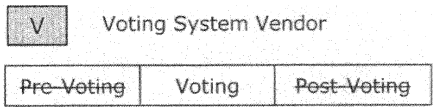
3.1.2 If the Normal Procedure Includes VVPAT, the Accessible Voting Station Should Provide Features That Enable Voters Who Are Blind to Perform This Verification



Discussion: This requirement is repeated from Section 2.2.7 and included here for emphasis. This requirement will be mandatory in future versions.

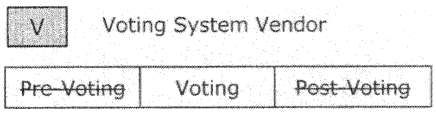
4. Approve or Spoil the Paper Record

4.1 The Voting Station Shall Allow the Voter to Approve or Spoil the Paper Record



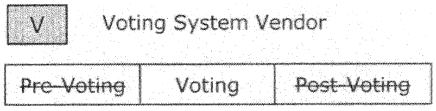
Discussion: The voting station cannot create an electronic record without its corresponding paper record. It requires that the voting station mark the electronic record as accepted or spoiled in the voter's presence, and if spoiled, the corresponding electronic record be marked as spoiled and be preserved. It requires that the voting station display a warning message when a spoil limit is reached.

4.1.1 The Voting Station Shall, in the Presence of The Voter, Mark the Paper Record as Being Accepted by the Voter or Spoiled



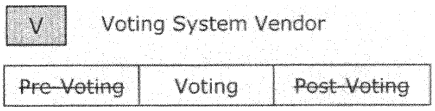
Discussion: If a paper record is marked as spoiled, then the corresponding electronic record is presented to the voter for update.

4.1.2 The Voting Station Should Mark and Preserve Electronic and Paper Records That Have Been Spoiled



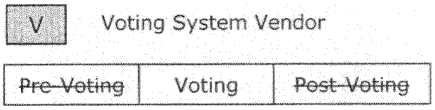
Discussion: For the purposes of reconciliation of records, electronic and paper spoiled records should be retained and analyzed.

4.1.3 Following the Close of Polls, a Means Shall Be Provided to Reconcile the Number of Spoiled Paper Records With the Number of Occurrences of Spoiled Electronic Records, and Procedures Shall Be in Place to Address Any Discrepancies



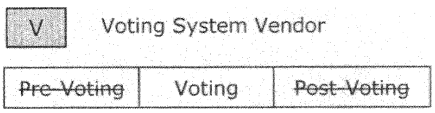
[Best practice for voting officials] Appropriate procedures are needed for reconciling the number of spoiled paper records with the number of spoiled electronic records and for addressing any discrepancies after the close of polls.

4.1.4 Prior to the Maximum Number of Spoiled Ballots Occurring, the Voting Station Shall Display a Warning Message to the Voter Indicating That the Voter May Spoil Only One More Ballot



Discussion: The maximum number of spoiled ballots varies from state to state.

4.1.5 If the Maximum Number of Spoiled Ballots Occurs, the Voting Station Should Provide a Way to Permit the Voter to Cast a Ballot, as Required



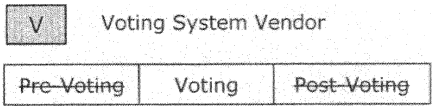
Discussion: Possible solutions include using other equipment, using a paper ballot, or accepting the last ballot cast. This capability defined by state and local jurisdiction.

[Best practice for voting officials] Appropriate procedures are needed to permit the voter to cast a ballot if the maximum number of spoiled ballots occurs.

[Best practice for voting officials] Appropriate procedures are needed to address situations in which a voter is unable to review the paper record.

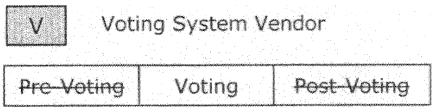
[Best practice for voting officials] Appropriate procedures are needed to address situations in which a voter indicates that the electronic and paper records do not match. If the records do not match, a potentially serious error has likely occurred, and voting officials may need to take appropriate actions such as removing the voting station from service and quarantining its records for later analysis.

4.1.6 The Voting Station Should Not Record the Electronic Record as Being Approved By The Voter Until the Paper Record Has Been Stored



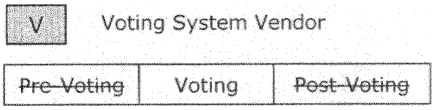
Discussion: In general it is better not to record any record as being approved until the record that is independent of the voting system is approved by the voter.

4.1.7 Vendor Documentation Shall Include Procedures for Returning a Voting Station 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



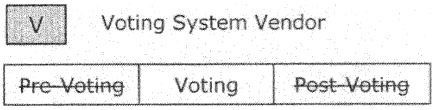
5. Preserve Voter Privacy and Anonymity

5.1 The Voter's Privacy and Anonymity Shall be Preserved During the Process of Recording, Verifying, and Auditing Ballot Choices

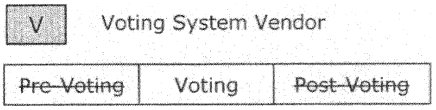


Discussion: Privacy requirements from Section 2.2.7 apply to voting stations with VVPAT; requirements in this section are in addition to those requirements from Section 2.2.7. They require that the voter's privacy be maintained during the verification step, including requirements that the paper record contain no human or machine-readable markings that could identify the voter and that the paper and electronic records be stored in ways that preserve the privacy and anonymity of the voter.

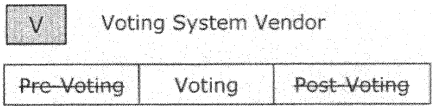
5.1.1 The Privacy and Anonymity of the Voter's Verification of His or Her Ballot Choices on the Electronic and Paper Records Shall Be Maintained



5.1.1.1 When the Voter is Responsible for Depositing a Paper Record in the Ballot Box, the Accessible Voting Station Shall Maintain the Privacy and Anonymity of Voters Unable to Manually Handle Paper

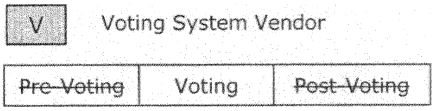


5.1.2 The Electronic and Paper Records Shall be Created and Stored in Ways that Preserve the Privacy and Anonymity of the Voter



Discussion: This can be accomplished in various ways including shuffling the order of the records or other methods to separate the order of stored records.

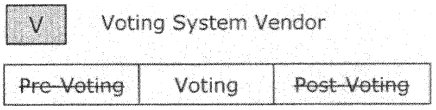
5.1.3 The Privacy and Anonymity of Voters Whose Paper Records Contain Any of the Alternative Languages Chosen for Making Ballot Selections Shall be Maintained



Discussion: One method for accomplishing this is to ensure that no less than, e.g., five voters use any of the alternative languages for their ballot selections.

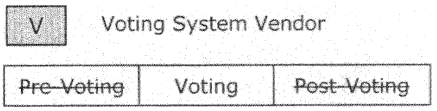
[Best practice for voting officials] Appropriate procedures are needed to ensure the privacy and anonymity of voters whose paper records contain any of the alternative languages chosen for making ballot selections.

5.1.4 The Voter Shall Not be Able to Leave the Voting Area With the Paper Record if the Information on the Paper Record Can Directly Reveal the Voter's Choices



[Best practice for voting officials] Appropriate procedures are needed to prevent voters from leaving the voting area with a paper record that can directly reveal the voter's choices.

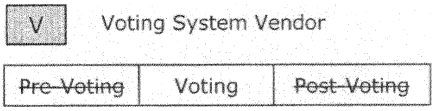
5.1.5 Unique Identifiers Shall Not be Displayed in a Way That Is Easily Memorable by the Voter



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.

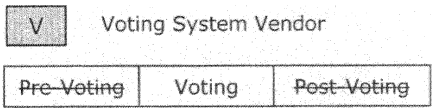
6. Electronic and Paper Record Structure

6.1 The Voting Station's Ballot Records Shall Be Structured and Contain Information So as to Support Highly Precise Audits of Their Accuracy



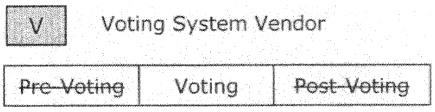
Discussion: It requires that electronic records and paper records contain election precinct information, information to link the paper record to its corresponding electronic record, and information identifying the voting station. It requires that the electronic records be maintained in a format that can be exported to a different computer, *e.g.,* a personal computer, and that the format be well-documented to support analysis of the records.

6.1.1 All Cryptographic Software in the Voting Station Should be Approved by the U.S. Government's Cryptographic Module Validation Program (CMVP) as Applicable

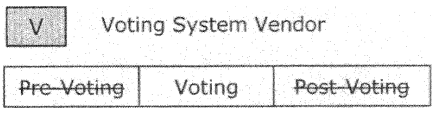


Discussion: The voting station may use cryptographic software for a number of different purposes, including calculating checksums, encrypting records, authentication, generating random numbers, and for digital signatures. This software should be reviewed and approved by the Cryptographic Module Validation Program. 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 web site is *http://csrc.nist.gov/cryptval.*

6.1.2 The Electronic and Paper Records Shall Include Information About the Election

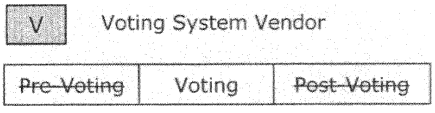


6.1.2.1 The Voting Station Shall be Able to Include an Identification of the Particular Election, the Voting Site/Precinct, and the Voting Station

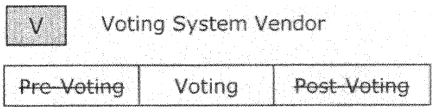


Discussion: If the voting site and precinct are different, both should be included. Some of this information may have to be excluded in certain cases to protect voter privacy.

6.1.2.2 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

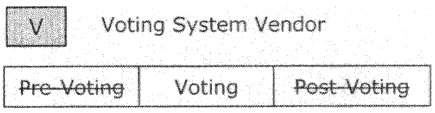


6.1.2.3 The Records Shall Include a Voting Session Identifier That is Generated When the Voting Station is Placed in Voting Mode and That can be Used to Identify the Records as Being Created During that Voting Session



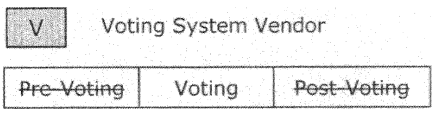
Discussion: If there are several voting sessions on the same voting station on the same day, the voting session identifiers must be different. They should be generated from a random number generator.

6.1.3 The Electronic 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

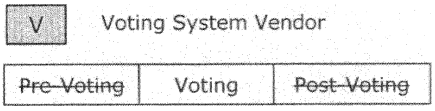


Discussion: The identifier serves the purpose of uniquely identifying the record so as to identify duplicates and/or for crosschecking two record types.

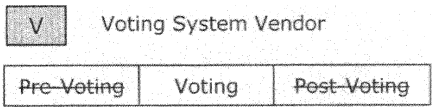
6.1.4 The Voting Station Should Generate and Store a Digital Signature for Each Electronic Record



6.1.5 The Electronic Records Shall be Able to be Exported for Auditing or Analysis on Standards Based and/or COTS Information Technology Computing Platforms

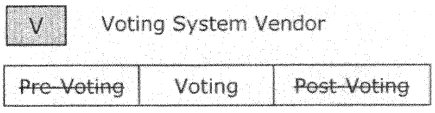


6.1.5.1 The Exported Electronic Records Shall be in a Publicly Available, Non-Proprietary Format



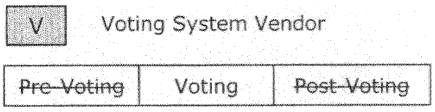
Discussion: It is advantageous when all electronic records, regardless of manufacture, use the same format or can easily be converted to a publicly available, non-proprietary format, e.g., the OASIS Election Markup Language (EML) Standard.

6.1.5.2 The Voting Station Should Export the Records Accompanied by a Digital Signature of the Collection of Records, Which Shall be Calculated on the Entire Set of Electronic Records and Their Associated Digital Signatures

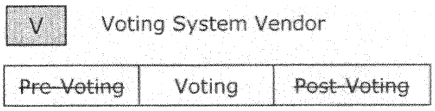


Discussion: This is necessary to determine if records are missing or substituted.

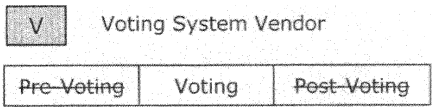
6.1.5.3 The Voting System Vendor Shall Provide Documentation as to the Structure of the Exported Records and How They Shall be Read and Processed by Software



6.1.5.4 The Voting System Vendor Shall Provide a Software Program That Will Display the Exported Records and That May Include Other Capabilities Such as Providing Vote Tallies and Indications of Undervotes

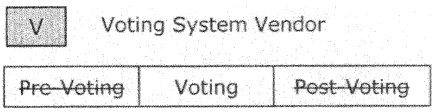


6.1.6 The Paper Record Should be Created in a Format That May be Made Available Across Different Manufacturers of Electronic Voting Systems



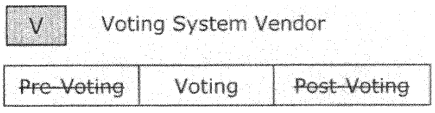
Discussion: Future standards may require some commonality in the format of paper records.

6.1.7 The Paper Record Shall be Created Such That Its Contents Are Machine-Readable



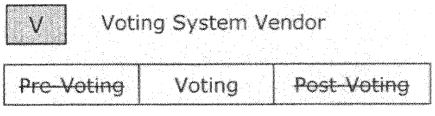
Discussion: This can be done by using specific OCR fonts.

6.1.7.1 The Paper Record Should Contain Error Correcting Codes for the Purposes of Detecting Read Errors and for Preventing Other Markings on the Paper Record to be Misinterpreted When Machine Reading the Paper Record

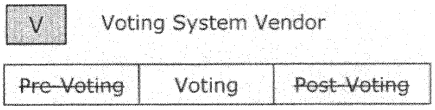


Discussion: This requirement is not mandatory if, for example, a state prohibits non-human-readable information on the paper record. This requirement serves the purpose of detecting scanning errors and preventing stray or deliberate markings on the paper from being interpreted as valid data.

6.1.8 Any Automatic Accumulation of Electronic or Paper Records Shall be Capable of Detecting and Discarding Duplicate Copies of the Records

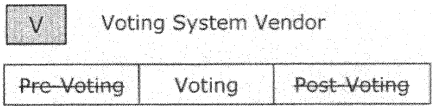


6.1.9 The Voting Station Should be Able to Print a Barcode With Each Paper Record that Contain the Human Readable Contents of the Paper Record and Digital Signature Information



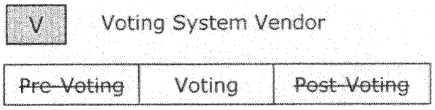
Discussion: This requirement is not mandatory if, for example, a state prohibits non-human-readable information on the paper record.

6.1.9.1 The Barcode Shall Use an Industry-Standard Format and Shall be Able to be Read Using Readily Available Commercial Technology

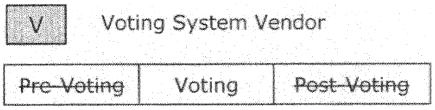


Discussion: Examples of such codes are Maxi Code or PDF417.

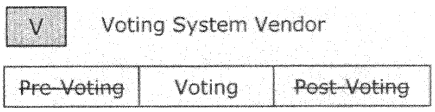
6.1.9.2 If the Paper Record's Corresponding Electronic Record Contains a Digital Signature, the Digital Signature Shall be Included in the Barcode



6.1.9.3 The Barcode Shall Not Contain Any Information Other Than the Paper Record's Human Readable Content and Digital Signature Information

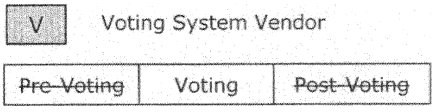


6.1.10 The Voting System Vendor Shall Provide Full Documentation of Procedures for Exporting Its Electronic Records and Reconciling Its Electronic Records With Its Paper Records

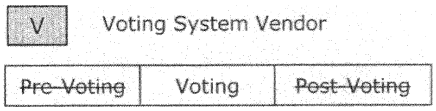


7. Equipment Security and Reliability

7.1 The Voting Station Equipment Shall be Secure, Reliable, and Easily Maintained

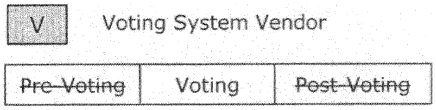


7.1.1 The Voting Station Shall be Physically Secure From Tampering, Including Intentional Damage



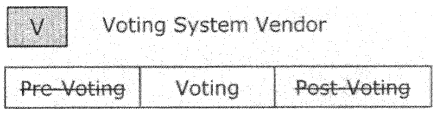
[Best practice for voting officials] Appropriate procedures are needed to ensure that voting systems are physically secured from tampering and intentional damage.

7.1.1.1 The Voting Station Shall Provide a Standard, Publicly Documented Printer Port (or the Equivalent) Using a Standard Communication Protocol

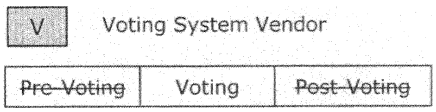


Discussion: Using a standard, publicly documented printer protocol assists in security evaluations of its software.

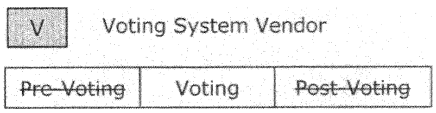
7.1.1.2 The Paper Path Between the Printing, Viewing and Storage of The Paper Record Shall be Protected and Sealed From Access Except by Authorized Election Officials



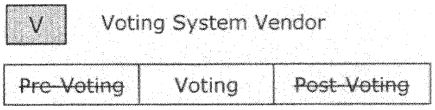
7.1.1.3 The Printer Shall Not be Permitted to Communicate With Any Other System or Machine Other Than the Single Voting Machine to Which it is Connected



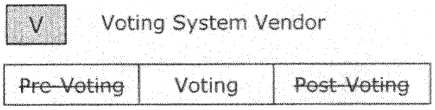
7.1.1.4 The Printer Shall Only be Able to Function as a Printer; It Shall Not Contain Any Other Services (e.g., Provide Copier or Fax Functions) or Network Capability



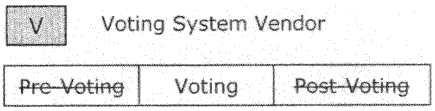
7.1.1.5 Printer Access to Replace Consumables Such as Ink or Paper Shall Only be Possible if it Does Not Compromise the Sealed Printer Paper Path



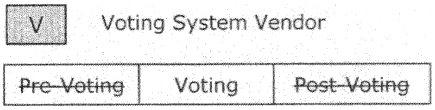
7.1.1.6 The Ballot Box Storing the Paper Records Shall be Sealed and Secured and No Access Shall be Provided to Poll Workers



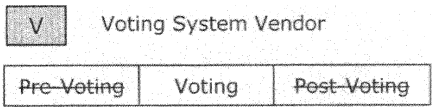
7.1.1.7 Tamper-Evident Seals or Physical Security Measures Shall Protect the Connection Between the Printer and the Voting Station, so that the Connection Cannot be Broken or Interfered With Without Leaving Extensive and Obvious Evidence



7.1.2 The Voting Station's Printer Shall be Highly Reliable and Easily Maintained

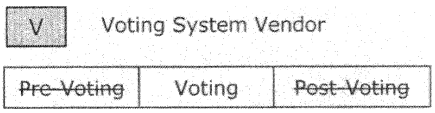


7.1.2.1 The Voting Station Should Detect Errors and Malfunctions such as Paper Jams or Low Supplies of Consumables such as Paper and Ink That May Prevent Paper Records from Being Correctly Displayed Printed or Stored



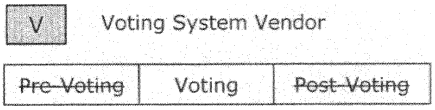
Discussion: This could be accomplished in a variety of different ways: for example, a printer that is out of paper or jammed could issue audible alarms, with the alarm different for each condition.

7.1.2.2 If Errors or Malfunctions Occur, the Voting Station Shall Suspend Voting Operations and Should Present a Clear Indication to The Voter and Election Officials of the Malfunctions

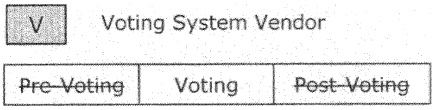


Discussion: The voting station does not record votes if errors or malfunctions occur.

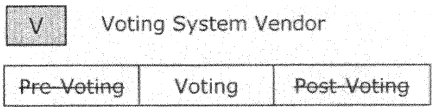
7.1.2.3 Printing Devices Should Either (a) Contain Paper and Ink of Sufficient Capacity so as not to Require Reloading or Opening Equipment Covers or Enclosures and Circumvention of Security Features, or (b) Be Able to Reload Paper and Ink with Minimal Disruption to Voting and Without Circumvention of Security Features such as Seals



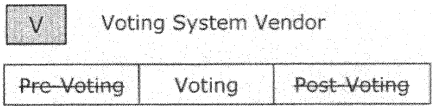
7.1.2.4 Vendor Documentation Shall Include Procedures for Investigating and Resolving Printer Malfunctions Including but Not Limited to Printer Operations, Misreporting of Votes, Unreadable Paper Records, and Power Failures



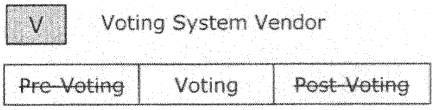
7.1.2.5 Vendor Documentation Shall Include Printer Reliability Information Including Mean Time Between Failure Information and Shall Include Recommendations for Appropriate Numbers of Backup Printer and Printer Supplies



7.1.3 Protective Coverings Intended to be Transparent on Voting Station Devices Shall be Maintainable via a Predefined Cleaning Process. If The Coverings Become Damaged Such That They Obscure the Paper Record, They Shall be Replaceable



7.1.4 The Paper Record Shall be Sturdy, Clean, and of Sufficient Durability to be Used for Verifications, Reconciliations, and Recounts Conducted Manually and via Machine Reading Equipment



3. Wireless Requirements (Normative)

This section provides wireless requirements for implementing and using wireless capabilities within a voting system. These requirements reduce, but don't eliminate, the risk of using wireless communications for voting systems.

Wireless is defined as any means of communication that occurs without wires. This normally covers the entire electromagnetic spectrum. For the purposes of this section wireless includes radio frequency (RF), infrared, (IR), and microwave.

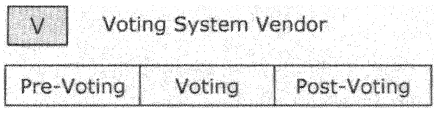
Since the wireless communications path on which the signals travel is via the air and not via a wire or cable, devices other than those intended to receive the wireless signal (e.g., voting data) can receive (intentionally and unintentionally) the wireless signals. Some of the wireless communications 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 use of wireless technology introduces severe risk and should be approached with extreme caution. The requirements in this section (i.e., controlling and identifying usage, protecting the transmitted data and path, and protecting the system) mitigate these risks.

The requirements that are applicable to all types of wireless communications are presented, followed by requirements that are applicable to a specific part of the electromagnetic spectrum (e.g., audible, radio frequency, and infrared). These latter requirements only apply to systems using those parts of the spectrum.

There are other concerns when evaluating wireless usage, specifically radio frequency. 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 RF wireless of 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.

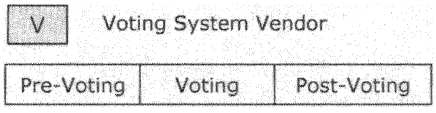
1. Relationship to Volume I, Section 5: ''Telecommunications''

1.1 At a Minimum Wireless Communications Shall Meet the Requirements Listed in Volume I, Section 5, ''Telecommunications''



2. Controlling Usage

2.1 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

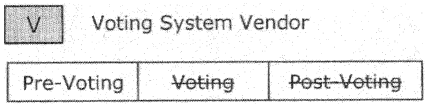


2.1.1 This documentation shall include:

- 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,
- 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,
- 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, and

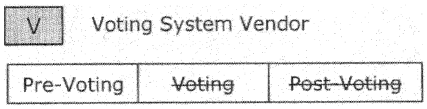
• A rationale for the inclusion of wireless in the proposed voting system, based on a careful and complete description of the perceived advantages and disadvantages of using wireless for the documented uses compared to using non-wireless approaches.



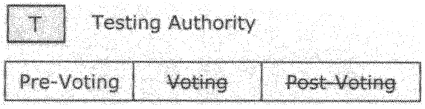
Discussion: In general, convenience is not a sufficiently compelling reason, on its own, to justify the inclusion of wireless communications in a voting system. If convenience is cited as an advantage of wireless, it shall be balanced against the difficulty of working with cryptographic keys.

[Best Practice for Voting Officials] When using encryption to ensure that the wireless communication is secure, appropriate procedures are needed for cryptographic key management.

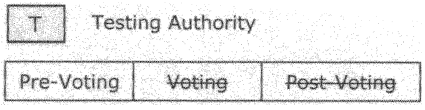
2.1.2 The Details of All Cryptographic Protocols Used for Wireless Communications, Including the Specific Features and Data, Shall be Documented



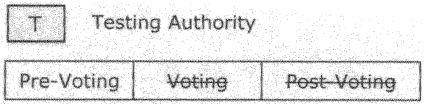
2.1.3 The Wireless Documentation Shall be Closely Reviewed for Accuracy, Completeness, and Correctness



2.1.3.1 This Review Shall be Done Either Through an Open and Public Review or by a Subject Area Recognized Expert

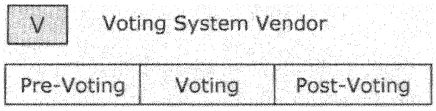


2.1.4 There Shall be No Undocumented Use of the Wireless Capability, Nor Shall There be Any Use of the Wireless Capability That Is Not Entirely Controlled by the Voting Official

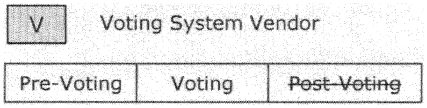


Discussion: This can be tested by reviewing all of the software, hardware, and documentation and by testing the status of wireless activity during all phases of testing.

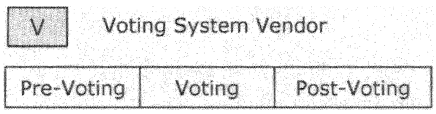
2.2 If a Voting System Includes Wireless Capabilities, Then the Voting System Should be Able to Accomplish the Same Function if Wireless Capabilities are Not Available Due to an Error or No Service



2.2.1 The Vendor Shall Provide Documentation How to Accomplish These Functions When Wireless Is Not Available

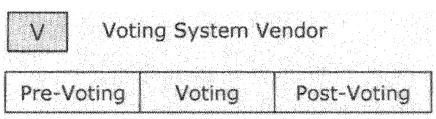


2.3 The System Shall be Designed and Configured Such That it Is Not Vulnerable to a Single Point of Failure Using Wireless Communications That Causes a Total Loss of Any of Voting Capabilities

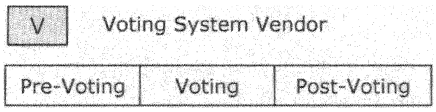


Discussion: Rewritten from Volume 1, Section 5.2.6 Integrity item (c)

2.4 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



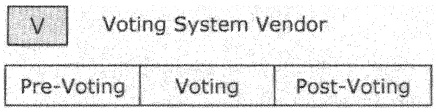
2.5 If a Voting System Includes Wireless Capabilities, Then the System Shall Not Activate the Wireless Capabilities without Confirmation From a Voting Official



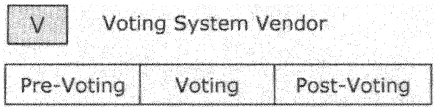
3. Identifying Usage

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

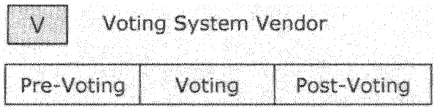
3.1 If a Voting System Provides Wireless Communications Capabilities, Then There Shall be a Method for Determining the Existence of the Wireless Communications Capabilities



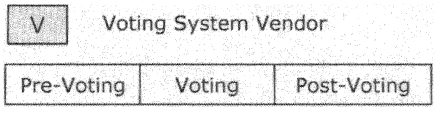
3.2 If a Voting System Provides Wireless Communications Capabilities, Then There Shall be An Indication that Allows One to Determine When the Wireless Communications (e.g., Radio Frequencies) Capability is Active



3.2.1 The Indication Should be Visual



3.3 If a Voting System Provides Wireless Communications Capabilities, Then the Type of Wireless Communications Used (e.g., Radio Frequencies) Shall be Identified Either via a Label or via the Voting Systems Documentation



4. Protecting the Transmitted Data

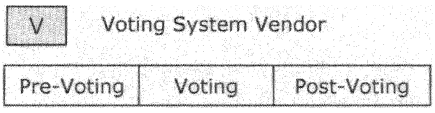
The transmitted data, especially via wireless communications, needs to be protected to ensure confidentiality and integrity. Examples of election information that needs to be protected

include: ballot definitions, ballot instructions (audio), voting device counts, precinct counts, opening of poll signal, and closing of poll signal.

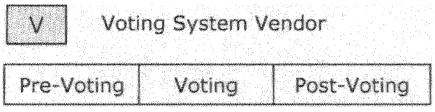
Examples of non—specific election information that needs to be protected include: Protocol messages, address or device identification information, and passwords.

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 materials. However to a lesser extent, infrared signals can still be received by other devices that are in the line of sight. Similarly, wireless signals can also be easily transmitted by others in order to create unwanted signals. Thus to protect the privacy and confidentiality of the information, encryption is required. The following requirements are rewritten from Volume I, Section 6.5.3.

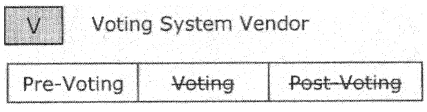
4.1 All Information Transmitted via Wireless Communications Shall be Encrypted and Authenticated, with the Exception of Wireless T-Coil Coupling, to Protect Against Eavesdropping and Data Manipulation Including Modification, Insertion, and Deletion



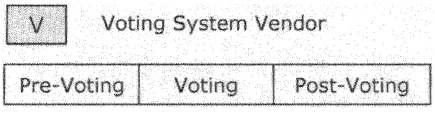
4.1.1 The Encryption Shall be as Defined in Federal Information Processing Standards (FIPS) 197, ''Advanced Encryption Standard (AES)''



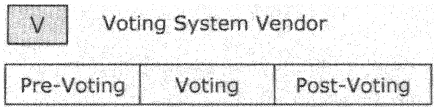
4.1.1.1 The Cryptographic Modules Used Shall Comply With FIPS 140–2, Security Requirements for Cryptographic Modules



4.1.2 The Capability to Transmit Non-Encrypted and Non-Authenticated Information via Wireless Communications Shall Not Exist



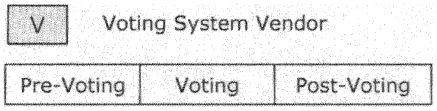
4.1.2.1 If Wireless Communication (Audible) is Used, and if the Receiver of the Wireless Transmission is the Human Ear, then the Information Shall Not be Encrypted (i.e., This Specifically Covers the Case of the Wireless T-Coil Coupling for Assistive Devices Used by People Who are Hard of Hearing—See Volume I, Section 2.2.7.2 DRE Standards Item C)



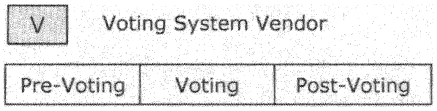
5. Protecting the Wireless Path

With the exception of wireless communications using audible and infrared, it is technically infeasible to use physical means to prevent denial of service (DoS) attacks. If wireless communications are used, then the following capabilities shall exist in order to mitigate the effects of a denial of service (DoS) attack:

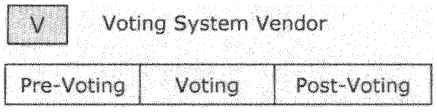
5.1 The Voting System Shall be Able to Function Properly Throughout a DoS Attack, Since the DoS Attack May Continue Throughout the Voting Process.



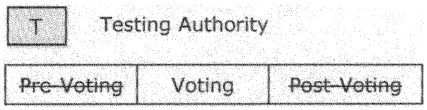
5.2 The Voting System Shall Function Properly as if the Wireless Capability Were Never Available for Use



5.3 Alternative Procedures or Capabilities Shall Exist to Accomplish the Same Functions That the Wireless Communications Capability Would Have Done



5.4 The Wireless (Audible) Path Shall be Protected or Shielded

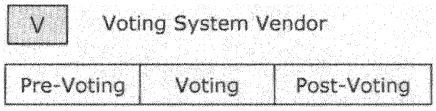


Discussion: Protecting the audible path is a tradeoff between the high volume level necessary for an individual to hear with the low volume level necessary to keep others from hearing, as well as protecting from interference (i.e., noise) from the polling place, voting station, or voting environment. The same is true for the audible path if a voter's speech is to be captured by the voting device. This wireless communication's path protection is necessary to protect privacy. Some audio headsets may already satisfy this requirement for the hearing part, while a soundproof voting booth may be necessary in some other cases (e.g., voice recordings).

5.5 Infrared

Since infrared has the line-of-sight (LoS) property, securing the wireless path can be accomplished by shielding the path between the wireless communicating devices with an opaque enclosure. However this is only practical for short distances. Additionally, this type of shielding can help to prevent accidental damage to the eyes by the infrared signal.

5.5.1 The Shielding Shall be Strong Enough to Prevent Escape of the Voting System's Signal, as well as Strong Enough to Prevent Infrared Saturation Jamming



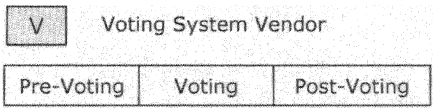
6. Protecting the Voting System from a Wireless-based Attack

The security of the wireless voting systems is as important as the information transmitted. If a voting system becomes compromised, there is no way to determine the harm to the system until the compromise is discovered and an investigation is conducted to determine the extent of the damage.

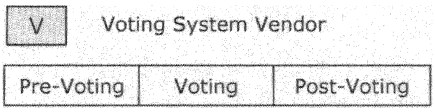
Physical security measures (Volume I, Section 6.3) to prohibit access to a voting system are not possible when using a wireless communications interface. This is similar to when access is through a telecommunications interface, but it is worsened by the fact that there is no wire (physical communication path) to physically secure and by the various physical properties of the electromagnetic spectrum used.

This section covers and reaffirms the applicable overall system capabilities defined in Volume I, Section 2 as well as authentication requirements.

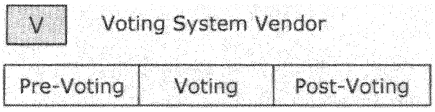
6.1 The Security Requirements Listed in Volume I, Section 2.2.1 Shall be Applicable to Systems With Wireless Communications



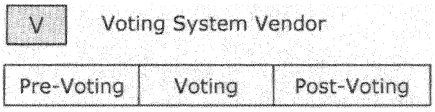
6.2 The Accuracy Requirements Listed in Volume I, Section 2.2.2 Shall be Applicable to Systems With Wireless Communications



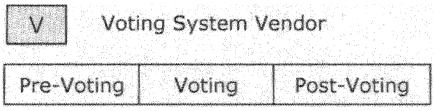
6.2.1 The Use of Wireless Communications That May Cause Impact to the System's Accuracy Through Electromagnetic Stresses Is Prohibited



6.3 The Error Recovery Requirements Listed in Volume I, Section 2.2.3, Shall Be Applicable to Systems With Wireless Communications

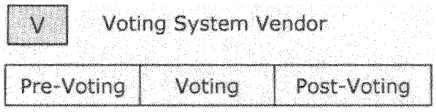


6.4 All Wireless Communications Actions Shall Be Logged



Discussion: A log of important information is maintained to monitor the wireless communications. This is to ensure that the wireless communications are only used by authorized users with authorized access to authorized devices or services, or to determine if these requirements were not followed. This relates to the system audit requirements (Volume I, Section 2.2.5) and integrity (Volume I, Section 2.2.4), if wireless communications are used.

6.4.1 The Log Shall Contain at Least the Following Entries: Times Wireless 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



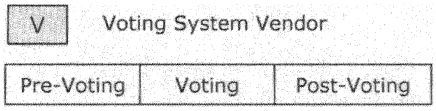
Discussion: Other information such as the number of frames or packets transmitted or received at various logical layers may be useful, but is dependent on the wireless technology used.

[Best Practice for Voting Officials] Appropriate procedures are needed to ensure that wireless communication actions are logged and capture at least the following information: Times wireless 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.

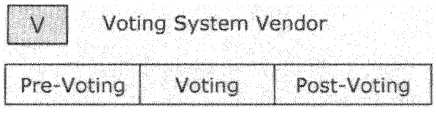
6.5 Authentication

Authentication is an important part in the protection and security of the wireless communications. It provides a mechanism to verify the identity and legitimacy of a person, device, services, or system. Authenticating users, devices and services helps to secure the wireless communications and prevent unauthorized access to the system, services and/or information.

6.5.1 Device Authentication Shall Occur Before Any Access to or Services From the Voting System are Granted Through Wireless Communications



6.5.2 User Authentication Shall Be at Least Level 2 as Per NIST Special Publication 800–63 Version 1.0.1, ''Electronic Authentication Guideline.''



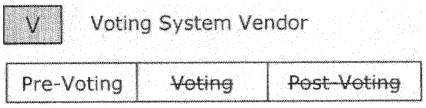
4. Distribution of Voting System Software and Setup Validation (Normative)

This section specifies 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 qualification 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 qualified software and the absence of other software, is to ensure that voting system equipment is in a proper initial state before being used.

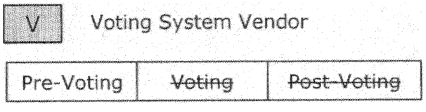
In general, a voting system can be considered to be composed of multiple other systems including polling place systems, central counting/aggregation systems, and election management systems. These other systems may reside on different computer based platforms at different locations and run different 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, etc.

1. Software Distribution Methodology Requirements

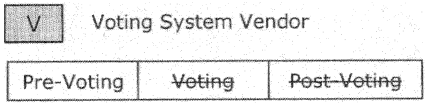
1.1 The Vendor Shall Document All Software Including Voting System Software, Third Party Software (Such as Operating Systems, Drivers, etc.) To Be Installed on Voting Equipment of the Qualified Voting System, and Installation Programs



1.1.1 The Documentation Shall Have a Unique Identifier (Such as a Serial Number) for the Following Set of Information: Documentation, Software Vendor Name, Product Name, Version, Qualification Number of the Voting System, File Names and Paths or Other Location Information (Such as Storage Addresses) of the Software

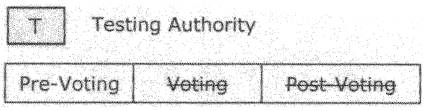


1.1.2 The Documentation Shall Designate All Software Files as Static, Semi-Static, or Dynamic

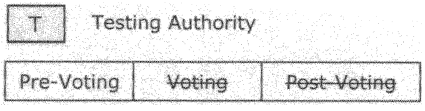


Discussion: Static voting system software such as executable code does not change based on the election being conducted or the voting equipment upon which it is installed. Semi-static voting system software contains configuration information for the voting system based on the voting equipment that is 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 a priori making it impossible to create reference information to verify the software.

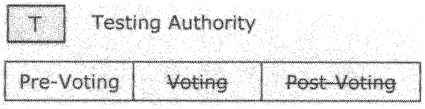
1.2 The EAC Accredited Testing Authority Shall Witness the Final Build of the Executable Version of the Qualified Voting System Software Performed by the Vendor



1.2.1 The Testing Authority Shall Create a Complete Record of the Build That Includes: A Unique Identifier (Such as a Serial Number) for the Complete Record, List of Unique Identifiers of Write-Once Media Associated with the record, Time, Date, Location, Name and Signatures of All People Present, Source Code and Resulting Executable File Names, Version of Voting System Software, Qualification 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

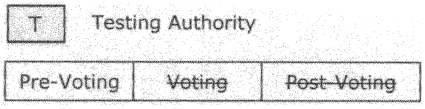


1.2.2 The Record of the Source Code and Executable Files Shall be Made on Write-Once Media. Each Piece of Write-Once Media Shall Have a Unique Identifier

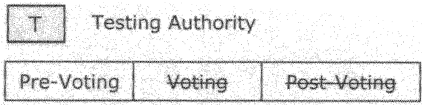


Discussion: Write-once media includes technology such as a CD–R, ROM, or PROM (but not EEPROM or CD–RW). The unique identifiers appear on indelibly printed labels and in a digitally signed file on the write-once media.

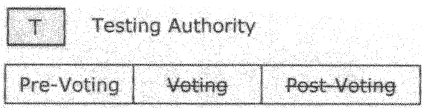
1.2.3 The Testing Authority Shall Retain This Record Until the Voting System Ceases to be Qualified



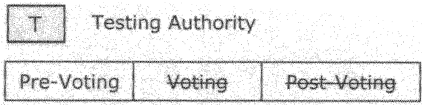
1.2.4 The EAC Accredited Testing Authority Shall Create a Subset of the Complete Record of the Build That Includes a Unique Identifier (Such as a Serial Number) of the Subset, the Unique Identifier of the Complete Record, List of Unique Identifiers of Write-Once Media Associated With the Subset, Vendor, Product Name, Version of Voting System Software, Qualification Number of the Voting System, All the Files That Resulted from the Build and Binary Images of All Installation Programs



1.2.5 The Record of the Software Shall be Made on Write-Once Media. Each Piece of Write-Once Media Shall Have a Unique Identifier

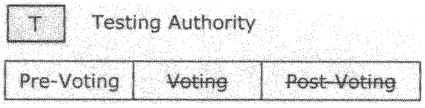


1.2.6 The Testing Authority Shall Retain a Copy, Send a Copy to the Vendor, and Send a Copy to the NIST National Software Reference Library (NSRL) [1] and/or to Any Other Repository Named by the Election Assistance Commission

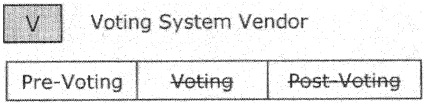


Discussion: The NSRL was established to meet the needs of the law enforcement community for court admissible digital evidence by providing an authoritative source of commercial software reference information. Information is available at *www.nsrl.nist.gov.*

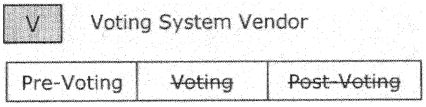
1.2.7 The Testing Authority Shall Retain This Record Until the Voting System Ceases to be Qualified



1.3 The Vendor Shall Provide the NSRL or Other EAC Designated Repository With a Copy of All Third Party Software



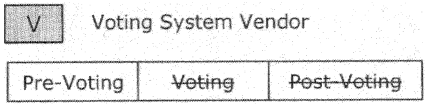
1.4 All Voting System Software, Installation Programs, Third Party Software (Such as Operating Systems, Drivers, etc.) Used to Install or to be Installed on Voting System Equipment Shall be Distributed on a Write-Once Media



[Best Practice for Voting Officials] Voting software used to install the qualified voting systems can be obtained on write-once media from the voting system vendor or an EAC accredited testing authority.

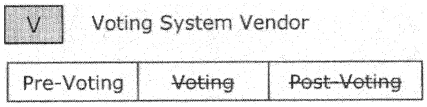
[1] The National Software Reference Library (NSRL) is a repository of software established and directed by the National Institute of Standards and Technology. It was designed to meet the need for court admissible evidence in the identification of software files. The EAC designated the NSRL as a repository for voting system software.

1.4.1 The Vendor Shall Document That the Process Used to Verify the Software Distributed on Write-Once Media is the Qualified Software by Using the Reference Information Provided by the NSRL or Other EAC Designated Repository

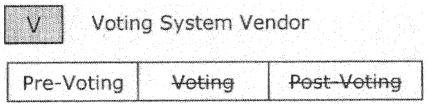


[Best Practice for Voting Officials] The reference information produced by the NSRL or other EAC designated repository can be used to verify that the correct software has been received.

1.4.2 The Voting System Equipment Shall be Designed to Allow the Voting System Administrator to Verify That the Software is the Qualified Software by Comparing it to Reference Information Produced by the NSRL or Other EAC Designated Repository Before Installing the Software

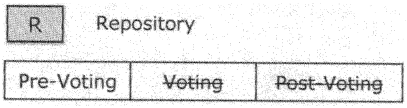


1.4.3 The Vendors and Testing Authority Shall Document to Whom They Provide Voting System Software Write-Once Media

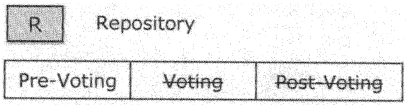


2. Generation and Distribution Requirements for Reference Information

2.1 The NSRL or Other EAC Designed Repository Shall Generate Reference Information Using the Binary Images of the (a) Qualified Voting System Software Received on Write-Once Media From Testing Authorities and (b) Election Specific Software Received on Write-Once Media From Jurisdictions

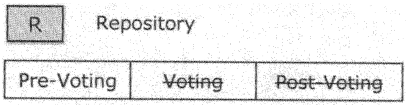


2.1.1 The NSRL or Other EAC Designated Repository Shall Generate Reference Information in at Least One of the Following Forms: (a) Complete Binary Images, (b) Cryptographic Hash Values, or (c) Digital Signatures of the Software

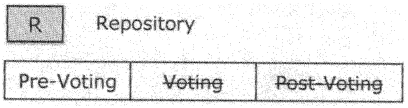


Discussion: Although binary images, cryptographic hashes, and digital signatures can detect a modification or alteration in the software, they cannot determine if the change to the software was accidental or intentional.

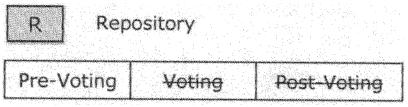
2.1.1.1 The NSRL or Other EAC Designated Repository Shall Create a Record of the Creation of Reference Information That Includes: A Unique Identifier (Such as a Serial Number) for the Record, File Names of Software and Associated Unique Identifier(s) of the Write-Once Media From Which Reference Information is Generated, Time, Date, Name of People Who Generated Reference Information, the Type of Reference Information Created, Qualification Number of Voting System (If Issued), Voting System Software Version, Product Name, and Vendor



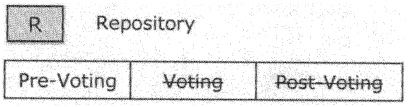
2.1.1.2 The NSRL or Other EAC Designated Repository Shall Retain the Write-Once Media Used to Generate the Reference Information Until the Voting System Ceases to be Qualified



2.1.1.3 The NSRL or Other EAC Designated Repository That Generates Hash Value and/or Digital Signature Reference Information Shall Use FIPS Approved Algorithms for Hashing and Signing

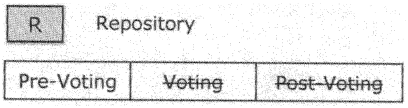


2.1.1.4 The NSRL or Other EAC Designated Repository That Generates Hash Values, Digital Signatures Reference Information, or Cryptographic Keys Shall Use a FIPS 140–2 Level 1 or Higher Validated Cryptographic Module



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

2.1.1.5 The NSRL or Other EAC 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



6.1 Scope

This section describes essential security capabilities for a voting system, encompassing the system's hardware, software, communications, and documentation. The Standards recognize that no predefined set of security standards will address and defeat all conceivable or theoretical threats. However, the Standards articulate requirements to achieve acceptable levels of integrity, reliability, and inviolability. Ultimately, the objectives of the security standards for voting systems are:

- To establish and maintain controls that can ensure that accidents, inadvertent mistakes, and errors are minimized,
- To protect the system from intentional manipulation and fraud, and from malicious mischief,
- To identify fraudulent or erroneous changes to the system, and
- To protect secrecy in the voting process.

The Standards 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, the Standards identify several types of risk that must be addressed by a voting system. These include:

- Unauthorized changes to system capabilities for:
- Defining ballot formats,
- Casting and recording votes,
- Calculating vote totals consistent with defined ballot formats, and
- 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, to unauthorized individuals, and
• 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 cast by the voter.

This section describes specific capabilities that vendors shall integrate into a voting system in order to address the risks listed above.

6.1.1 System Components and Sources

The requirements of this section apply to the broad range of hardware, software, communications components, and documentation that comprises a voting system. These requirements apply to components:
• Provided by the voting system vendor and the vendor's suppliers,
• Furnished by an external provider (for example providers of personal computers and commercial off-the-shelf (COTS) operating systems) where the components are capable of being used during voting system operation, and
• Developed by a voting jurisdiction.

6.1.2 Location and Control of Software and Hardware on Which It Operates

The requirements of this section 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, and
• Ballot printers, vote counting devices, and other hardware typically installed at central or precinct locations (including contractor facilities).

However, some requirements are applicable only in circumstances specified by this section.

6.1.3 Elements of Security Outside Vendor Control

The requirements of this section apply to the capabilities of a voting system provided by the vendor. The Standards recognizes that effective security requires safeguards beyond those provided by the vendor. Effective security demands diligent security practices by the purchasing jurisdiction and the jurisdictions representatives. 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, and
• Organizational responsibilities and personnel screening.

Because specific standards for these elements are not under the direct control of the vendor, they will be addressed in forthcoming Operational Guidelines that address best practices for jurisdictions conducting elections and managing the operation of voting systems.

6.1.4 Organization of this Section

The standards presented in this section are organized as follows:
• *Access Control:* These standards addresses 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.
• *Equipment and Data Security:* These standards address physical security measures and procedures that prevent disruption of the voting process at the poll site 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.
• *Telecommunication and Data Transmission:* These standards address security for the electronic transmission of data between system components or locations over both private and public networks
• *Security for Transmission of Official Data Over Public Communications Networks:* These standards address security for systems that communicate individual votes or vote totals over public communications networks.

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 section 4.

6.2 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 contained in this section of the Standards are limited to those controls required of system vendors. Access controls required of jurisdictions will be addressed in future documents detailing operational guidelines for jurisdictions.

6.2.1 Access Control Policy

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

6.2.1.1 General Access Control Policy

Although the jurisdiction in which the voting system is operated is responsible for determining the access policies applying to 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, and
h. Any additional relevant characteristics.

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

6.2.2 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, and

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.

6.3 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.

6.3.1 Polling Place Security

For polling place operations, vendors shall develop and provide detailed documentation of measures to anticipate and counteract vandalism, civil disobedience, and similar occurrences. The measures shall:

a. Allow the immediate detection of tampering with vote casting devices and precinct ballot counters, and

b. Control physical access to a telecommunications link if such a link is used.

6.3.2 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:

a. Handling of ballot boxes,

b. Preparing of ballots for counting,

c. Counting operations, and

d. Reporting data.

6.4 Software Security

Voting systems shall meet specific security requirements for the installation of software and for protection against malicious software.

6.4.1 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 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 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 computer chip) other than the component on which the operating system resides; and

e. After initiation of election day testing, no source code or compilers or assemblers shall be resident or accessible.

6.4.2 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.

6.5 Telecommunications and Data Transmission

There are four areas that must be addressed by telecommunications and data transmission security capabilities:

- Access control for telecommunications capabilities,
- Data integrity,
- Detection and prevention of data interception, and
- Protection against external threats to which commercial products used by a voting system may be susceptible.

6.5.1 Access Control

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.

6.5.2 Data Integrity

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.

6.5.3 Data Interception Prevention

Voting systems that use telecommunications as defined in Section 5 to communicate between system components and locations before the poll site is officially closed shall:

a. Implement an encryption standard currently documented and validated for use by an agency of the U.S. Federal Government; and

b. Provide a means to detect the presence of an intrusive process, such as an Intrusion Detection System.

6.5.4 Protection Against External Threats

Voting systems that use public telecommunications networks shall implement protections against external threats to which commercial products used in the system may be susceptible.

6.5.4.1 Identification of COTS Products

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:

a. Operating systems,

b. Communications routers,

c. Modem drivers, and

d. Dial-up networking software.

Such documentation shall identify the name, vendor, and version used for each such component.

6.5.4.2 Use of Protective Software

Voting systems that use public telecommunications networks shall use

protective software at the receiving-end of all communications paths to:

a. Detect the presence of a threat in a transmission,

b. Remove the threat from infected files/data,

c. Prevent against storage of the threat anywhere on the receiving device,

d. Provide the capability to confirm that no threats are stored in system memory and in connected storage media, and

e. Provide data to the system audit log indicating the detection of a threat and the processing performed.

Vendors shall use multiple forms of protective software as needed to provide capabilities for the full range of products used by the voting system.

6.5.4.3 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), for which a current listing can be found at *http://www.nipc.gov/warnings/warnings.htm,* and the Federal Computer Incident Response Capability (FedCIRC), for which additional information can be found at *http://www.fedcirc.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 ITAs 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 no later than one month before an election, and

f. Address threats emerging too late to correct the system at least one month before the election, including:

(1) Providing prompt, emergency notification to the ITAs and the affected states and user jurisdictions,

(2) Assisting client jurisdictions directly, or advising them through detailed written procedures, to disable the public telecommunications mode of the system, and

(3) After the election, modifying the system to address the threat, submitting the modified system to an ITA and appropriate 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.

6.5.5 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. Controlled system access by means of passwords, and restriction of account access to necessary functions only, and

d. Have capabilities in place to control the flow of information, precluding data leakage through shared system resources.

6.5.6 Access to Incomplete Election Returns and Interactive Queries

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

a. For equipment that operates in a central counting environment, be designed to provide external access to incomplete election returns 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. Use voting system software and its security environment designed such that data accessible to interactive queries resides in an external file, or database, that is created and maintained by the elections software under the restrictions applying to any other output report, namely, that:

(1) The output file or database has no provision for write-access back to the system.

(2) 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.

6.6 Security for Transmission of Official Data Over Public Communications Networks

DRE systems that transmit data over public telecommunications networks face security risks that are not present in other DRE systems. This section describes standards applicable to DRE systems that use public telecommunications networks.

6.6.1 General Security Requirements for Systems Transmitting Data Over Public Networks

All systems that transmit data over public telecommunications networks shall:

a. Preserve the secrecy of a voter's ballot choices, and prevent anyone from violating ballot privacy,

b. Employ digital signature for all communications between the vote server and other devices that communicate with the server over the network, and

c. Require that at least two authorized election officials activate any critical operation regarding the processing of ballots transmitted over a public communications network takes place, i.e. the passwords or cryptographic keys of at least two employees are required to perform processing of votes.

6.6.2 Voting Process Security for Casting Individual Ballots over a Public Telecommunications Network

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 poll sites 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.

6.6.2.1 Documentation of Mandatory Security Activities

Vendors of systems that cast individual ballots over a public

telecommunications network shall provide detailed descriptions of:

a. All activities mandatory to ensuring effective system security to be performed in setting up the system for operation, including testing of security before an election; and

b. All activities that should be prohibited during system setup and during the time frame for voting operations, including both the hours when polls are open and when polls are closed.

6.6.2.2 Capabilities to Operate During Interruption of Telecommunications Capabilities

These systems shall provide the following capabilities to provide resistance to interruptions of telecommunications service that prevent voting devices at the poll site from communicating with external components via telecommunications:

a. Detect the occurrence of a telecommunications interruption at the poll site and switch to an alternative mode of operation that is not dependent on the connection between poll site voting devices and external system components,

b. Provide an alternate mode of operation that includes the functionality of a conventional DRE machine 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 DRE system mode,

d. Upon reestablishment of communications, transmit and process votes accumulated while operating in conventional DRE system mode with all security safeguards in effect, and

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.

Volume I, Section 7

Table of Contents

7 Quality Assurance

7.1 Scope

Quality Assurance provides continuous confirmation that a voting system conforms with the Standards and to the requirements of state and local jurisdictions. Quality Assurance is a vendor function with associated practices that is initiated prior to system development and continues throughout the maintenance life cycle of the voting system. Quality Assurance focuses on building quality into a system and reducing dependence on system tests at the end of the life cycle to detect deficiencies, thus helping ensure the system:

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

7.2 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 of this standard 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:

(1) In-process inspection and testing that the manufacturer deems necessary to ensure proper fabrication and assembly of hardware, and

(2) Installation and operation of software (including firmware).

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

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

7.3 Components from Third Parties

A vendors 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, should 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.

7.4 Responsibility for Tests

The manufacturer or vendor shall be responsible for:

a. Performing all quality assurance tests;

b. Acquiring and documenting test data; and

c. Providing test reports for review by the ITA, and to the purchaser upon request.

7.5 Parts & 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 operating environment; and

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

7.6 Quality Conformance Inspections

The vendor performs conformance inspections to ensure the overall quality of the voting system and components delivered to the ITA for 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; and

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

7.7 Documentation

Vendors are required to produce documentation to support the development and formal testing of voting systems. To meet documentation requirements, vendors shall provide complete product documentation with each voting systems or components, as described Volume II, Section 2 for the TDP. This documentation shall:

a. Be sufficient to serve the needs of the ITA, voters, election officials, and maintenance technicians;

b. Be prepared and published in accordance with standard industrial practice for information technology and electronic and mechanical equipment; and

c. Consist, at a minimum, of the following:

(1) System overview;

(2) System functionality description;
(3) System hardware specification;
(4) Software design and specifications;
(5) System security specification;
(6) System test and verification specification;
(7) System operations procedures;
(8) System maintenance procedures;
(9) Personnel deployment and training requirements;
(10) Configuration management plan;
(11) Quality assurance program; and
(12) System Change Notes.

Volume I, Section 8

Table of Contents

8 Configuration Management

8.1 Scope

This section contains specific requirements for configuration management of voting systems. For the purpose of the Standards, 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 to the Independent Test Authority (ITA) as part of the Technical Data Package (TDP) for system qualifications described in Volume II, Voting Systems Qualification Testing Standards, for review against the requirements of this section. Additionally, state or local election legislation, regulations, or contractual agreements may require the vendor to conform to additional standards for configuration management or to adopt specific required procedures. Further, authorized election officials or their representatives reserve the right to inspect vendor facilities and operations to determine conformance with the vendor's reported procedures and with any additional requirements.

8.1.1 Configuration Management Requirements

Configuration management addresses a broad set of recordkeeping, audit, 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 to ITAs;
- Releasing new versions of the system to customers;
- Auditing the system, including its documentation, against configuration management records;
- Controlling interfaces to other systems; and
- Identifying tools used to build and maintain the system.

8.1.2 Organization of Configuration Management Standards

The standards for configuration management presented in this section include:

- Application of configuration management requirements;
- Configuration management policy;
- Configuration identification;
- Baseline, promotion, and demotion procedures;
- Configuration control procedures;
- Release process;
- Configuration audits; and
- Configuration management resources.

8.1.3 Application of Configuration Management Requirements

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

a. Software components;
b. Hardware components;
c. Communications components;
d. Documentation;
e. Identification and naming and conventions (including changes to these conventions) for software programs and data files;
f. Development and testing artifacts such as test data and scripts; and
g. File archiving and data repositories.

8.2 Configuration Management Policy

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

a. Scope and nature of configuration management program activities; and
b. 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.

8.3 Configuration Identification

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

8.3.1 Structuring and Naming Configuration Items

The vendor shall describe the procedures and conventions used to:

a. Classify configuration items into categories and subcategories;
b. Uniquely number or otherwise identify configuration items; and
c. Name configuration items;

8.3.2 Versioning Conventions

When a system component is used to identify higher-level system elements, a vendor shall describe the conventions used to:

a. Identify the specific versions of individual configuration items and sets of items that are used by the vendor to identify higher level system elements such as subsystems;
b. Uniquely number or otherwise identify versions; and
c. Name versions.

8.4 Baseline, Promotion, and Demotion 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 ITAs for qualification testing; and
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).

8.5 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; and

d. Resolve externally identified and reported defects (i.e., by customers and ITAs).

8.6 Release Process

The release process is the means by which the vendor installs, transfers, or migrates the system to the ITAs 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 ITA;

b. Perform a subsequent maintenance or upgrade release of the system, or a particular components, to an ITA;

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 qualified system version; and

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 qualified system version.

8.7 Configuration Audits

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

8.7.1 Physical Configuration Audit

The PCA is conducted by the ITA to compare the voting system components submitted for qualification 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; and

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; and

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

(1) Establishing a configuration baseline of the software and hardware to be tested; and

(2) Confirming whether the system documentation matches the corresponding system components.

8.7.2 Functional Configuration Audit

The FCA is conducted by the ITA 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:

(1) Copies of all procedures used for module or unit testing, integration testing, and system testing;

(2) Copies of all test cases generated for each module and integration test, and sample ballot formats or other test cases used for system tests; and

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

In addition to such audits performed by ITAs during the system qualification 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.

8.8 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 if 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, audit, and reporting activities of the configuration management standards. The resources documentation standard provided below 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;

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

c. Procedures and training materials for using the tools.

Volume I, Section 9

Table of Contents

9 Overview of Qualification Tests

9.1 Scope

This section provides an overview of the testing process for qualification testing of voting systems. Qualification testing is the process by which a voting system is shown to comply with the requirements of the Standards and the requirements of its own design and performance specifications.

Qualification testing encompasses the examination 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 function 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. Since 1994, qualification tests for voting systems have been performed by Independent Test Authorities (ITAs) certified by the National Association of State Election Directors (NASED). NASED has certified an ITA for either the full scope of qualification testing or a distinct subset of the total scope of testing. The test process described in this section may be conducted by one or more ITAs, depending on the nature of tests to be conducted and the expertise of the certified ITAs.

Qualification testing is distinct from all other forms of testing, including developmental testing by the vendor, certification testing by a state election organization, and system acceptance testing by a purchasing jurisdiction:

- Qualification testing follows the vendor's developmental testing;
- Qualification testing provides an assurance to state election officials and local jurisdictions of the conformance of a voting system to the Standards as input to state certification of a voting system and acceptance testing by a purchasing jurisdiction; and
- Qualification testing may precede state certification testing, or may be conducted in parallel as established by the certification program of individual states.

Generally a voting system remains qualified under the standards against which it was tested, as long as all modifications made to the system are evaluated and passed by a certified ITA. The qualification test report remains valid for as long as the voting system remains unchanged from the last tested configuration. However, if a new threat to a particular voting system is discovered, it is the prerogative of NASED to determine which qualified voting systems are vulnerable, whether those systems need to be retested, and the specific tests to be conducted. In addition, when new standards supersede the standards under which the system was qualified, it is the prerogative of NASED to determine when systems that were qualified under the earlier standards will lose their qualification, unless they are tested to meet current standards.

The remainder of this section describes the documentation and equipment required to be submitted by the vendor, the scope of qualification testing, the applicability to voting system components, and the flow of the test process.

9.2 Documentation Submitted by Vendor

The vendor shall submit to the ITA documentation necessary for the identification of the full system configuration submitted for evaluation and for the development of an appropriate test plan by the ITA for system qualification testing.

One element of the documentation is the Technical Data Package (TDP). The TDP contains information that 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 the system was previously qualified, the TDP also includes the system change notes.

This documentation is used by the ITA in constructing the qualification testing plan and is particularly important in constructing plans for the re-testing of systems that have been qualified previously. Re-testing of systems submitted by vendors that consistently adhere to particularly strong and well documented quality assurance and configuration management practices will generally be more efficient than for systems developed and maintained using less rigorous or less well documented practices. Volume II provides a detailed description of the documentation required for the vendor's quality assurance and configuration management practices used for the system submitted for qualification testing.

9.3 Voting Equipment Submitted by Vendor

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

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

b. The software submitted for qualification 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 in both performance and construction; and

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.

9.4 Testing Scope

The qualification test 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.

Five types of focuses guide the overall qualification testing 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 (while it would be desirable that there be an error rate of zero, if this had to be proven by a test, the test itself would take an infinity of time);
- 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; and
- Completeness and accuracy of the system documentation and configuration management records to enable purchasing jurisdictions to effectively install, test, and operate the system.

Qualification testing complements and evaluates the vendor's developmental testing, including any beta testing. The ITA evaluates the completeness of the vendor's

developmental test program, including the sufficiency of vendor tests conducted to demonstrate compliance with the Standards as well as the system's performance specifications. The ITA 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 qualification 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. The ITA may use automated software testing tools to assist in this process if they are available for the software under examination.

The procedure for disposition of system deficiencies discovered during qualification testing is described in Volume II of the Standards. This procedure recognizes that some but not necessarily all operational malfunctions (apart from software logic defects) may result in rejection. Basically, any defect that results in or may result in the loss or corruption of voting data, whether through failure of system hardware, software, or communication, through procedural deficiency, or through deficiencies in security and audit provisions, shall be cause for rejection. Otherwise, malfunctions that result from failure to comply fully with other requirements of this standard will not in every case warrant rejection. Specific failure definition and scoring criteria are also contained in Volume II.

9.4.1 Test Categories

The qualification test procedure is presented in several parts:

- Functionality testing;
- Hardware testing;
- Software evaluation;
- System-level integration tests, including audits; and
- 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 qualification. Security tests exercise hardware, software and communications capabilities. Documentation review conducted during software qualification supplements the review undertaken for system-level testing.

The qualification test procedures are presented in these categories because test authorities frequently focus separately on each. The following subsections provide information that test authorities need to conduct testing.

Not all systems being tested are required to complete all categories of testing. For example, if a previously-qualified system has had hardware modifications, the system may be subject only to non-operating environmental stress testing of the modified component, and a partial system-level test. If a system consisting of general purpose COTS hardware or one that was previously qualified has had modifications to its software, the system is subject only to software qualification and system-level 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.

9.4.1.1 Focus of Functionality Tests

Functionality testing is performed to confirm the functional capabilities of a voting system submitted for qualification. The ITA designs and performs procedures to test a voting system against the requirements outlined in Section 2. In order to best compliment the diversity of the voting systems industry, this part of the qualification 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.

9.4.1.2 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 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) 810D, 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 Section 3. 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, rather than military and aerospace, practice.

9.4.1.3 Focus of Software Evaluation

The software qualification 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 4. Essentially, the ITA will look at programming completeness, consistency, correctness, modifiability, structuredness 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 ITA may inspect COTS generated software source code in the 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.

9.4.1.4 Focus of System-Level Integration Tests

The functionality, hardware, and software qualification 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 ITA tests the interface of all system modules and subsystems with each other against the vendor's specifications. Some, but not all, systems use telecommunications capabilities as defined in Section 5. 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 ITA 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 Section 6. 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 ITA 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. At this time, general standards for the usability of voting systems by the average voter and election officials have not been defined, but are to be addressed in the next update of the Standards. However, standards for usability by individual voters with disabilities have been defined in Section 2.7 based on Section 508 of the Rehabilitation Act Amendments of 1998. Voting systems are tested to ensure that an accessible voting station is included in the system configuration and that its design and operation conforms with these standards.

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 Standards. As part of the PCA, the ITA 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 vendors' documentation. Through use, the FCA verifies the accuracy and completeness of the system's 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.

9.4.1.5 Focus of Vendor Documentation Examination

The ITA reviews the documentation submitted by the vendor to evaluate the extent to which it conforms to the requirements outlined in Sections 7 and 8 for vendor configuration and quality assurance practices. The ITA also evaluates the conformance of other documentation and information provided by the vendor with the vendor's documented practices for quality assurance and configuration management.

The Standards do not require on-site examination of the vendor's quality assurance and configuration management practices during the system development process. However, the ITA 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.

9.4.2 Sequence of Tests and Audits

There is no required sequence for performing the system qualification tests and audits. For a new system, not previously qualified, a test using the generic test ballot decks might be performed before undertaking any of the more lengthy and expensive tests or documentation review. The ITA or vendor may, however, schedule the PCA, FCA, or other tests in any convenient order, provided that the prerequisite conditions for each test have been met before it is initiated.

9.5 Test Applicability

Qualification tests are conducted for new systems seeking initial qualification as well as for systems that are modified after qualification.

9.5.1 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 described in Section 2. 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 all other components of the voting system shall be determined through functional tests integrating these products with the remainder of the system.

9.5.1.1 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; and

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.

9.5.1.2 Software

Software qualification 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; and

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).

9.5.2 Modifications to Qualified Systems

Changes introduced after the system has completed qualification under these Standards or earlier versions of the national Voting System Standards will necessitate further review.

9.5.2.1 General Requirements for Modifications

The ITA will determine tests necessary for to qualify 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 ITA may:

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

b. Determine that all changes must be retested against the previously qualified version (this will include review of changes to source code, review of all updates to the TDP, and a performance of system-level and functional tests); or

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

9.5.2.2 Basis for Limited Testing Determinations

The ITA may determine that a modified system will be subject only to limited qualification testing if the vendor demonstrates that the change does not affect demonstrated compliance with these Standards for:

a. Performance of voting system functions;

b. Voting system security and privacy;

c. Overall flow of system control; and

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

Limited qualification 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.

9.6 Qualification Test Process

The qualification test process may be performed by one or more ITAs that together perform the full scope of tests required by the Standards. Where multiple ITAs 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 ITA independently of the other testing performed by other ITAs. Testing may be coordinated across ITAs so that hardware/firmware tested by one ITA can be used in the overall system tests performed by another ITA.

Whether one or more ITAs are used, the testing generally consists of three phases:

- Pre-test Activities;
- Qualification Testing; and
- Qualification Report Issuance and Post-test Activities.

9.6.1 Pre-test Activities

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

9.6.1.1 Initiation of Testing

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

a. Request the performance of qualification testing from among the certified ITAs,

b. Enter into formal agreement with the ITAs for the performance of testing, and

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

Qualification 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 Section 9.5.2, the nature and scope of testing for system changes or new versions shall be determined by the ITA 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.

9.6.1.2 Pre-test Preparation

Pre-test preparation encompasses the following activities:

a. The vendor shall prepare and submit a complete TDP to the ITA. The TDP should consist of the items listed in Section 9.2 and specified in greater detail in Standards Volume II;

b. The ITA 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 ITA;

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

e. The vendor shall deliver to the ITA all hardware and software needed to perform testing.

9.6.2 Qualification Testing

Qualification 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 qualification test data, and the evaluation of the data resulting from tests and examinations.

9.6.2.1 Qualification Test Plan

The ITA shall prepare a Qualification Test Plan to define all tests and procedures required to demonstrate compliance with Standards, including:

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

b. Establishing the test environment or the special environment required to perform the test;

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

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

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

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

g. Confirming that documented vendor practices for quality assurance and configuration management comply with the Standards.

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

9.6.2.2 Qualification Test Conditions

The ITA may perform Qualification 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, who 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; and

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

(1) Temperature +/−4 degrees F

(2) Electrical supply voltage +/−2 vac.

9.6.2.3 Qualification Test Fixtures

ITAs may use test fixtures or ancillary devices to facilitate qualification 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. ITAs 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; and

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.

9.6.2.4 Witness of System Build and Installation

Although most testing is conducted at facilities operated by the ITA, a key element of voting system testing shall be conducted at the vendor site. The ITA responsible for testing voting system software, telecommunications, and integrated system operation (i.e., system wide 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 qualification.

9.6.2.5 Qualification Test Data Requirements

The following qualification 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; and

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.

9.6.2.6 Qualification Test Practices

The ITA shall conduct the examinations and tests defined in the Test Plan such that all applicable tests identified in Standards Volume II are executed to determine compliance with the requirements in Sections 2–8 of the Standards. The ITA 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, 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 ITA 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:

(1) Vendor submits a design, manufacturing, or packaging change notice to correct the deficiency, together with test data to verify the adequacy of the change;

(2) Examiner of the equipment agrees that the proposed change will correct the deficiency; and

(3) Vendor certifies that the change will be incorporated into all existing and future production units; and

f. If corrective action cannot be successfully taken as defined above, then the test shall be terminated, and the equipment shall be rejected.

9.6.3 Qualification Report Issuance and Post-Test Activities

Qualification report issuance and post-test activities encompass the activities described below:

a. The ITA may issue interim reports to the vendor, informing the vendor of the testing status, findings to date, and other information. Such reports do not constitute official test reports for voting system qualification;

b. The ITA shall prepare a Qualification Test Report that confirms the voting has passed the testing conducted by the ITA. The ITA shall include in the Qualification Test Report 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 Volume II;

c. Where a system is tested by multiple ITAs, each ITA shall prepare a Qualification Test Report;

d. The ITA shall deliver the Qualification Test Report to the vendor and to NASED;

e. NASED shall issue a single Qualification Number for the system to the vendor and to the ITAs. The issuance of a Qualification Number indicates that the system has been tested by certified ITAs for compliance with the national test standards and qualifies for the certification process of states that have adopted the national standards;

f. This number applies to the system as a whole only for the configuration and versions of the system elements tested by the ITAs and identified in the Qualification Test Reports. The Qualification Number does not apply to individual system components or untested configurations; and

g. The Qualification 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 ITA Qualification Test Reports based on the Qualification Number as part of their voting system certification and procurement processes systems that rely on the Standards.

9.6.4 Resolution of Testing Issues

The NASED Voting Systems Board (the Board) is responsible for resolving questions about the application of the Standards in the testing of voting systems. The Secretariat for the Board will relay its decisions to the NASED certified ITAs and voting system vendors. The Federal Election Commission will monitor these decisions in order to determine which of them, if any, should be reflected in a subsequent version of the standards.

Table of Contents

Volume I, Appendix A

A Glossary for Voting Systems

Glossary for Voting Systems

This glossary contains terms from the VSS–2002 as well as the inclusion of additional terms needed to understand voting and related areas such as security, human factors, and testing. Each term includes a definition and its source as well as an association, where

- Source is the source from which the definition originates. A list of these sources is found in section A.2.
- Association is the domain for which the term applies, e.g., voting, testing, security. There may be multiple domains identified for a term. There is no relevance given to the order in which the domains are listed. A list of these associations is found in section A.3.

At this time, a term may contain multiple definitions. The intent is to eventually select one definition per term, unless multiple definitions are necessary to convey the appropriate meanings of the term.

Some of the terms in the VSS–2002 have been deprecated due to changes in voting systems, voting process and/or mandates in HAVA. A list of these deprecated terms is in section A.4 List of Deprecated Terms.

A.1 Glossary

A

Abandoned Ballot: Ballot that the voter did not cast into the ballot box or record vote on DRE before leaving the polling place. See also fled voter.

Association: Voting.

Source: No attribution.

Absentee Ballot: Ballot prepared or designed for an absentee voter. Definition of an absentee ballot is jurisdiction dependent.

Association: Voting.

Source: No attribution.

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 or qualified system purchased.

Association: Testing, voting.

Source: VSS.

Access Board: Independent federal agency devoted to accessibility for people with disabilities.

Association: Human factors, HF: Accessibility.

Source: No attribution.

Accessibility: Measurable characteristic that indicates 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. The HAVA also includes accessibility requirements for Native American and Alaska Native citizens and alternative language access for voters with limited English proficiency.

Association: Human factors, HF: Accessibility.

Source: NIST HF Rpt, HAVA.

Accessible Voting Station (Acc-VS): Voting Station equipped for individuals with disabilities referred to in HAVA 301(a)(3)(B)

Association: HF: Accessibility, voting.

Source: HAVA.

Accreditation: (1) Formal recognition that a laboratory is competent to carry out specific tests or calibrations or types of tests or calibrations. (2) Procedure by which an authoritative body gives formal recognition that a body or person is competent to carry out specific tasks.

Association: Testing, standardization.

Source: (1) NIST HB 150, (2) ISO Guide 2–6.

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.

Association: Testing, conformity assessment.

Source: (1) ISO 17000, (2) IEEE 1583.

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.

Note 1: Accuracy is a qualitative concept.
NOTE 2: The term precision should not be used for accuracy.

Association: Testing.

Source: (1) IEEE 1583, (2) VIM.

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.

Association: Voting, testing.

Source: VSS.

Adequate Security: Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. See also risk assessment.

Association: Computer security.

Source: OMB A130.

Alternative Formats: In the context of voting systems, the ballot or accompanying information is said to be in an alternative format if it is in a representation other than the written English normally displayed to non-disabled English-literate voters. NOTE: The usual purpose of these formats is to provide accessibility to voters with disabilities or those with limited English proficiency. Examples include, but are not limited to, Braille, ASCII text, large print, recorded audio, and electronic formats that comply with Part 1194 of the standards for Section 508 of the Rehabilitation Act Amendments.

Association: HF: Accessibility.
Source: IEEE 1583, Section 508.

Alternative Language Voting Station (ALVS): voting station designed to be usable by voters who have limited English proficiency, i.e., cannot read English.

Association: HF: Accessibility, voting.
Source: No attribution.

Approval: Permission for a product or process to be marketed or used for stated purposes or under stated conditions. NOTE: Approval can be based on fulfillment of specified requirements or completion of specified procedures.

Association: Testing, conformity assessment.
Source: ISO 17000.

Attestation: Issue of a statement, based on a decision following review, that fulfillment of specified requirements has been demonstrated. NOTE: The resulting statement is also known as a statement of conformity.

Association: Testing, conformity assessment.
Source: ISO 17000.

Audio Ballot: Voter interface which provides the voter with audio stimuli and allows the voter to communicate intent to the voting system through vocalization or physical actions. See also ballot.

Association: Voting, human factors, HF: Accessibility.
Source: FL Statutes.

Audio-Tactile Interface (ATI): Voter interface designed so as 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.

Association: HF: Accessibility, voting.
Source: No attribution.

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. NOTE: While audit applies to management systems, assessment applies to conformity assessment bodies as well as more generally.

Association: Testing, conformity assessment, security.
Source: ISO 17000.

Audit Trail: Recorded information that allows election officials to view the steps that occurred on the equipment included in an election to verify or reconstruct the steps followed without compromising the ballot or voter secrecy.

Association: Voting, security.
Source: No attribution.

Audit Trail for DRE: Paper printout of votes cast, produced by direct response electronic (DRE) voting machines, which election officials may use to crosscheck electronically tabulated totals.

Association: Voting, security.
Source: NASS.

Availability: Ensuring timely and reliable access to and use of information.

Association: Security.
Source: 44 U.S.C.

B

Ballot: (1) Physical record of the selections made by a voter in all of the races or contests in a particular election. Typically used in the context of hand-counted paper, punched card, or optical mark-sense ballots. When the ballot is recorded in electronic form, the term ballot image is preferred. (2) An official presentation of all of the contests to be decided in a particular election. These may be printed on the ballot (sense 1), printed on a ballot label (as used for punched-card and mechanical-lever voting machines), presented on a computer display screen, or in some alternative form such as audio. See also, audio ballot, ballot image, video ballot, electronic voter interface.

Association: Voting.
Source: No attribution.

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.

Association: Voting.
Source: No attribution.

Ballot Counter: Counter in a voting device that counts the ballots cast in a single election or election test.

Association: Voting.
Source: VSS.

Ballot Counting Logic: 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. States differ from each other in the way they define valid and invalid votes and in their vote-counting procedures.

Association: Voting.
Source: VSS.

Ballot Format: One of any number of specific ballot configurations issued to the appropriate precinct. At a minimum, ballot formats differ from one another in content. They may also differ in size of type, graphical presentation, language used, or method of presentation (e.g., visual or audio). Also referred to as ballot style.

Association: Voting.
Source: VSS.

Ballot Image: (1) Electronically produced record of all votes cast by a single voter. (2) Record of all votes produced by a single voter. See also Cast Vote Record

Association: Voting.
Source: (1) VSS, (2) no attribution.

Ballot Instructions: The official instructional material presented with the ballot (sense 2) to the voter. In some contexts, this is in the form of an instructional poster in the voting booth, in some contexts, as text on the ballot label, in any form, presented to voters for expressing their selections in an election. This may be printed on the ballot (sense 1), presented in audio form, posted in the voting booth, printed on the ballot label or presented with the ballot presentation.

Association: Voting.
Source: No attribution.

Ballot Measure: A contest on ballot where the voter may vote yes or no. This term is typically used for referenda, amendments to state constitutions and tax questions, but not for yes/no votes in judicial retention races.

Association: Voting.
Source: No attribution.

Ballot Preparation: Process of using election databases or other means to select 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.

Association: Voting.
Source: VSS.

Ballot Position: Abstract choice that is represented by a single line item where a vote may be recorded in a ballot or ballot image.

Association: Voting.
Source: VSS.

Ballot Production: Process of converting the ballot format to a medium ready for use in the physical ballot production or electronic presentation.

Association: Voting.
Source: VSS.

Ballot Rotation: Process of varying the order of the candidate names within a given contest to reduce the impact of voter bias towards the candidate(s) listed first.

Association: Voting.
Source: VSS.

Ballot Set: See ballot image.
Association: Voting.

Source: VSS.

Ballot Scanner: Device used to read the data from a marksense ballot.
Association: Voting.
Source: VSS.

Ballot Style: See ballot format.
Association: Voting.
Source: VSS.

Baseline: Product configuration that has been formally submitted for review against the VVSG, which thereafter serves as the basis for further development; and can be changed and offered to jurisdictions only through formal change control and requalification procedures (and/or recertification procedures where applicable).
Association: Voting, testing.
Source: VSS.

C

Calibration: Set of operations that establish, under specified conditions, the relationship between values indicated by a measuring instrument or measuring system, or values represented by a material measure, and the corresponding known values of a quantity intended to be measured.
Association: Testing.
Source: NIST HB 150.

Candidate: Person contending in a race for office. A candidate may be explicitly presented as one of the choices on the ballot or may be a write-in candidate.
Association: Voting.
Source: NIST HF Rpt.

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.
Association: Voting.
Source: VSS, IEEE 1583.

Canvass: (1) Compilation of election returns and validation of the outcome that form the basis of the official results by political subdivision. (2) Compilation of election returns for validation and approval by the political subdivision of the outcome, which form the basis for the official results.
Association: Voting.
Source: (1) VSS, IEEE 1583, (2) no attribution.

Cast Ballot: Ballot in which voter has taken final action in the selection of candidates and measures and submits the ballot to the appropriate jurisdiction.
Association: Voting.
Source: No attribution.

Cast Vote Record (CVR): Permanent record of all votes produced by a single voter whether in electronic or paper copy form. Used for counting votes. Also referred to as ballot set or ballot image when used to refer to electronic ballots.
Association: Voting.
Source: (1) IEEE 1583.

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.
Association: Voting.
Source: VSS.

Central Counting: Counting of ballots in one or more locations selected by the election authority for the processing or counting, or both, of ballots.
Association: Voting.
Source: IL Statutes.

Certification: (1) Procedure by which a third party gives written assurance that a product, process or service conforms to specified requirements. (2) Third-party attestation related to products, processes, systems or persons. See also State Certification and EAC Certification.
Association: Testing, conformity assessment.
Source: (1) ISO Guide 2–6, (2) ISO 17000.

Certification Testing: Deprecated, replaced by State Certification. Note: This term is being clarified with respect to testing State or Federal Standards. See also EAC Certification.
Association: Testing, conformity assessment, voting.
Source: VSS.

Challenged Ballot: Ballot provided to individuals whose eligibility to vote has been questioned. Once voted, such ballots are not included in the tabulation until after the voter's eligibility is confirmed. See also provisional ballot.
Association: Voting.
Source: VSS.

Checksum: Computed value representing the sum of the contents of an instance of digital data; used to check whether errors have occurred in transmission or storage.
Association: Security.
Source: No attribution.

Claim of Conformance: Statement by a vendor proclaiming that a specific product conforms to a particular standard or set of standard profiles, a claim which is verified or refuted by a testing authority.
Association: Testing, conformity assessment.
Source: No attribution.

Client: Any person or organization that engages the services of a testing or calibration laboratory.
Association: Testing.
Source: NIST HB 150.

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, along with nonpartisan offices and ballot issues presented at the same election.
Association: Voting.
Source: VSS.

Commercial Off-the-Shelf (COTS): Commercial, readily available hardware devices (which may be electrical, electronic, mechanical, etc.; such as card readers, printers, or personal computers) or software products (such as operating systems, programming language compilers, database management systems, subsystems, components; software, etc.).
Association: IT.
Source: VSS, IEEE 1583.

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

Compliance point: Identified, testable requirement.
Association: Testing, conformity assessment.
Source: No attribution.

Component: (1) Element within a larger system; a component can be hardware or software. For hardware, 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, a module of executable code that performs a well-defined function and interacts with other components. (2) Individual elements or items that collectively comprise a device, e.g., circuit boards, internal modems, processors, disk drives, and computer memory.
Association: IT.
Source: (1) No attribution, (2) VSS.

Confidentiality: (1) Prevention of unauthorized disclosure of information. (2) Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Association: Security.
Source: (1) IEEE 1583, (2) 44 U.S.C.

Configuration Identification: Element of configuration management, consisting of selecting the configuration items for a system and recording their functional and physical characteristics in technical documentation.
Association: Testing, software engineering.

Source: IEEE 1583.

Configuration Item: Aggregation of hardware, software, or both that is designated for configuration management and treated as a single entity in the configuration management process.

Association: Testing, software engineering.

Source: IEEE 1583.

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.

Association: Testing, software engineering.

Source: IEEE 1583.

Configuration Management Plan: Document detailing the process for identifying, controlling and managing various released items (code, hardware, documentation etc.)

Association: Testing, software engineering.

Source: IEEE 1583.

Conformance: See conformity

Association: Testing, standardization.

Source: No attribution.

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 conformity assessment.

Association: Testing, standardization.

Source: NIST HB 150.

Conformity: Fulfillment by a product, process or service of specified requirements.

Association: Testing, standardization.

Source: ISO Guide 2–6.

Conformity Assessment: Demonstration that specified requirements relating to a product, process, system, person or body are fulfilled. See also testing, inspection, certification, accreditation, conformity assessment bodies.

Association: Testing, standardization.

Source: ISO 17000.

Conformity Assessment Body: Body that performs conformity assessment services. NOTE: An accreditation body is not a conformity assessment body.

Association: Testing, standardization.

Source: ISO 17000.

Consensus: General agreement, characterized by the absence of sustained opposition to substantial issues by any important part of the concerned interests and by a process that involves seeking to take into account the views of all parties concerned and to reconcile any conflicting arguments.

Association: Standardization.

Source: ISO Guide 2–4.

Contest: Decision to be made within an election, which may be a race for office or a referendum, propositions and/or questions. A single ballot may contain one or more contests.

Association: Voting.

Source: No attribution.

Count: Process of totaling votes.

Association: Voting.

Source: VSS, IEEE 1583.

Counted Ballot: Ballot that has been processed and whose votes are included in the candidate and measures vote totals.

Association: Voting.

Source: No attribution.

Corrective Action: Action taken to eliminate the causes of an existing deficiency or other undesirable situation in order to prevent recurrence.

Association: Testing.

Source: NIST HB 143.

Cross Filing: See Cross-party Endorsement.

Association: Voting.

Source: VSS.

Cross-party Endorsement: Endorsement of a single candidate or slate of candidates by more than one political party. The candidate or slate appears on the ballot representing each endorsing political party. Also referred to as cross filing.

Association: Voting.

Source: VSS, IEEE 1583.

Cryptographic Key: Value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification.

Association: Security.

Source: NIST SP 800–63.

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, or prevent their undetected modification.

Association: Security.

Source: NIST SP 800–59.

Cumulative Voting: Practice where voters are permitted to cast as many votes as there are seats to be filled. Voters are not limited to giving only one vote to a candidate. Instead, they can put multiple votes on one or more candidates.

Association: Voting.

Source: VSS, IEEE 1583.

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.

Association: Testing, security.

Source: (1) VSS, (2) IEEE 1583.

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.

Association: Security.

Source: IEEE 1583.

Decertification: Withdrawal of certification of voting system hardware and software.

Association: Testing, conformity assessment.

Source: HAVA.

Design Entity: Component of a design, named and referenced uniquely, that is both structurally and functionally different from other elements.

Association: Software engineering.

Source: IEEE 1583.

Design Entity Attributes: Named characteristic or property of a design entity, which provides a statement of fact about the entity. Attributes define the design entity and not the design process.

Association: Software engineering.

Source: IEEE 1583.

Designating Authority: Body established within government or empowered by government to designate conformity assessment bodies, suspend or withdraw their designation or remove their suspension from designation.

Association: Testing, conformity assessment.

Source: ISO 17000.

Designation: Governmental authorization of a conformity assessment body to perform specified conformity assessment activities.

Association: Testing, conformity assessment.

Source: ISO 17000.

Device: Functional unit that performs its assigned tasks as an integrated whole.

Association: IT.

Source: VSS.

Digital Signature: 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 authentication and integrity protection.

Association: Security.

Source: SP 800–63.

Direct Record Electronic (DRE) Voting System: Voting system that records votes by means of a ballot display provided with mechanical or electro-optical components that can be actuated by the voter, that processes the data by means of a computer program, and that records voting data and cast vote records in internal and/or external memory components. It produces a tabulation of the voting data stored in a removable memory component and/or in printed copy.

Association: Voting

Source: VSS, IEEE 1583.

Directly Verified: Voting system 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 of a directly verified voting system include DRE with a voter verified paper trail or marksense system. This is in contrast with an indirectly verified voting system.

Association: Voting, security.

Source: No attribution.

Disability: Disability means, with respect to an individual, (a) a physical or mental impairment that substantially limits one or more of the major life activities of such individual, (b) a record of such an impairment, or (c) being regarded as having such an impairment.

Association: Human factors, HF: Accessibility

Source: ADA.

DRE Display: Part of the DRE that displays the electronic record.

Association: Security, voting.

Source: No attribution.

DRE–VVPAT: DRE voting system containing VVPAT capability. See also Direct Record Electronic Voting System and Voter Verified Paper Audit Trail.

Association: Security, voting.

Source: No attribution.

Dynamic Voting System Software: Software that changes over time once it is installed on the voting equipment. See also voting system software.

Association: Voting.

Source: No attribution.

E

EAC: Election Assistance Commission.

Early Voting: Voter completes the ballot in person at a county office or other designated polling site or ballot drop site prior to Election Day. The ballot is cast and not retrievable. NOTE: Early voting is not the same as absentee voting. Also known as Early In-Person Voting.

Association: Voting.

Source: Electionline.

Election Coding: See Election Programming.

Association: Voting.

Source: IEEE 1583.

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.

Association: Voting.

Source: VSS, IEEE 1583.

Election Definition: Abstract definition of the races and questions that may appear on ballot forms.

Association: Voting.

Source: No attribution.

Election District: 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.

Association: Voting.

Source: VSS, IEEE 1583.

Election Management System: Set of processing functions and databases within a Voting System that define, develop and maintain election databases, perform election definition and setup functions, format ballots, count votes, consolidate and report results, and maintain audit trails.

Association: Voting.

Source: VSS, IEEE 1583.

Election Officials: Term used to designate the group of people associated with conducting an election, including election personnel and poll workers.

Association: Voting.

Source: No attribution.

Election Programming: Process by which election officials or their designees use voting system software to logically define the ballot for a specific election.

Association: Voting.

Source: VSS, IEEE 1583.

Electronic Ballot Printer (EBP): DRE-like device that fully prints paper-based ballots with selected vote choices for tabulation by a separate ballot scanner.

Association: Voting.

Source: IEEE 1583.

Electronic Cast Vote Record (ECVR): Deprecated, replaced by Cast Vote Record (CVR).

Association: Voting.

Source: IEEE 1583.

Electronic Vote Capture System (EVCS): Election system that encompasses DREs as well as accessible ballot printers (ABPs) when they are combined with the ballot scanner that processes the printed ballot. See also Voter Verified Paper Audit.

Association: Voting.

Source: IEEE 1583.

Electronic Voter Interface: Subsystem within a DRE voting system which communicates ballot information to a voter in video, audio or Braille form and which allows the voter to select candidates and issues by means of vocalization or physical actions.

Association: Voting, Human factors, HF: Accessibility.

Source: FL Statutes.

Electronic Voting Machine: Any system that utilizes an electronic component. Term is generally used to refer to DREs. See also Voting Equipment, Voting System.

Association: Voting.

Source: NASS.

Electronically-Assisted Ballot Marker (EBM): Machines that provide assistance to voters who are visually impaired, who have difficulty reading English, or in other cases where a voter has difficulty correctly marking by hand a preprinted paper ballot that is to be counted in optical scan systems. The device marks, or helps to mark selected vote choices on a previously inserted, preprinted paper ballot. The machine then provides audio, tactile, or visual feedback to the voter on what choices they have made on the ballot. The resulting ballots are later tabulated on the same unit that processes ordinary hand-marked paper ballots.

Association: Voting, human factors.

Source: IEEE 1583.

Entity Relationship Diagram (ERD): A data modeling technique that creates a graphical representation of the entities, and the relationships between entities, within an information system.

Association: Software engineering.

Source: IEEE 1583.

Error correction code: Coding system that incorporates extra parity bits in order to detect errors.

Association: Security.

Source: WordNet.

E-Voting: (1) Term frequently used to refer to DREs and other types of electronic voting equipment, but may be misleading as it implies remote access via a computer network or the Internet. (2) Election system that allows a voter to record his or her secure and secret ballot electronically. See also DRE, Electronic Voting Machine.

Association: Voting.
Source: (1) NASS, (2) Whatis.com.

F

Federal Information Processing Standard (FIPS): Standard for adoption and use by federal agencies that has been developed within the National Institute of Standards and Technology (NIST) Information Technology Laboratory and published by NIST, an part of the U.S. Department of Commerce.
Association: Security, standardization.
Source: No attribution.

Firmware: Computer programs (software) stored in read-only memory (ROM) devices embedded in the system and not capable of being altered during system operation.
Association: IT.
Source: IEEE 1583.

Fled Voter: Voter who has begun the process of using voting equipment to cast a ballot and has exited the polling site without completing the casting of the ballot, thereby leaving the voting equipment in a state in which election procedures must be used to decide whether the fled voter's incomplete ballot will be cast before the voting equipment is reset. See also abandoned ballot.
Association: Voting.
Source: No attribution.

Font: Family or assortment of characters of a given size and style, e.g., 9-point Bodoni modern. See type font.
Association: Human factors, typography.
Source: ANSI Dict.

Functional Configuration Audit (FCA): 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's Voter Manual, Operations Procedures, Maintenance Procedures, and Diagnostic Testing Procedures.
Association: testing, voting.
Source: VSS, IEEE 1583.

Functional Test: Test performed to verify or validate the accomplishment of a function or a series of functions.
Association: Testing.
Source: VSS, IEEE 1583.

G

General Election: Election in which voters, regardless of party affiliation, are permitted to select persons to fill public office and vote on ballot issues. Where the public office may be filled by a candidate affiliated with a political party or when permitted by law, unaffiliated candidate and voters choose among the candidates.
Association: Voting.
Source: VSS, IEEE 1583.

H

Hash: Algorithm that maps a bit string of arbitrary length to a fixed-length bit string. Approved hash functions satisfy the following properties: (a) It is computationally infeasible to find any input that map to any prespecified output, and (b) it is computationally infeasible to find any two distinct inputs that map to the same output.
Association: Voting.
Source: NIST SP 800–63.

HAVA: Help America Vote Act of 2002.
Association: Voting.
Source: No attribution.

Human Computer Interaction: Discipline concerned with the design, evaluation and implementation of interactive computing systems for human use and with the study of major phenomena surrounding them.
Association: Human factors.
Source: ACM SIGCHI.

Human Factors (or Ergonomics): Scientific discipline concerned with the understanding of interactions among humans and other elements of a system, and the profession that applies theory, principles, data and methods to design in order to optimize human well-being and overall system performance.
Association: Human factors.
Source: IEA.

I

Indirectly Verified: Voting system that allows a voter to verify the ballot produced by his or her vote only via hardware or software intermediary. An example of an indirectly verified voting system is a touch screen DRE where the voter verifies the ballot through the assistance of audio stimuli. This is in contrast to directly verified voting systems.
Association: Voting, security.
Source: No attribution.

Implementation Conformance Statement: See Implementation Statement.

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.
Association: Testing.
Source: No attribution.

Independent Testing Authority (ITA): Deprecated, replaced by Voting System Testing Laboratory. Organization certified by the National Association of State Election Directors (NASED) to perform qualification testing.
Association: Testing, Voting.
Source: VSS.

Information Security: Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.
Association: Security.
Source: 44 U.S.C.

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. NOTE: Inspection of a process may include inspection of persons, facilities, technology and methodology.
Association: Testing, conformity assessment.
Source: ISO 17000.

Integrity: (1) Prevention of unauthorized modification of information. (2) Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Association: Security.
Source: (1) IEEE 1583, (2) 44 U.S.C.

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.
Association: Security.
Source: FIPS 140–2.

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, etc.) and that all voting positions can be voted for the maximum number of eligible candidates and that results are accurately tabulated and reported.
Association: Voting, testing.
Source: IEEE 1583.

Logical Correctness: Condition signifying that, for a given input, a computer program will satisfy the program specification (produce the required output).
Association: Testing.
Source: VSS, IEEE 1583.

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.
Association: Voting.
Source: VSS, IEEE 1583.

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.
Association: Voting.
Source: VSS, IEEE 1583.

Mechanical Lever Voting Machine: Machine that directly records a voter's choices via mechanical level-actuated controls into a counting mechanism that tallies the votes without using a physical ballot.
Association: Voting.
Source: ME Statutes.

Multi-seat Content: 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. Also known as field race.
Association: Voting.
Source: NIST HF Rpt.

N

NVLAP: The NIST National Voluntary Laboratory Accreditation Program.
Association: Testing.
Source: No attribution.

Non-partisan Office: Elected office for which candidates run independent of political party affiliation.
Association: Voting.
Source: VS, IEEE 1583.

Nonvolatile Memory: Memory in which information can be stored indefinitely with no power applied. Static RAM, ROMs and EPROMs are examples of nonvolatile memory.
Association: IT.
Source: VSS, IEEE 1583.

O

On-Site Absentee Voting: See Early Voting.

Open Primary: Primary election in which voters, regardless of political affiliation, may choose in which party's primary they will vote. 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. Voters also may be permitted to vote on nonpartisan offices and ballot issues that are presented at the same election.
Association: Voting.
Source: VSS, IEEE 1583.

Operational Environment: See Voting Equipment Operational Environment.
Association: Voting, IT.
Source: IEEE 1583.

Operations Procedures: See Voting Equipment Operations Procedures.
Association: Voting, IT.
Source: IEEE 1583.

Optical Scan, Optical Scan System: See Marksense.
Association: Voting.
Source: IEEE 1583.

Overvotes: (1) Generally prohibited practice of voting for more than the allotted number of candidates for the office being contested. (2) The voting for more than the allotted number of selections in a race. (3) Occurs when the number of alternatives selected by a voter in a contest exceeds the maximum number allowed for that contest. Also known as overvoting.
Association: Voting.
Source: (1) VSS, (2) IEEE 1583, (3) NIST HF Rpt.

P

Paper-based Voting System: Voting system that records votes, counts votes, and produces a tabulation of the vote count, using one or more ballot cards or a written list of choices.
Association: Voting.
Source: VSS, IEEE 1583.

Paper Record: Paper ballot image or summary that is a copy of the electronic record and that is verifiable by a voter. See also ballot image.
Association: Voting, security.
Source: No attribution.

Partisan Office: Elected office for which (partisan and non-partisan) candidates run as representatives of a political party.
Association: Voting.
Source: VSS, IEEE 1583.

Pass/Fail Criteria: Decision factor or expected result used to determine if software or hardware passes a test case.
Association: Testing.
Source: IEEE 1583.

Physical Configuration Audit (PCA): (1) Inspection that 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 VVSG. As part of the PCA, the building of the executable system to ensure that the qualified executable release is built from the tested components is also witnessed. (2) Review, by the test authority, of the vendor's technical documentation, source code, and observation of the code compile.
Association: Testing, voting.
Source: (1) VSS, (2) IEEE 1583.

Precinct Count: Counting of ballots on automatic tabulating equipment provided by the election authority in the same precinct polling place in which those ballots have been cast.
Association: Voting.
Source: IL Statutes.

Point Size: Method of measuring type, where the size of a font is measured from the top of the tallest character to the bottom of the lowest character.
Association: Human factors, typography.
Source: No attribution.

Political Subdivision: Any unit of government, such as counties and cities but often excepting school districts, having authority to hold elections for public offices or on ballot issues.
Association: Voting.
Source: VSS.

Polling Location: Physical address of a polling place.
Association: Voting.
Source: VSS, IEEE 1583.

Polling Place: Facility that is staffed by poll workers and equipped with voting equipment, to which voters from a given precinct come to cast in-person ballots. See also voting station.
Association: Voting.
Source: VSS, IEEE 1583.

Precinct: Administrative division representing a geographic area in which voters cast ballots at the same polling place. Voters casting absentee ballots may also be combined into one or more administrative absentee precincts for purposes of tabulating and reporting votes. Generally, voters in a polling place precinct are eligible to vote in a general election using the same ballot format. In some jurisdictions, however, the ballot formats may be different due to split precincts or required ballot rotations within the precinct.
Association: Voting.
Source: VSS, IEEE 1583.

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 in short intervals of time. (2) Degree of refinement in measurement or specification, especially as represented by the number of digits given.
Association: Testing, statistics.

Source: IEEE 1583.

Pre-Standard: Document that is adopted provisionally by a standardizing body and made available to the public in order that the necessary experience may be gained from its application on which to base a standard.
Association: Standardization.
Source: ISO Guide 2–4.

Primary Election: Election held to determine which candidate will represent a political party 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.
Association: Voting.
Source: VSS.

Primary Presidential Delegation Nominations: Primary election in which voters choose the delegates to the Presidential nominating conventions allotted to their states by the national party committees.
Association: Voting.
Source: VSS.

Privacy: Voting system is said to provide privacy when it makes it impossible for others to find out how the voter voted.
Association: Security, voting.
Source: No attribution.

Private Key: The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data.
Association: Security.
Source: NIST SP 800–63.

Profile: (1) Subset of a standard for a particular constituency that identifies the features, options, parameters, and implementation requirements necessary for meeting a particular set of requirements. (2) Specialization of a standard for a particular context, with constraints and extensions that are specific to that context.
Association: Standardization.
Source: (1) ISO 8632, (2) no attribution.

Provisional Ballot: Ballot provided to individuals who claim they are eligible to vote but whose eligibility cannot be confirmed when they present themselves to vote. Once voted, such ballots are not included in the tabulation until after the voter's eligibility is confirmed. See also challenged ballot.
Association: Voting.
Source: VSS, IEEE 1583, NASS.

Public Information Package (PIP): Data to be published openly and made available to all without let or hindrance, irrespective of need-to-know.
Association: Testing.
Source: No attribution.

Public Key: Public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.
Association: Security.
Source: NIST SP 800–63.

Public Key Certificate: Digital document issued and digitally signed by the private key of a Certification Authority that binds the name of a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the private key.
Association: Security.
Source: NIST SP 800–63.

Public Network Direct Record Electronic (DRE) Voting System: Form of DRE voting system that uses electronic ballots and transmits vote data from the polling place to another location (such as a central count facility) over a public network beyond the control of the election authority.
Association: Voting.
Source: VSS.

Punchcard Voting System: Voting system where votes are recorded by means of punches made in voting response fields designated on one or both faces of a ballot card or series of cards.
Association: Voting.
Source: VSS, IEEE 1583.

Q

Qualification Number: Deprecated. A number issued by NASED (National Association of State Election Directors) to a system that has been tested by certified Independent Test Authorities for compliance with the qualification test standards. Issuance of a Qualification Number indicates that the system qualifies for certification process of states that have adopted the Standards. Note: Qualification Numbers for Voting Systems that were qualified for compliance to the 1990 Voting System Standards are still valid. Voting Systems that were qualified for compliance to the Voting System Standards 2002 will need to be assigned an EAC Certification number.
Association: Testing, voting.
Source: VSS.

Qualification Test Report: Deprecated, replaced by Test Report for EAC Certification.
Association: Testing, voting.
Source: VSS, NIST HB150.

Qualification Testing: Examination and testing of a computerized voting system by using qualification test standards to determine if the system complies with the qualification performance and test standards and with its own specifications. This process occurs prior to state certification.
Association: Testing, voting.
Source: VSS.

Quality Assurance Plan: Document that identifies the system and actions required to provide adequate assurance that an item or product conforms to the documented technical requirements.
Association: Testing.
Source: IEEE 1583.

Quality Control: Operational techniques and activities that are used to fulfill requirements for quality.
Association: Testing.
Source: NIST HB 150.

Quality Manual: Document stating the quality policy and describing the quality system of an organization.
Association: Testing, software engineering.
Source: NIST HB 150.

R

Race: Contest between candidates.
Association: Voting.
Source: No attribution.

Ranked Order Voting: Practice that allows voters to rank candidates in a contest in order of choice: 1, 2, 3 and so on. It takes a majority to win. If anyone receives a majority of the first choice votes, that candidate wins that election. If not, the last place candidate is deleted, and all ballots are counted again, but this time each ballot cast for the deleted candidate counts for 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.
Association: Voting.
Source: VSS, IEEE 1583.

Read Ballot: Ballot that has been processed but may or may not be counted.
Association: Voting.
Source: No attribution.

Recall Issue with Options: Process that allows voters to remove their elected representatives from office prior to the expiration of their terms of office. Often, the recall involves not only the question of whether a particular officer should be removed from office, but also the question of naming a successor in the event that there is an affirmative vote for the recall.
Association: Voting.
Source: VSS.

Recertification: State examination, and possibly the retesting of a voting system that was modified subsequent to

receiving state certification. The object of this process is to determine if the modification still permits the system to function properly in accordance with state requirements.

Association: Voting.

Source: VSS, IEEE.

Record: (n) Data that are preserved by a voting system, not necessarily in any particular form. (v) To preserve such data.

Association: Voting.

Source: No attribution.

Records: Recordings of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).

Association: Security.

Source: NIST SP 800–53.

Recount: Process conducted for verifying the votes counted in an election.

Association: Voting.

Source: No attribution.

Referendum: Contest between two (or more) choices in response to a question (e.g., bond issue, recall, retention of a judge in office, proposed amendment).

Association: Voting.

Source: NIST HF Rpt.

Repeatability: Ability to obtain independent test results by using the same testing method on identical test items in the same testing laboratory by the same operator using the same equipment within short intervals of time.

Association: Testing, conformity assessment.

Source: ISO 5725.

Report: (n) Printed record, formatted for human readability, that is produced by a voting system. (v) to produce such a record.

Association: Voting.

Source: No attribution.

Reproducibility: Ability to obtain test results with the same test method on identical test items in different testing laboratories with different operators using different equipment.

Association: Testing, conformity assessment.

Source: ISO 5725.

Requirement: Provision that conveys criteria to be fulfilled. See also compliance point.

Association: Testing, standardization.

Source: NIST HB 150.

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, failure to cast ballot before leaving polling place).

Association: Voting, human factors.

Source: NIST HF Rpt.

Risk Assessment: Process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact.

Association: Security.

Source: NIST SP 800–30.

Rolloff: Difference between number of votes cast for contests in the higher offices on the ballot and the number cast for contests that are lower on the ballot. It sometimes referred to as voter fatigue.

Association: Voting, human factors.

Source: NIST HF Rpt.

Runoff Election: Election to select a winner following a primary, or sometimes 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 race in question proceed to the runoff election.

Association: Voting.

Source: VSS, IEEE 1583.

S

Second Chance Voting: Provides that voters are notified when their ballots contain errors and are given a chance to correct them. Required by HAVA 2002.

Association: Voting.

Source: NASS.

Secret Key: Cryptographic key that is used with a symmetric cryptographic algorithm that is uniquely associated with one or more entities and is not be made public. The use of the term ''secret'' in this context does not imply a classification level, but rather implies the need to protect the key from disclosure.

Association: Security.

Source: NIST SP 800–57.

Section 508: Amendment by Congress in 1998, to the Rehabilitation Act to require federal agencies to make their electronic and information technology accessible to people with disabilities. Section 508 was enacted to eliminate barriers in information technology.

Association: HF: accessibility

Source: No attribution.

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.

Association: Security.

Source: FIPS 199, NIST SP 800–53.

Semi-static Voting System Software: Software that 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 the voting system software on voting equipment or the election specific software such as ballot formats. See also voting system software.

Association: Voting.

Source: No attribution.

Specification, Technical: Document that prescribes technical requirements to be fulfilled by a product, process or service.

Association: Standardization.

Source: ISO Guide 2–4.

Split Precinct: Precinct containing more than one ballot format in order to accommodate a contiguous geographic area served by the precinct that contains more than one election district.

Association: Voting.

Source: VSS, IEEE 1583.

Spoiled Ballot: Ballot that has been voted but will not be cast.

Association: Voting.

Source: No attribution.

Standard: Document established by consensus and approved by a recognized body that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.

Association: Standardization.

Source: ISO Guide 2–4.

Standard, Product: Standard that specifies requirements to be fulfilled by a product or a group of products, to establish its fitness for purpose. A product standard may include, in addition to the fitness for purpose requirements, directly or by reference, aspects such as terminology, sampling, testing, packaging, and labeling and sometimes processing requirements.

Association: Standardization.

Source: ISO Guide 2–6.

Standard, Testing: Standard that is concerned with test methods, sometimes supplemented with other provision related to testing, such as sampling, use of statistical methods, or sequence of test.

Association: Standardization.

Source: ISO Guide 2–6.

Standard on Data to Be Provided: Standard that contains a list of characteristics for which values or other data are to be stated for specifying the product, process, or service.

Association: Standardization.

Source: ISO Guide 2–4.

State Certification: State examination and possibly testing of a voting system to determine its compliance with state laws, regulations, and rules and any other state requirements for vote systems.

Association: Testing, conformity assessment, voting.

Source: VSS.

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. See also voting system software.

Association: Voting.

Source: No attribute.

Straight Party Voting: Mechanism by which voters are permitted to cast a vote indicating the selection of all candidates on the ballot for a single political party.

Association: Voting.

Source: VSS, IEEE 1583.

Support Software: Software that aids in the development or maintenance of other software, for example, compilers, loaders and other utilities.

Association: IT.

Source: VSS, IEEE 1583.

Symmetric (Secret) Encryption Algorithm: Encryption algorithms using the same secret key for encryption and decryption.

Association: Security.

Source: NIST SP 800–49.

T

Tabulation: See Count.

Association: Voting.

Source: VSS, IEEE 1583.

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.

Association: Human Factors, HF: Accessibility.

Source: ANSI C63.19.

Tabulator: Device that counts votes.

Association: Voting.

Source: No attribution.

Technical Data Package: Vendor documentation relating to the voting system that shall be submitted with the system as a precondition of qualification testing.

Association: Testing, voting.

Source: VSS.

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.

Association: IT.

Source: IEEE 1583.

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.

Association: Testing.

Source: ISO Guide 2–4, NIST HB 150.

Test Campaign: Sum of the work by a VSTL on a single product or system from contract through test plan, conduct of testing for each requirement (including hardware, software, and systems), reporting, archiving, and responding to issues afterwards.

Association: Testing, voting.

Source: NIST HB 150–22.

Test Case Specification: Document identifying the specific inputs and expected result for each test identified in the test plan.

Association: Testing.

Source: IEEE 1583.

Test Design Specification: Expanded detail of the test approach identified in the test plan for the related tests.

Association: Testing.

Source: IEEE 1583.

Test Method: Specified technical procedure for performing a test.

Association: Testing, conformity assessment.

Source: ISO Guide 2.

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.

Association: Testing, conformity assessment.

Source: IEEE 1583.

Testing: Determination of one or more characteristics of an object of conformity assessment, according to a procedure. Testing typically applies to materials, products, or processes.

Association: Testing, conformity assessment.

Source: ISO 17000.

Testing Authority: Organization that performs qualification testing and produces qualification test reports. See also Voting System Testing Laboratory.

Association: Testing, conformity assessment.

Source: No attribution.

Test Report for EAC Certification: Report of results of independent testing of a voting system indicating the data testing was completed, the specific system version tested, and the scope of tests conducted.

Association: Testing, voting.

Source: VSS, NIST HB 150.

Touch Screen Voting Machine: Machine that utilizes a computer screen whereby a voter executes that voter's choices by touching designated locations on the screen and that then tabulates those choices.

Association: Voting.

Source: ME Statutes.

Traceability: Ability to relate a property of the result of a measurement or the value of a standard to stated references.

Association: Testing.

Source: VIM.

Type font: Type of a given size and style, e.g., 10-point Bodoni Modern.

Association: Human factors.

Source: ANSI Dict.

U

Uncertainty: Parameter, associated with the result of a measurement that characterizes the dispersion of the values that could reasonably be attributed to that which is being measured.

Association: Testing.

Source: VIM, NIST HB 150.

Undervote: (1) Occurs when the number of alternatives selected by a voter in a contest is less than the maximum number allowed for that contest. (2) Practice of voting for less than the total number of election contests listed on the ballot, or of voting for less than the number of positions to be filled for a single office (i.e., A person would undervote if a contest required the selection of three out of a given number of candidates, and the voter chose only two candidates). Also known as undervoting.

Association: Voting.

Source: (1) NIST HF Rpt. (2) VSS, IEEE 1583, NASS.

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 system standards refers to voters being able to cast valid votes as they intended quickly, without errors and with confidence that their ballot choices as marked were recorded correctly. It also refers to the usability of the setup of voting equipment for the election and the running of the election by poll workers and election administrators.

Association: Human factors, HF: Usability.

Source: ISO 9241, NIST HF Rpt.

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.

Association: Human factors, HF: Usability.

Source: Usability First Usability Glossary.

User Documentation: See Voting Equipment User Documentation.

Association: Vote, test.

Source: IEEE 1583.

V

Valid Vote: Vote from a ballot or ballot image that conforms to jurisdiction dependent criteria for accepting or rejecting entire ballots, such as stray marks policies and voter eligibility criteria, in a contest that was not overvoted.

Association: Voting.

Source: No attribution.

Validation: Process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements.

Association: Testing.

Source: VSS.

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.

Association: Testing.

Source: VSS.

Verification and Validation (V&V): Process of determining whether requirements for a system or component are complete and correct, the products of each development phase fulfill the requirements or conditions imposed by the previous phase, and the final system or component complies with specified requirements.

Association: Testing.

Source: IEEE 1583.

Video Ballot: Electronic voter interface which presents ballot information and voting instructions as video images. See also ballot.

Association: Voting, human factors, HF: Accessibility.

Source: FL Statutes.

Vote Capture Station: Component of a voting system that captures and stores records of voter choices. See also witness device.

Association: Voting.

Source: No attribution.

Vote for N of M: Ballot choice in which voters are allowed to vote for a limited number of candidates for a single office from a larger field of candidates.

Association: Voting.

Source: VSS, IEEE 1583.

Voted Ballot: Ballot that a voter has finished filling in, but has not yet cast or spoiled.

Association: Voting.

Source: No attribution.

Voter Registration System: Set of processing functions and data storage that maintains records of eligible voters. This system generally is not considered a part of a Voting System subject to the 2002 Voting System Standards.

Association: Voting.

Source: VSS.

Voter Verified Audit Record: (1) Human-readable printed record of all of a voter's selections presented to the voter before the vote is cast. (2) Printed version of the ballot that voters may view and check for accuracy before their votes are cast. See also Voter Verified Record or Voter Verified Paper Trail.

Association: Voting.

Source: (1) IEEE 1583, (2) NASS.

Voter-Verified Paper Trail (VVPT): See Voter Verified Audit Record.

Voting Environment: Aspects of the voting milieu outside of the voting system that are encountered by voters, e.g., ramps, lighting, noise, temperature, electro-magnetic interference. See also voting equipment operational environment.

Association: Human factors, voting.

Source: No attribution.

Voting Equipment: Any mechanical, electromechanical, or electronic components of a voting system. See also Electronic Voting Machine.

Association: Voting.

Source: No attribution.

Voting Equipment 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. See also voting environment.

Association: Voting.

Source: IEEE 1583.

Voting Equipment Operations Procedures: Ordered steps that election personnel, poll workers or voters follows to perform the tasks for each operational environment.

Association: Voting.

Source: IEEE 1583.

Voting Equipment User Documentation: Electronic or printed material that provides information for the election officials or voters.

Association: Voting.

Source: IEEE 1583.

Voting Machine: Mechanical or electronic equipment for the direct recording and tabulation of votes. See also voting system.

Association: Voting.

Source: OH Statutes.

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.

Association: Voting.

Source: No attribution.

Voting Position: Specific response fields on a ballot where the voter indicates the selection of a candidate or ballot proposition.

Association: Voting.

Source: VSS, IEEE 1583.

Voting Process: Entire array of procedures, people, resources, equipment and locales by which elections are conducted.

Association: Voting.

Source: No attribution.

Voting Station: Location within the polling place where voters may record their votes. A voting station includes the voting booth or enclosure and the vote-recording device.

Association: Voting.

Source: VSS, IEEE 1583.

Voting System: Combination of mechanical, electromechanical, or electronic equipment and any corresponding documentation. It includes the software required to program, control, and support the equipment that is used to define ballots; to cast and count votes; to report and/or display election results; and to maintain and produce all audit trail information. A voting system may also include the transmission of results over telecommunication networks. It additionally includes the associated documentation used to operate the system, maintain the system, identify system components and their versions, test the system during its development and maintenance, maintain records of system errors and defects, and determine specific changes made after system qualification. See also electronic voting machine, voting equipment, voting machine.

Association: Voting.

Source: VSS.

Voting System Software: All the executable code and associated configuration files needed 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, etc. See also dynamic voting system software, semi-static voting system software, and static voting system software.

Association: Voting.

Source: No attribution.

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. This process occurs prior to EAC certification and subsequent State certification.
Association: Testing, voting.
Source: VSS.

Voting System Testing Laboratory (VSTL): Testing laboratory accredited by the National Voluntary Laboratory Accreditation Program for testing of voting systems. The Director of NIST submits a list of independent, non-Federal VSTLs to the EAC for accreditation.
Association: Testing.
Source: NIST HB 150–22.

VVPAT-Ballot Box: Ballot box containing the paper record.
Association: Security, voting.
Source: No attribution.

VVPAT-Display: Transparent covering over the paper record printed by the DRE-VVPAT. It permits a voter to inspect the paper record but prevents the voter from physically handling the paper record.
Association: Security, voting.
Source: No attribution.

VVPAT-Printer: Printing capability of the voting system, including the printer and any associated device involved in printing the paper records and transferring them to ballot boxes.
Association: Security, voting.
Source: No attribution.

W

Witness Device: Component of a voting system that captures voter verification of the records at the voting station. See also vote capture station.
Association: Voting.
Source: No attribution.

Write-in Voting: Means to cast a vote for an individual not listed on the ballot. 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 indicate their choice.
Association: Voting.
Source: VSS, IEEE 1583.

Workspace: See voting station.
Association: Voting.
Source: VSS.

A.2 Sources

Definitions in this Glossary are either extracted from or based on the following sources:

44 U.S.C. 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 Dict. 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 *electionline.org/*, (March 2005).

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.

FL Statutes Florida Statutes: Section 97.021(3) and Section 101.56062(1)(n) Standards for accessible voting.

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.

IL Statutes Illinois Public Act 093–0574.

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.

ME Statutes Maine LD 1759 Enacted 4/22/2004.

NASS National Association of Secretaries of State Election Reform Key Terms, *http://www.nass.org/Election%20Reform%20Key%20Terms.pdf* (February 2005).

NIST HB 143 NIST Handbook 143 State Weights and Measures Laboratories Program Handbook.

NIST HB 150 NIST Handbook 150:2001 NVLAP Procedures and General Requirements.

NIST HF Rpt. NIST Special Publication 500–256 Improving the Usability and Accessibility of Voting Systems and Products, May 2004.

NIST SP 800–30 NIST Special Publication 800–30 Risk Management Guide for Information Technology Systems, July 2002.

NIST SP 800–49 NIST Special Publication 800–49 Federal S/MIME V3 Client Profile, November 2002.

NIST SP 800–53 NIST Special Publication 800–53 Recommended Security Controls for Federal Information Systems, Appendix B, Glossary.

NIST SP 800–59 NIST Special Publication 800–59 Guideline for Identifying an Information System as a National Security System, August 2003.

NIST SP 800–63 NIST Special Publication 800–63 Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology, June 2004.

OH Statutes Ohio HB–262 enacted 5/7/2004.

OMB A130 OMB Circular A–130, Appendix III.

Section 508 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 Voting Systems Standards of 2002 (Federal Election Commission), Volumes I and II.

Whatis.com Whatis.com, IT Encyclopedia, *http://whatis.techtarget.com/definition/0,,sid9_gci491925,00.html* (*February* 2005).

WordNet WordNet ®2.0, © 2003 Princeton University.

A.3 List of Associations

Conformity Assessment
Human Factors (HF)

HF: accessibility
HF: usability
IT—Information Technology
Security
Software Engineering
Standardization
Testing
Typography
Voting

A.4 List of Deprecated Terms

The following terms are being phased out and replaced by newer terms. Note that there is a transition period where both terms are in use at the same time.

Deprecated term	Replaced by
Certification Testing	State Certification
Electronic Cast Vote Record.	Cast Vote Record
Qualification Number	no replacement at this time
Qualification Test Report.	Test Report for EAC Certification
Qualification Testing	Voting System Testing

Volume I, Appendix B

Table of Contents

B Appendix—Applicable Documents

B.1 Documents Incorporated in the Standards

The following publications have been incorporated into the Standards. When specific provisions from these publications have been incorporated, specific references are made in the body of the Standards.

Federal Regulations	Code of Federal Regulations, Title 20, 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 354–2001	Industry Usability Reporting and the Common Industry Format.
International Electrotechnical Commission (IEC)	IEC 61000–4–2 (1995–01)	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 Standards Development Documents

The following publications have been used for guidance in the revision of the Standards.

American National Standards Institute (ANSI)	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.
International Organization for Standardization (ISO).	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.
International Electro-technical Commission (IEC).	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 Mgmt. Guidelines for Configuration Management.
	ISO 10005–1995	Quality Mgmt. 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 Guidance Documents

The following publications contain information that is useful in understanding and complying with the Standards.

American National Standards Institute (ANSI) ...	ANSI/ISO/IEC TR 10176.1998	Information Technology Guidelines for the Preparation of Programming Language Standards.
	ANSI/ISO/IEC 6592.2000	Information Technology Guidelines for the Documentation of Computer Based Application Systems.
International Organization for Standardization (ISO).	ANSI/ISO/ASQC Q9000–3–1997	Quality management and quality assurance standards Part 3: Guidelines for the application of ANSI/IAO/ASQC Q9001–1994 to the Development, supply, installation and maintenance of computer software.
International Electro-technical Commission (IEC).	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 9594–8:2001	ITU–T Recommendation X.509 (2000), Information technology—Open Systems Interconnection—The Directory: Public-key and attribute certificate frameworks.
National Institute of Standards and Technology	FIPS 102	Guideline for Computer Security Certification and Accreditation.
	FIPS 112	Password Usage (3).
	FIPS 113	Computer Data Authentication.
Institute of Electrical and Electronics Engineers	488–1987	IEEE Standard Digital Interface for Programmable Instrumentation.
	796–1983	IEEE Standard Microcomputer System Bus IEEE/ANSI Software Engineering Standards.
	750.1–1995	IEEE Guide for Software Quality Assurance Planning.
	1008–1987	IEEE Standard for Software Unit Testing.
	1016–1998	IEEE Recommended Practice for Software Design Descriptions.
	1012–1998	IEEE Guide for Software Verification and Validation Plans.
Military Standards	MIL–HDBK–454	Standard General Requirements for Electronic Equipment.
	MIL–HDBK–470	Maintainability Program for Systems & Equipment.
	MIL–HDBK–781A	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. 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*.

Volume I, Appendix C

Table of Contents

Best Practices for Voting Officials

Many requirements for human factors and security (e.g., wireless communications, software distribution, and setup validation, voter verified paper audit trails) depend not only on voting systems providing specific capabilities but on voting officials developing and carrying out appropriate procedures. Consequently, the Voluntary Voting System Guidelines (VVSG) Version 1 provides guidance in the form of best practices for voting officials. These best practices provide adjuncts to the technical requirements for voting systems in order to ensure the integrity of the voting process and to assist States in properly setting up, deploying, and operating voting systems.

This appendix contains a list of best practices that have been extracted from the body of the VVSG Version 1. The section numbering and introductory text from the VVSG has been retained to provide the context for the best practice as well as to indicate from where it was extracted.

C.1 Best Practices for Human Factors

2.2.7 Human Factors

Human factors is concerned with the understanding of interactions among humans and other elements of a system. The importance of human factors in the design of voting systems has become increasingly apparent. It is not sufficient that the internal operation of these systems is correct; in addition, voters and poll workers must be able to use them effectively. The challenge, then, is to provide a voting system and voting environment that all voters can use comfortably, efficiently, and with justified confidence that they have cast their votes correctly.

2.2.7.1 Accessibility

The Help America Vote Act (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.''

Ideally every voter would be able to vote independently and privately.

Best Practices

- When the provision of accessibility involves an alternative format for ballot presentation, then all the other information presented to voters in the case of non-disabled English-literate voters (including instructions, warnings, messages, and ballot choices) is also presented in that alternative format.
- When the primary means of voter identification or authentication uses biometric measures that require a voter to possess particular biological characteristics, the voting process provides a secondary means that does not depend on those characteristics.
- Polling places are subject to the appropriate guidelines of the Americans with Disabilities Act (ADA) of 1990 and of the Architectural Barriers Act (ABA) of 1968.
- On all voting stations, the default color coding maximizes correct perception by voters and operators with color blindness.
- A sanitized headphone or handset is made available to each voter.
- If the normal procedure is for voters to submit their own ballots, then the voting process provides features that enable voters who are blind to perform this submission.
- The Acc-VS provides 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 is level with no slope exceeding 1:48 and positioned for a forward approach or a parallel approach.
- All controls, keys, audio jacks and any other part of the Acc-VS necessary for the voter to operate the voting system are within the reach regions as specified in the VVSG Volume I, Section 2.2.7.1.4.3.
- The Acc-VS incorporates the features listed in the VVSG Volume I, Section 2.2.7.1.2.2.3 (audio presentation) to provide accessibility to voters with hearing disabilities.
- The voting process is made accessible to voters with cognitive disabilities.

2.2.7.2 Limited English Proficiency

HAVA Section 301(a)(4) reads in part: ''Alternative language accessibility—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.

Best Practices

• Regardless of the language, candidate names are displayed or pronounced in English on all ballots. For written languages that do not use Roman characters (e.g. Chinese, Japanese, Korean, Arabic), the ballot includes transliteration of candidate names into the relevant language.

2.2.7.3 Usability

HAVA Section 301 begins by addressing the interaction between the voter and the voting system. In addition to these mandates, HAVA Sections 243 and 221(e)(2)(D) address support for improved usability. 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 users are the voters (but also poll workers), the product is the voting system, and the task is the correct representation of one's choices in the election.

Best Practices

• The voting station does not visually present a single race spread over two pages or two columns.
• The ballot clearly indicates the maximum number of candidates for which one can vote within a single race.
• The ballot presents the relationship between the name of a candidate and the mechanism used to vote for that candidate in a consistent manner.

2.2.7.4 Privacy

Voter privacy is strongly supported by HAVA—Sections 221(e)(2)(C) and 301(a)(1). Privacy in the voting context, including the property of the voter being unable to disclose his or her vote, ensures that the voter can make choices 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 to another how he or she voted.

Note that these best practices address privacy concerns in relation to human factors issues and not with respect to the processing of cast ballots.

Best Practices

• The ballot and any input controls are visible only to the voter during the voting session and ballot submission. Poll workers need to take into account such factors as visual barriers, windows, permitted waiting areas for other voters, and procedures for ballot submission when not performed at the voting station, e.g. submission of optiscan ballots to a central reader.
• The audio interface is audible only to the voter.
• As mandated by HAVA 301(a)(1)(C), the voting system notifies the voter of an attempted overvote in a way that preserves the privacy of the voter and the confidentiality of the ballot.
• Appropriate procedures are needed to ensure that absentee balloting enable the voter to preserve privacy. There is no practical means to prevent a voter from revealing an absentee paper ballot to others. But the procedures should ensure that if a voter chooses to maintain privacy, it is not violated at a later stage, in particular when the ballot is received by voting officials.

C.2 Best Practices for Security

VVSG Version 1 addresses four new aspects of voting systems security. The first, independent dual verification is informative and provide characteristics of these systems. It does not yet contain any best practices. There are best practices for the other three sections: Voter Verified Paper Audit Trails, Wireless Requirements, and Software Distribution and Setup Validation.

6.0.2 Requirements for Voter Verified Paper Audit Trails

VVSG Version 1 provides requirements for voter verified paper audit trails (VVPAT) so that States that choose to implement VVPAT or States that are considering implementation can utilize these requirements to help ensure the effective operation of these systems.

6.0.2.4 Approve or Spoil the Paper Record

Best Practices

• Appropriate procedures are needed for reconciling the number of spoiled paper records with the number of spoiled electronic records and for addressing any discrepancies after the close of polls.
• Appropriate procedures are needed to permit the voter to cast a ballot if the maximum number of spoiled ballots occurs.
• Appropriate procedures are needed to address situations in which a voter is unable to review the paper record.
• Appropriate procedures are needed to address situations in which a voter indicates that the electronic and paper records do not match. If the records do not match, a potentially serious error has occurred. Election officials should first verify that the records do not match and then take appropriate actions such as removing the voting station from service and quarantining its records for later analysis.

6.0.2.5 Preserve Voter Privacy and Anonymity

Best Practices

• Appropriate procedures are needed to ensure the privacy and anonymity of voters whose paper records contain any of the alternative languages chosen for making ballot selections.
• Appropriate procedures are needed to prevent voters from leaving the voting area with a paper record that can directly reveal the voter's choices.

6.0.2.7 Equipment Security, Reliability, and Maintainability

Best Practices

• Appropriate procedures are needed to ensure that voting systems are physically secured from tampering and intentional damage.

6.0.3 Wireless Requirements

Wireless is defined as any means of communication that occurs without wires. This includes radio frequency (RF), infrared, (IR) and microwave. The use of wireless technology within a voting system introduces risk and should be approached with caution. Wireless communication is susceptible to disruption, eavesdropping, and interference from other wireless signals. The combination of technical features and functionality built into the voting system along with procedural practices in using and handling the voting system can mitigate the risks of using wireless communications.

6.0.3.2 Controlling Usage

Best Practices

• When using encryption to ensure that the wireless communication is secure, appropriate procedures are needed for cryptographic key management.

6.0.3.6 Protecting the Voting System From a Wireless-Based Attack

Best Practices

• Appropriate procedures are needed to ensure that wireless communication actions are logged and capture at least the following information: times wireless is activated and deactivated, services accessed, identification of device to which data was transmitted to or received from, identification of authorized user, successful and unsuccessful attempts to access wireless communications or service.

6.0.4 Distribution of Voting System Software and Setup Validation

The goal of 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 qualified software and the absence of other software, is to ensure that voting system equipments is in a proper initial state before being used.

6.0.4.1 Software Distribution Methodology Requirements

Best Practices

- Voting software used to install the qualified voting systems can be obtained on write-once media from the voting system vendor or an EAC accredited test authority.
- The reference information produced by the NSRL or other EAC designated repository can be used to verify that the correct software has been received.

6.0.4.2 Generation and Distribution Requirements for Reference Information

Best Practices

- To ensure that the write-once media contains the correct information, a digital signature can be used. The digital signature can replace secure storage of reference information since the digital signature can be used to verify that the reference information media has not been modified or corrupted.
- The vendor's documented values can be used to verify that all voting systems' static and initial register and variable values are correct prior to an election.
- The reference information can be used to verify that voting system software is the correct version of the software prior to an election.
- If differences between the reference information and voting system software are found, then appropriate procedures are needed to handle and resolve these anomalies.

Volume I, Appendix D

Table of Contents

Appendix D

Appendix D is an informative section with characteristics of independent dual verification systems followed by characteristics of the types of independent dual verification systems which will be used as the basis for future requirements. They are preliminary and will be evolving with further research.

D.1. Independent Dual 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 choices whose handling requirements are reasonable. To meet this objective, there are many factors to consider in an electronic voting system's design, including:

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

Independent Dual Verification (IDV) systems have as their primary objective the production of ballot records that are capable of being used in audits in which their correctness can be audited to very high levels of precision. The primary security issues addressed by IDV systems are:

- Whether electronic voting systems are accurately recording ballot choices, and
- Whether the ballot record contents can be audited precisely post-election.

The threats addressed by IDV systems are those that could cause a voting system to inaccurately record the voter's intent or cause a voting system's records to become damaged, i.e., inserted, deleted, or changed. These threats could occur via any number of means including accidental damage or various forms of fraud. 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.

1.1 Independent Dual Verification Systems: Improved Accuracy in Audits

Independent Verification is the top-level categorization for electronic voting systems that produce multiple records of ballot choices whose contents are capable of being audited to high levels 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 the voter's choices 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 the voter's choices and then copies it to some write-once media.
- The voter must be able to verify that both records are correct, e.g., verify his or her choices on the voting system's display and also verify the second record of choices stored on the write-once media.
- The verification processes for the two verifications 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 different systems produced by different vendors.
- 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 by using an electronic voting system, 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 above, 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 up on 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.

1.2 Example Independent Dual Verification Systems

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

- Voting systems with a split process architecture,[1]
- End-to-end voting systems that include cryptographic audit schemes,
- Witness voting systems that take a picture of or otherwise capture an indirect verification of ballot choices, and
- Direct independent verification, including some types of voting systems that produce an optically scanned ballot or that produce a voter-verified paper audit trail (VVPAT).

1.2.1 The Split Process Architecture for IDV 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 some write-once read-only 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:

1. A voter is given a token object that has been initialized to be blank.
2. Supporting information is written to the token object including the ballot and identification information about the election and precinct.

[1] 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 available for download at *http://www.vote.caltech.edu/*.

3. 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 on an input device such as a touch screen. The voter to makes his or her ballot choices, which causes a record of the vote to be recorded on the token object.

4. 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.

5. The voter verifies that the information is correct and then deposits the token object into a container where 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's records. Typically, the electronic records recorded by the verification station would be counted in the election. At least one of the sets of records should be different in form from the other set of records and be resistance to accidental or deliberate damage so that it can remain useful for audits and recounts.

In theory, the physical separation of the ballot capture from the ballot 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 choices.

The verification station's software is considered to be the ''trusted computing base'' of the voting system, because it must be trusted in the verification process and then trusted to store the record for counting, i.e, cast the voter's ballot. The software to implement this capability should be relatively small and thus easier to inspect and test.

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.

1.2.2 End to End (Cryptographic) IDV Systems

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

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

1. A voter uses a voting station such as a DRE to make ballot choices.

2. 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 choices.

3. The voter may have the option to check that his or her ballot choices were included in the election count, e.g., by checking a Web site of values 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 choices 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.

1.2.3 Witness IDV Systems

A witness voting 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:

1. A voter makes ballot choices at the DRE and then presses a button to record his or her vote.

2. The DRE records the ballot choices and uses them in the election count.

3. At the time the button is pressed, the camera takes a picture of the DRE's screen and saves the image (the voter is not included in the picture).

4. 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 choices 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's 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.

1.2.4 Direct IDV Systems

Direct independent dual verification systems produce a record for voter verification that the voter may verify directly with the voter's senses and which is then preserved for auditing or counting. Some optical scan voting system approaches fit into this category (albeit loosely), as well as those systems with VVPAT (Voter Verified Paper Audit Trail) capability.

Some optical scan voting system approaches fit into this category (albeit loosely), as well as those systems with VVPAT (Voter Verified Paper Audit Trail) capability.

The optical scan voting systems approaches 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:

1. A voter uses a marking device such as a DRE to mark a ballot and then presses a button to print the marked ballot onto a piece of paper.

2. The voter directly reviews the paper to ensure its correctness, and if correct, places the paper record into a scanner (some procedure would need to be included to handle spoiled ballots).

3. 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 barcoded representation of the human readable portion of the ballot.

4. The paper record gets preserved in a ballot box.

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.

An electronic voting system with VVPAT (Voter Verified Paper Audit Trail) 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 audit trail of the voter's choices. Like the optical scan system, it creates two distinct representations of the voter's ballot choices: an electronic record and a paper record.

Typically, a voter would use the voting system (called a DRE–VVPAT) as follows:

1. A voter makes ballot selections and indicates that his or her selections are complete.

2. The VVPAT–DRE prints a paper record summary of the voter's ballot choices. An alternative approach to VVPAT involves printing the voter's ballot selections as they are made, e.g., a concurrent or contemporaneous record.

3. The voter inspects and directly verifies that the paper record matches the displayed electronic record (again, a procedure would need to be included to handle spoiled ballots).

4. The paper record gets preserved in a ballot box.

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

1.3 Issues in Handling Multiple Records Produced by Independent Dual Verification Systems

There are several fundamental questions that need to be addressed when designing the structure and selecting the physical characteristics of IDV systems 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, and

• 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.

As a consequence, 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, such as the following:

• 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 using public key cryptography,

• 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, and

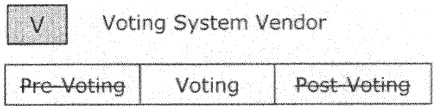
• Structuring the records in open, publicly documented formats that can be readily analyzed on different computing platforms

The ease or relative difficulty with which some types of records must be handled is also a determining factor in the practical capability to conduct precise audits, given that some types of records are better suited to different types of 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 voters or poll workers and thus be more susceptible to damage or loss. 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.

D.2. Core Characteristics for Independent Verification Systems

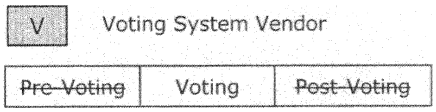
This section contains a preliminary set of characteristics for IDV systems. These characteristics are fundamental in nature and apply to all categories of IDV systems. They will form the basis for future requirements for independent verification systems.

2.1 An Independent Dual Verification Voting System Produces Two Distinct Sets of Records of Ballot Choices Via Interactions With the Voter Such That One Set of Records Can Be Compared Against the Other To Check Their Equality of Content



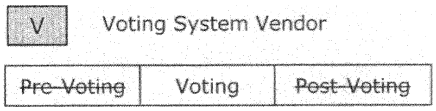
Discussion: This is the fundamental core definition for IDV systems. The records can be checked against one another to determine whether or not the voter's choices were correctly recorded.

2.1.1 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



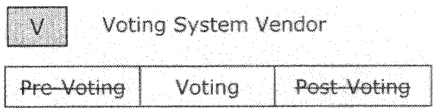
Discussion: Direct Verification involves using human senses, e.g., directly verifying a paper record via one's eyesight. Indirect Verification involves using an intermediary to perform the verification, e.g., verifying an electronic ballot image at the voting system.

2.1.2 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



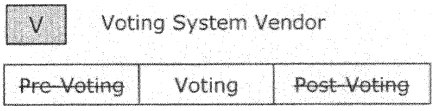
Discussion: The records must be stored on different media and handled independently of each other, so that no one process could compromise all records. If an attack can alter one record, it should still be very difficult to alter the other record.

2.1.2.1 At Least One Record Is Highly Resistant to Damage or Alteration and Should Be Capable of Long-Term Storage



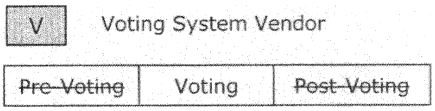
Discussion: At least one of the records should be difficult to alter or damage so that it could be used in case the counted records are damaged or lost.

2.1.3 The Processes of Verification for the Multiple Records Do Not All Depend for Their Integrity on the Same Device, Software Module, or System, and Are Sufficiently Separate Such That Each Record Provides Evidence of the Voter's Choices Independently of Its Other Corresponding Record



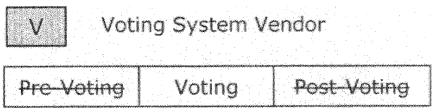
Discussion: For example, the verification of an electronic record on a DRE is not sufficiently separate from the verification of an electronic record located on a token but performed by the same DRE as the verification for the first record. Verification of a paper record by one's senses is sufficiently separate in this case.

2.1.4 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



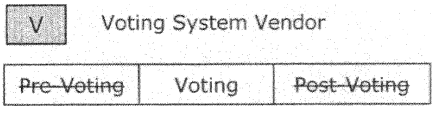
Discussion: For example, an electronic record can be used in an efficient counting process. A second paper record can be used to verify the accuracy of the electronic record; however its suitability for efficient counting is less clear. If a paper record can be used in an automated scan process, it may be more suitable.

2.1.5 The Records Within a Set Are Linked to Their Corresponding Records in the Other Set By Including a Unique Identifier Within Each Record That Can Be Used to Identify the Record's Corresponding Record in the Other Set



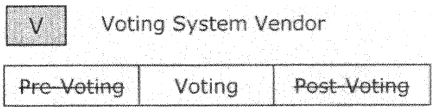
Discussion: The identifier should serve the purpose of uniquely identify the record so as to identify duplicates and/or for cross-checking two record types.

2.1.6 Each Record Includes an Identification of the Voting Site/Precinct

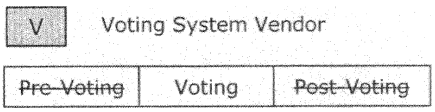


Discussion: If the voting site and precinct are different, both should be included.

2.1.7 The Records Include Information Identifying Whether the Balloting Is Provisional, Early, or on Election Day, and Information That Identifies the Ballot Style in Use

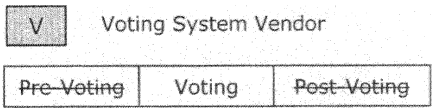


2.1.8 The Records Include a Voting Session Identifier That Is Generated When the Voting Station Is Placed in Voting Mode and That Can Be Used To Identify the Records as Being Created During That Voting Session



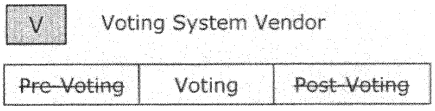
Discussion: If there are several voting sessions on the same voting station on the same day, the voting session identifiers must be different. They should be generated from a random number generator.

2.1.9 The Records Include an Identifier of the Voting System That Is Unique to That Style of Voting Systems



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

2.1.10 The Cryptographic Software in Independent Verification Voting Systems Is Approved by the U.S. Government's Cryptographic Module Validation Program (CMVP) as Applicable



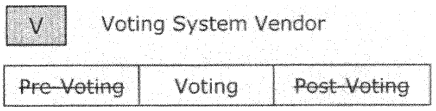
Discussion: The voting systems may use cryptographic software for a number of different purposes, including calculating checksums, encrypting records, authentication, generating random numbers, and for digital signatures. This software should be reviewed and approved by the Cryptographic Module Validation Program. 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*.

D.3. Split Process IDV Systems

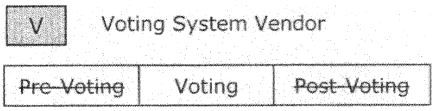
This section contains characteristics specific to split process IDV systems. The characteristics build on and are in addition to the core characteristics for IDV systems. Split process systems consist of separate vote capture and verification stations, i.e., two physical devices. A voter inserts an object 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.

3.1 Capture and Verification Stations

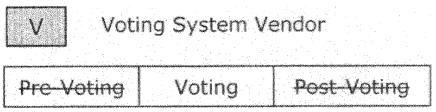
3.1.1 The Verification Station Is Able To Add Information to the Token Object But Cannot Change Prior Recorded Information



3.1.2 The Capture and Verification Stations Do Not Permit any Communications Between Them Except Via the Token Object

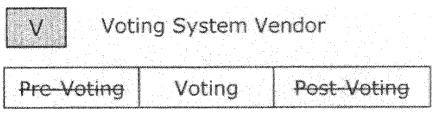


3.1.3 The Verification Station Log All Rejected Votes, Including the Precise Contents of the Votes and the Identifier of the Token Object



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

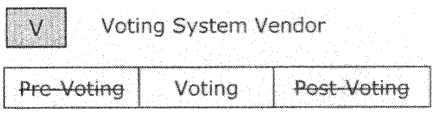
3.1.4 The Capture and Verification Stations Could Be Purchased From Different Manufacturers and Could Use Different Operating Systems



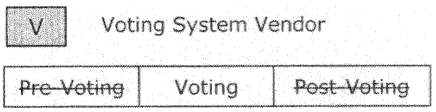
Discussion: The greater the diversity between the systems, the less likely they could be compromised by the same threats, e.g., software viruses, or by a single conspiracy.

3.2 Data Formats for Token Objects

3.2.1 The Format for Data Written to the Token Object Is Specified and Publicly Available for Use Without Licensing Fees

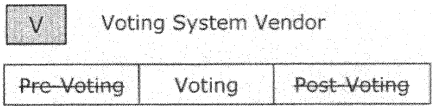


3.2.2 The Verification Station Verifies the Correctness of the Data on the Token Object and Provides an Indication of any Errors to the Voter

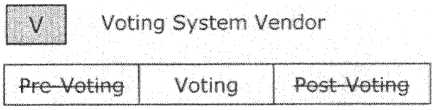


Discussion: The verification station needs to verify, in essence, that the data written to the token object was formatted properly according to the rules of the format's specification and reject ill-formatted data. It also checks that the votes are consistent with the voting instructions, e.g., ''vote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

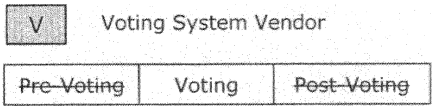
3.2.3 The Record on the Token Object Is Digitally Signed Using a Private Key Known Only to the Vote Capture Station and Whose Public Key Is Distributed in an Authenticated Way To Auditing Systems



3.2.4 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

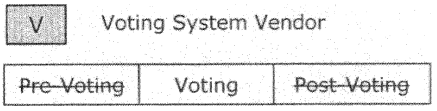


3.2.5 The Capture Station Associates With Each Record of Voter Choices a Unique Identifier That Is Capable of Being Used To Identify the Record Uniquely and To Identify Its Corresponding Record Created by the Verification Station

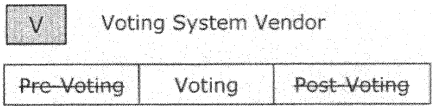


Discussion: The identifier serves the purpose of uniquely identifying the record to identify duplicates and/or for cross-checking two record types.

3.2.6 The Records From the Verification Station Are Randomly Shuffled in Memory and When Exported, so That the Order of the Records Cannot Be Used To Identify Any Voter

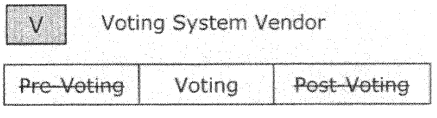


3.2.7 Rejected Token Objects Are Stored Separately From Accepted Memory Devices for Later Auditing



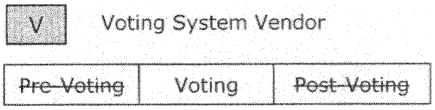
3.3 Storage and Communications of Records

3.3.1 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

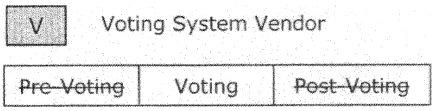


Discussion: This is necessary to determine if records are missing or substituted.

3.3.2 The Token Objects Are Carried in a Physically Secure Way, Using Chain-of-Custody Mechanisms To Ensure Their Integrity



3.3.3 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

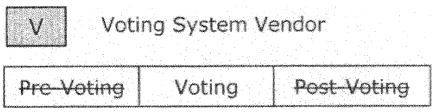


D.4. Witness IDV Systems

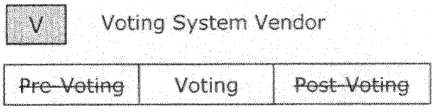
This section contains preliminary characteristics for Witness IDV systems. They are consistent with the definition of IDV systems from Section 6.0 and build on the core characteristics for IDV systems.

Witness IDV systems are composed of two physically separate devices: the vote capture station that captures and stores records of voters' choices, 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 (with or without VVPAT capability), a number of the definitions for VVPAT that are specific to DRE systems 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 in the device be made immediately obvious to voters and poll workers.

4.1 A Witness Device Records Only a Voter's Verification at a Voting Station and Stores the Record so That It Can Be Used for Audit and Recounts as Applicable

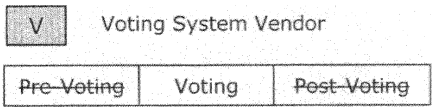


4.2 A Witness Device Acts as a Passive Device That Cannot Perform any Operation With Respect to the Voting Station Other Than To Capture the Voter's Ballot Choices as the Voter Verifies Them



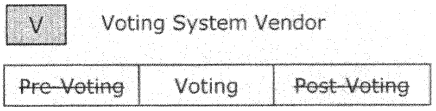
Discussion: The witness device is synchronized with the voter verification of the ballot choices.

4.3 A Witness Device, if Attached to the Voting Station, Is Attached Such That it Can Capture Only the Voter's Verification of Ballot Choices



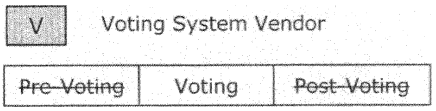
Discussion: For example, the witness device could be connected only to the display unit and not the vote capture station's memory or disk drive.

4.4 The Voting Station Is Not Able To Detect in Its Function Whether a Witness Device Is Electrically Connected or in Operation



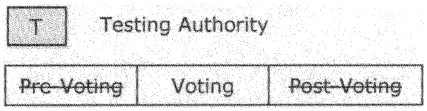
Discussion: If the witness device is connected to or attached electrically to the vote capture station, the capture station is not able to determine or be aware in its function that a witness device is attached.

4.5 The Witness Device Operates Properly With Most if Not All Electronic Voting Systems Functioning as Voting Stations

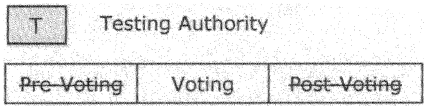


Discussion: This is desirable but may require some degree of openness in witness device specifications to enable the desired compatibility.

4.6 The Witness Device Is Not Designed or Built or Manufactured by the Same Manufacturer of the Voting Station to Which it Is Attached

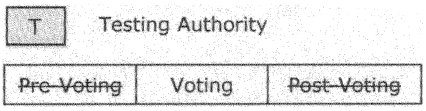


4.7 Because Voters Must Trust That the Witness Device Records Their Verifications Accurately, Assessments of Its Software and Functionality Are Straightforward, Readily Performed, and Include Extensive Evaluation and Penetration Testing Above and Beyond What May Be Performed on Voting Systems That Do Not Contain Witness Devices

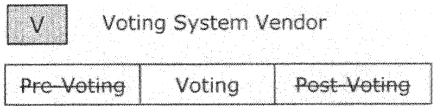


Discussion: Witness device manufacturers will need to document their systems extensively and subject them to highly stringent testing.

4.8 Because Voters Must Trust That the Witness Device Records Their Verifications Accurately, the Results of Witness System Assessments Are Made Publicly Available

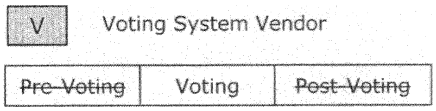


4.9 A Voter Should Be Able To Inspect the Record of the Voter's Verification Upon the Voter's Request



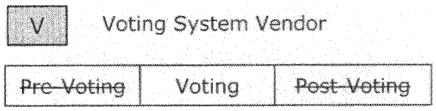
Discussion: It is desirable that a voter have some capability to verify that the witness device is operating as specified.

4.10 The Witness Device Clearly Indicates Any Malfunction in a Way That Is Obvious to Poll Workers and Voters

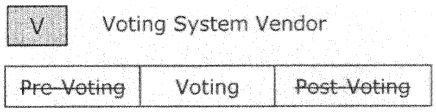


Discussion: This serves to ensure that voting cannot continue if the witness device is not operating or is malfunctioning.

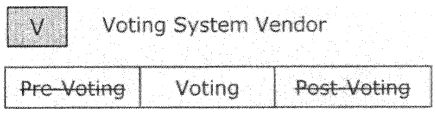
4.11 The Records Captured by the Witness Device Are Able To Be Used in Highly Accurate Verifications of the Voting Records of the Voting Station



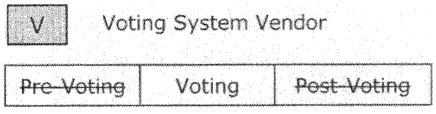
4.12 The Records Contain Unique Identifiers That Correspond to Records Stored by the Voting Station



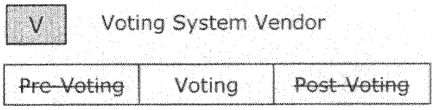
4.13 The Records Are Digitally Signed by the Witness Device so That the Integrity and Authenticity of Its Records Can Be Verified



4.14 A Witness Device Is Able To Export Its Records in an Open, Nonproprietary Format Such That the Records Can Be Used in Automated Audits



4.15 The Records Are Stored in the Witness Device and Exported Such That Voter Privacy Is Protected, e.g., by Making the Order of the Records Randomly Determined



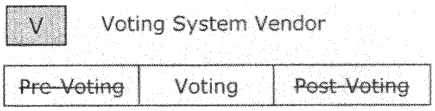
D.5. End to End (Cryptographic) IDV Systems

This section contains very preliminary definitions for End to End (or cryptographic-based) IDV systems. They are consistent with the characteristics of IDV systems and build on the core characteristics of IDV systems.

End to end voting systems use cryptographic mechanisms as a substitute for some of the physical, computer-security, or procedural mechanisms used to secure other voting systems. 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.

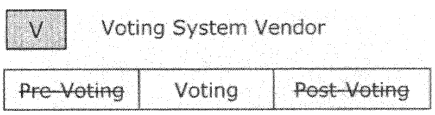
End to end systems use cryptographic mechanisms as a substitute for some of the physical, computer security, and procedural mechanisms used to secure voting systems. These cryptographic mechanisms can be used by a voter to verify that ballot choices were recorded correctly and counted in the election.

5.1 End to End Systems Use Cryptographic Mechanisms as a Substitute for Some of the Physical, Computer Security, and Procedural Mechanisms Used To Secure Voting Systems. These Cryptographic Mechanisms Can Be Used by a Voter To Verify That Ballot Choices Were Recorded Correctly and Counted in the Election



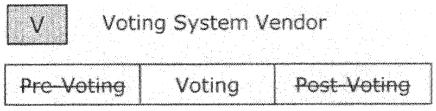
Discussion: There are potentially many types of end to end systems that could perform a variety of different functions.

5.2 End to End Systems Record Voters Ballot Choices at an Electronic Voting System and Encrypt the Records of Votes for Later Counting by Designated Trustees



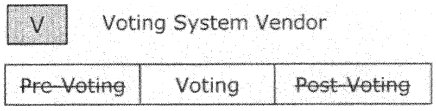
Discussion: The voting station would operate much as a DRE.

5.3 End to End Systems Produce a Receipt That Can Be Used by the Voter in Some Process Made Available by Voting Officials That Would Enable the Voter to Verify That the Voter's Ballot Choices Were Recorded Correctly and Counted in the Election



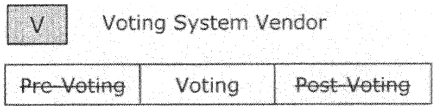
Discussion: The receipt could have a variety of different forms but likely would be printed on paper for the voter's ease of handling.

5.4 No One Designated Trustee Is Able to Decrypt the Records; Decryption of the Records Is Performed by a Process That Involves Multiple Designated Trustees

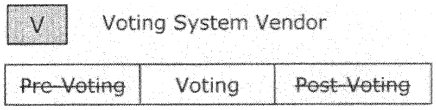


Discussion: For example, multiple keys could be combined to decrypt the records.

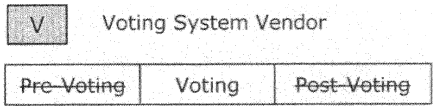
5.5 The Receipt Preserves Voter Privacy by Not Containing any Information That Can Be Used To Show the Voter's Choices



5.6 The Process Used To Verify That Ballot Choices Were Recorded Correctly or Counted in the Election Preserves Voter Privacy by not Revealing any Information That Can Be Used to Show the Voter's Choices

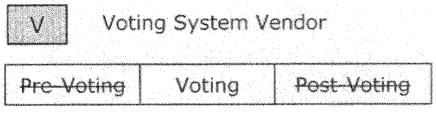


5.7 End to End Systems Store Backup Records of Voter's Ballot Choices That Can Be Used in Contingencies Such as Damage to or Loss of Its Counted Records

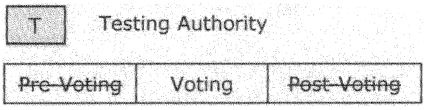


Discussion: This is necessary because the handling of the encrypted records requires the same chain of custody procedures as records produced by other voting systems and are thus subject to loss or damage. This could be paper for example.

5.8 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

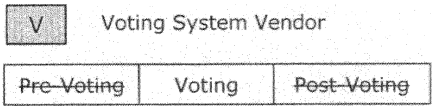


5.9 Cryptographic Software in End to End Systems Is Documented Thoroughly and Subject To Extensive Verification Testing for Correctness. The Documentation Includes Extensive Discussion of How Cryptographic Keys Are To Be Generated, Distributed, Managed, Used, Certified, and Destroyed

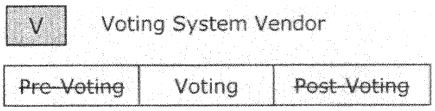


Discussion: The correctness of the system depends on the correctness of the cryptographic algorithms and their implementations. Thus, rigorous testing is necessary.

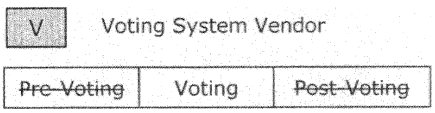
5.10 Vote Capture Stations Used in End to End Systems Meet All Security, Usability, and Accessibility Requirements for Similar Stations in Other Voting Systems



5.11 Reliability, Usability, and Accessibility Requirements for Printers in Other Voting Systems Apply As Well to Receipt Printers Used in End to End Systems

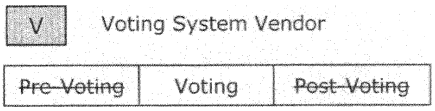


5.12 Trustee Systems Are Subject to the Same Evaluations and Assessments as Other Voting Systems



Discussion: Trustee systems include systems to perform cryptographic functions such as encrypting or decrypting votes.

5.13 Systems for Verifying That Voters' Ballots Were Recorded Properly and Counted in the Election 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.

Volume II, Section 1

Table of Contents

1.1 Objectives and Usage of Volume II of the Voting Systems Standards

Volume II, Voting System Qualification Testing Standards, is a complementary document to Volume I, Voting System Performance Standards. While Section 9 of Volume I provides an overview of the qualification testing process performed by the Independent Test Authorities (ITAs), Volume II provides specific detail about the process that is necessary for ITAs, vendors, and election officials participating in the qualification process. The Standards envision a diverse set of users for Volume II, including:

- Vendors: Voting system vendors will use Volume II to guide the design, construction, documentation, internal testing, and maintenance of voting systems to ensure conformance with the Standards. Vendors will also use Volume II to help define the obligations of organizations that support the vendor's system, such as suppliers, testers, and consultants.
- Independent Testing Authorities: Testing authorities certified to qualify systems will use Volume II to guide the testing of voting systems and preparation of test reports. Laboratories and other parties interested in becoming ITAs can use Volume II to understand the requirements and obligations placed on the ITAs involved in the process.
- Election officials: Voting officials in many jurisdictions will use Volume II to guide system certification, procurement and acceptance requirements and processes, which may include additional requirements and adjustments to those requirements included in the Standards.

1.2 General Contents of Volume II

To support these primary users of the Standards, Volume II provides:

a. A discussion of the general sequencing of tests performed by the ITAs: Volume II identifies the tests where sequencing is important and provides such required sequences. Volume II also indicates other tests that may be conducted in parallel.

b. A detailed description of the information required to be submitted by voting system vendors in the Technical Data Package (TDP): The TDP is a comprehensive set of documents that describe system design specifications, operating procedures, system testing information, facility and resource requirements for system operations, system maintenance instructions for jurisdictions, and vendor practices for quality assurance and configuration management that underlie the development and update of the system. The TDP focuses predominantly on the required documentation contents, providing flexibility to vendors to determine the best format for meeting the content requirements.

c. Delineation of specific system tests to be conducted by the ITAs: Volume II identifies specific tests that are to be conducted relating to system components and to the integrated system as a whole. Tests are defined for system functionality, hardware, software, telecommunications, and security that address the performance standards delineated in Volume I.

d. Delineation of specific examinations of other information provided by the vendor: Volume II identifies the criteria to be used by the ITAs in conducting examinations of the information submitted in the TDP. These criteria address the documentation provided in the TDP, including documentation of the system and related operational procedures as well as vendor practices for quality assurance and configuration management.

e. Description of process for handling failures: A system may fail to pass one or more of the tests and examinations performed by the ITAs. Volume II describes the practices to be used by the ITAs when the system or its documentation fails a test or examination, including the nature and depth of re-testing required for corrections submitted by the vendor.

f. Outline of Qualification Test Report. Volume II provides an outline of the report issued by the ITAs at the conclusion of testing, providing the specific requirements for this report.

1.3 Qualification Testing Focus

Qualification tests focus on multiple aspects of the voting system and the process for development and maintenance. Although multiple ITAs may conduct qualification testing, with each ITA conducting tests in its areas of expertise, the focus of their combined activities remains the same. Overall, qualification testing focuses on:

a. The functional capabilities of the system to support specific election activities performed by system users, including election officials and voters, as defined in Volume I, Section 2 of the Standards;

b. The performance capabilities of the system that ensure accuracy, integrity, and reliability of system operations and the election activities that rely on them, as defined in Volume I, Sections 3, 4, 5 and 6 of the Standards;

c. The system development and maintenance processes and related quality assurance activities performed by the vendor to ensure system quality, as addressed in Volume I, Section 7 of the Standards;

d. The configuration management activities used to control the development and modification of the system and its individual components, and maintain accurate information about the version and status of the system and its components throughout the system life cycle, as addressed in Volume I, Section 8 of the Standards; and

e. The documentation developed and maintained by the vendor to support system development, testing, installation, maintenance and operation, as addressed by the TDP described in Volume II, Section 2.

1.4 Qualification Testing Sequence

The overall qualification test process progresses through several stages involving pre-testing, testing, and post-testing activities as described in Volume I, Section 9 of the Standards. Whereas Volume I describes the flow of the overall process, Volume II focuses on the details of activities conducted by the ITA and activities conducted by the vendor to facilitate testing and respond to errors, anomalies, and other findings of concern during the test process.

Qualification testing involves a series of physical tests and other examinations that are conducted in a particular sequence. This sequence is intended to maximize overall testing effectiveness, as well as conduct testing in as efficient a manner as possible. The ITA follows the general sequence of activities indicated below. Note that test errors and anomalies are communicated to the vendor throughout the process.

a. Initial examination of the system and TDP 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. Development of a detailed system test plan that reflects the scope and complexity of the system, and the status of system qualification (i.e., initial qualification or re-qualification);

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

d. Functional and performance testing of hardware components;

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

f. Code review for selected software components;

g. Functional and performance testing of software components;

h. System installation testing and testing of related documentation for system installation and diagnostic testing;

i. 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;

j. Examination of the System Maintenance Manual;

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

l. Preparation of the Qualification Test Report.

1.5 Evolution of Testing

The ITA will conduct extensive tests on a voting system to evaluate it against the requirements of the Standards. Taking advantage of the experience gained in examining other voting systems, ITAs will design tests specifically for the system design, configuration, and documentation provided by the vendor. Additionally, new threats may be identified that are not directly addressed by the Standards or the system. As new threats to a voting system are discovered, either during the system's operation or during the operation of other computer-based systems that use technologies comparable to those of another voting system, ITAs shall expand the tests used for system security to address the threats that are applicable to a particular design of voting system.

1.6 Outline of Contents

Volume II of the Voting Systems Standards is organized as follows:

- Section 2 describes the requirements for the Technical Data Package;
- Section 3 describes functionality testing;
- Sections 4 and 5 describe specific testing standards for hardware and software;
- Section 6 describes standards for testing the fully integrated system, including telecommunications and security capabilities, and the documentation used to operate the system;
- Section 7 describes the standards for examining the documentation of vendor practices for quality assurance and configuration management;
- Appendix A provides an outline for the Qualification Test Plan;
- Appendix B provides an outline for the Qualification Test Report; and
- Appendix C describes the guiding principles used to design the voting system qualification testing process performed by ITAs.

Volume II, Section 2

Table of Contents

2 Technical Data Package

2.1 Scope

This section contains a description of vendor documentation relating to the voting system that shall be submitted with the system as a precondition of qualification 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. Other items relevant to the system evaluation shall be submitted along with this documentation (such as disks, tapes, 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 outlining system development permits assessment of the vendor's systematic efforts to test the system and correct defects. Inspection of this process also enables the design of a more precise qualification test plan. If the vendor's developmental test data is incomplete, the test agency shall design and conduct the appropriate tests.

2.1.1 Content and Format

The content of the Technical Data Package (TDP) is intended to collect 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; and
- Vendor practices for managing the configuration of the system during development and for modifications to the system throughout its life cycle.

The vendor shall list all documents 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 Qualification

At minimum, the TDP shall contain the following documentation:

a. System configuration overview;
b. System functionality description;
c. System hardware specifications;
d. Software design and specifications;
e. System test and verification specifications;
f. System security specifications;
g. User/system operations procedures;
h. System maintenance procedures;
i. Personnel deployment and training requirements;
j. Configuration management plan;
k. Quality assurance program; and
l. System change notes.

2.1.1.2 Required Content for System Changes and Re-qualification

For systems seeking re-qualification, vendors shall submit System Change Notes as described in section 2.13, as well as current versions of all documents that have been updated to reflect system changes.

Systems in existence at the time the revised standards are released may not

have all required developmental documentation. When such a system is subject to evaluation as a result of system modification, the vendor shall provide what information they can.

Vendors may also submit other information relevant to the evaluation of the system, such as documentation of tests performed by other independent test authorities and records of the system's performance history, if any.

2.1.1.3 Format

The requirements for formatting the TDP are general in nature; specific format details are of the vendor's choosing. Other items submitted by the vendor, such as documentation of tests conducted by other test authorities, performance history, failure analysis, and corrective action may be provided in a format 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 using the vendor's format.

2.1.2 Other Uses for Documentation

Although all of the TDP documentation is required for qualification 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 test agency 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 test authority 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. 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 interconnection);

b. A description of the operational environment of the system that provides an overview of the hardware, software, and communications structure;

c. A theory of operation that explains each system function, and how the function is achieved in the design;

d. Descriptions of the functional and physical interfaces between subsystems and components;

e. 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:

(1) Operating systems;

(2) Database software;

(3) Communications routers;

(4) Modem drivers; and

(5) Dial-up networking software;

f. 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:

(1) File specifications, data objects, or other means used for information exchange; and

(2) The public standard used for such file specifications, data objects, or other means; and

g. Benchmark directory listings for all software (including firmware elements) and associated documentation included in the vendor's release in order of how each piece of software would normally be installed upon setup and installation.

2.2.2 System Performance

The vendor shall provide system performance information that includes descriptions of:

a. 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;

b. Quality attributes such as reliability, maintainability, availability, usability, and portability;

c. Provisions for safety, security, privacy, and continuity of operation; and

d. 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 Standards 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 as indicated by the standards for that documentation.

a. 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 of the Standards. The contents of Volume I Section 2 may be used as the basis for a checklist whereby the vendor indicates the specific functions provided and those not provided by the system;

b. 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;

c. Required capabilities that may be bypassed or deactivated during installation or operation by the user shall be clearly indicated;

d. Additional capabilities that function only when activated during installation or operation by the user shall be clearly indicated; and

e. 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, Sections 3, 4, 5 and 6 of the Standards, including:

a. 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;

b. 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;

c. Reliability: This discussion addresses system and component reliability stated in terms of the systems operating functions, and identification of items that require special handling or operation to sustain system reliability;

d. 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; and

e. 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 qualification 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:

a. Materials, processes, and parts used in the system, their assembly, and the configuration control measures to ensure compliance with the system specification;

b. The electromagnetic environment generated by the system;

c. Operator and voter safety considerations, and any constraints on system operations or the use environment;

d. Human engineering 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. A description of the software system concept, including specific software design objectives, and the logic structure and algorithms used to accomplish these objectives;

b. The general design, operational considerations, and constraints influencing the design of the software;

c. Identification of all software items, indicating items that were:

(1) Written in-house;

(2) Procured and not modified; and

(3) Procured and modified including descriptions of the modifications to the software and to the default configuration options;

d. Additional information for each item that includes:

(1) Item identification;

(2) General description;

(3) Software requirements performed by the item;

(4) Identification of interfaces with other items that provide data to, or receive data from, the item; and

(5) 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 ITA 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:

a. System development methodology;

b. Software design standards, including internal vendor procedures;

c. Software specification standards, including internal vendor procedures;

d. Software coding standards, including internal vendor procedures;

e. Software testing and verification standards, including internal vendor procedures, that can assist in determining the program's correctness and ACCEPT/REJECT criteria; and

f. Quality assurance standards or other documents that can be used by the ITA to examine and test the software. These documents include standards for program flow and control charts, program documentation, test planning, and for 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:

a. The logic and arithmetic capability of the processor;

b. Memory read-write characteristics;

c. External memory device characteristics;

d. Peripheral device interface hardware;

e. Data input/output device protocols; and

f. 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. A definition of the inputs to the function or mode (with characteristics, tolerances or acceptable ranges, as applicable);

b. An explanation of how the inputs are processed; and

c. 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:

a. Exception conditions;

b. System failures;

c. Data input/output errors;

d. Error logging for audit record generation;

e. Production of statistical ballot data;

f. Data quality assessment; and

g. 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, HIPOs, 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:

a. Module and unit design decisions, if any, such as algorithms used;

b. Any constraints, limitations, or unusual features in the design of the software module or unit;

c. The programming language to be used and rationale for its use if other than the specified module or unit language;

d. If the software module or unit consists of or contains procedural commands (such as menu selections in a database management system (DBMS) for defining forms and reports, on-line DBMS queries for database access and manipulation, input to a graphical user interface (GUI) 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;

e. If the software module or unit contains, receives, or outputs data, a description of its inputs, outputs, and other data elements as applicable. (Section 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;

f. If the software module or unit contains logic, the logic to be used by the software unit, including, as applicable:

(1) Conditions in effect within the software module or unit when its execution is initiated;

(2) Conditions under which control is passed to other software modules or units;

(3) Response and response time to each input, including data conversion, renaming, and data transfer operations;

(4) Sequence of operations and dynamically controlled sequencing during the software module's or unit's operation, including:

(i) The method for sequence control;

(ii) The logic and input conditions of that method, such as timing variations, priority assignments;

(iii) Data transfer in and out of memory; and

(iv) The sensing of discrete input signals, and timing relationships between interrupt operations within the software module or unit; and

(5) Exception and error handling; and

g. If the software module is a database, provide the information described in Volume II, Section 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:

a. The number of levels of design and the names of those levels (such as conceptual, internal, logical, and physical);

b. Design conventions and standards (which may be incorporated by references) needed to understand the design;

c. Identification and description of all database entities and how they are implemented physically (e.g., tables, files, etc.);

d. Entity relationship diagram and description of relationships; and

e. Details of table, record or file contents (as applicable) to include individual data elements and their specifications, including:

(1) Names/identifiers;

(2) Data type (alphanumeric, integer, etc.);

(3) Size and format (such as length and punctuation of a character string);

(4) Units of measurement (such as meters, dollars, nanoseconds);

(5) Range or enumeration of possible values (such as 0–99);

(6) Accuracy (how correct) and precision (number of significant digits);

(7) Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether business rules apply;

(8) Security and privacy constraints; and

(9) Sources (setting/sending entities) and recipients (using/receiving entities); and

f. 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:

a. Provide a unique identifier assigned to the interface;

b. Identify the interfacing entities (systems, configuration items, users, etc.) by name, number, version, and documentation references, as applicable; and

c. 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:

a. The type of interface (such as real-time data transfer, storage-and-retrieval of data, etc.) to be implemented;

b. Characteristics of individual data elements that the interfacing entity(ies) will provide, store, send, access, receive, etc., such as:

(1) Names/identifiers;

(2) Data type (alphanumeric, integer, etc.);

(3) Size and format (such as length and punctuation of a character string);

(4) Units of measurement (such as meters, dollars, nanoseconds);

(5) Range or enumeration of possible values (such as 0–99);

(6) Accuracy (how correct) and precision (number of significant digits);

(7) Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether business rules apply;

(8) Security and privacy constraints; and

(9) Sources (setting/sending entities) and recipients (using/receiving entities);

c. Characteristics of communication methods that the interfacing entity(ies) will use for the interface, such as:

(1) Communication links/bands/frequencies/media and their characteristics;

(2) Message formatting;

(3) Flow control (such as sequence numbering and buffer allocation);

(4) Data transfer rate, whether periodic/aperiodic, and interval between transfers;

(5) Routing, addressing, and naming conventions;

(6) Transmission services, including priority and grade; and

(7) Safety/security/privacy considerations, such as encryption, user authentication, compartmentalization, and auditing;

d. Characteristics of protocols the interfacing entity(ies) will use for the interface, such as:

(1) Priority/layer of the protocol;

(2) Packeting, including fragmentation and reassembly, routing, and addressing;

(3) Packeting, including fragmentation and reassembly, routing, and addressing;

(4) Legality checks, error control, and recovery procedures;

(5) Synchronization, including connection establishment, maintenance, termination; and

(6) Status, identification, and any other reporting features; and

e. Other characteristics, such as physical compatibility of the interfacing entity(ies) (dimensions, tolerances, loads, voltages, plug compatibility, etc.).

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:

a. 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;

b. References: A list of references to all related vendor documents, data, standards, and technical sources used in software development and testing; and

c. 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 6 of the Standards. 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 5, 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 by the test authority to assist in developing and executing the system qualification 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 to meet the specific requirements of Volume I, Section 6.2.1. The access control policy shall address the general features and capabilities and individual access privileges indicated in Volume I, Section 6.2.1.

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, Section 6.2.2.

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, Section 6.3 of the Standards. 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, Section 6.4 of the Standards. 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, Section 6.5:

a. For all systems, this information shall address access control, and prevention of data interception; and

b. For systems that use public communications networks as defined in Volume I Section 5, this information shall also include:

(1) Capabilities used to provide protection against threats to third party products and services;

(2) Policies and processes used by the vendor to ensure that such protection is updated to remain effective over time;

(3) 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;

(4) 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;

(5) 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; and

(6) 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:

a. Administrative and management controls for the voting system and election management, including access controls;

b. Internal security procedures, including operating procedures for maintaining the security of the software for each system function and operating mode;

c. Adherence to, and enforcement of, operational procedures (e.g., effective password management);

d. Physical facilities and arrangements; and

e. 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:

a. Development test specifications; and

b. Qualification 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:

a. Test identification and design, including:

(1) Test structure;

(2) Test sequence or progression; and

(3) Test conditions;

a. Standard test procedures, including any assumptions or constraints;

b. Special purpose test procedures including any assumptions or constraints;

c. Test data; including the data source, whether it is real or simulated, and how test data is controlled;

d. Expected test results; and

e. Criteria for evaluating test results.

Additional details for these requirements are provided by MIL–STD–498, Software Test Plan (STP) and Software Test Description (STD). In the event that test data is not available, the ITA shall design test cases and procedures equivalent to those ordinarily used during product verification.

2.7.2 Qualification Test Specifications

The vendor shall provide specifications for verification and validation of overall software performance. These specifications shall cover:

a. Control and data input/output;

b. Acceptance criteria;

c. Processing accuracy;

d. Data quality assessment and maintenance;

e. Ballot interpretation logic;

f. Exception handling;

g. Security; and

h. Production of audit trails and statistical data.

The specifications shall identify procedures for assessing and demonstrating the suitability of the software for elections 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 Section 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, including the sections listed 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 elections 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:

a. Polling place;

b. Central count facility; and

c. 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 Section 2.3 above, including:

a. Pre-voting functions;

b. Voting functions;

c. Post-voting functions; and

d. General capabilities.

These specifications also serve to provide guidance to the procuring agency in developing its acceptance test plan and procedure 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. Provides a detailed description of all input, output, control, and display features accessible to the operator or voter;

b. Provide examples of simulated interactions in order to facilitate

understanding of the system and its capabilities;

c. Provide sample data formats and output reports; and

d. 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:

a. Provides a detailed description of procedures required to initiate, control, and verify proper system operation;

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

c. Provides procedures that clearly enable the operator to intervene the system operations to recover from an abnormal system state;

d. Defines and illustrates the procedures and system prompts for situations where operator intervention is required to load, initialize, and start the system;

e. Define and illustrate procedures to enable and control the external interface to the system operating environment if supporting hardware and software are involved (such information shall be provided for the interaction of the system with other data processing systems or data interchange protocols as well);

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

g. To support successful ballot and program installation and control by election officials, provide 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; and

h. To support diagnostic testing, specify diagnostic tests that may be employed to identify problems in the system, verify the correction of maintenance problems; and isolate and diagnose faults from various systems states.

2.8.6 Operations Support

The vendor shall provide documentation of system operating procedures that meets the following requirements:

a. 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 provided to the ITA and to system users); and

b. Describe 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:

a. *Glossary:* A listing and brief definition of all terms that may be unfamiliar to persons not trained in either voting systems or computer operations;

b. *References:* A list of references to all vendor documents and to other sources related to operation of the system;

c. *Detailed Examples:* Detailed scenarios that outline correct system responses to faulty operator input. Alternative procedures may be specified depending on the system state; and

d. *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 Procedures

The system maintenance procedures shall provide information in sufficient detail to support election workers, data 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 theory of operation that fully describes such items as:

a. The electrical and mechanical functions of the equipment;

b. How the processes of ballot handling and reading are performed (paper-based systems);

c. How vote selection and casting of the ballot are performed (DRE systems);

d. How transmission of data over a network are performed (DRE systems, where applicable);

e. How data are handled in the processor and memory units;

f. How data output is initiated and controlled;

g. How power is converted or conditioned; and

h. 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:

a. All required and recommended preventive maintenance tasks, including software tasks such as software backup, database performance analysis, and database tuning;

b. Number and skill levels of personnel required for each task;

c. Parts, supplies, special maintenance equipment, software tools, or other resources needed for maintenance; and

d. 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:

a. Steps to replace failed or deficient equipment;

b. Steps to correct deficiencies or faulty operations in software;

c. Modifications that are necessary to coordinate any modified or upgraded software with other software modules;

d. The number and skill levels of personnel needed to accomplish each procedure;

e. Special maintenance equipment, parts, supplies, or other resources needed to accomplish each procedure; and

f. 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 tests 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:

a. Type;

b. Size;

c. Value or range;

d. Manufacturer's designation;

e. Individual quantities needed; and

f. 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:

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

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

c. 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 appendix include:

a. *Glossary:* A listing and brief definition of all terms that may be unfamiliar to persons not trained in either voting systems or computer maintenance;

b. *References:* A list of references to all vendor documents and other sources related to maintenance of the system;

c. *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; and

d. *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 level required to perform each of the following functions:

a. Pre-election or election preparation functions (e.g., entering an election, race and candidate information; designing a ballot; generating pre-election reports;

b. System operations for voting system functions performed at the polling place;

c. System operations for voting system functions performed at the central count facility;

d. Preventive maintenance tasks;

e. Diagnosis of faulty hardware or software;

f. Corrective maintenance tasks; and

g. 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:

a. Poll workers supporting polling place operations;

b. System support personnel involved in election programming;

c. User system maintenance technicians;

d. Network/system administration personnel (if a network is used);

e. Data personnel; and

f. Vendor personnel.

2.11 Configuration Management Plan

Vendors shall submit a Configuration Management Plan that addresses the configuration management requirements of Volume I, Section 8 of the Standards.

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 test authority to assist in developing and executing the system qualification 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 test authority 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, Section 8.3 of the Standards. These requirements pertain to:

a. Scope and nature of configuration management program activities; and

b. 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, Section 8.4. These requirements pertain to:

a. Classifying configuration items into categories and subcategories;

b. Uniquely numbering or otherwise identifying configuration items; and

c. Naming configuration items.

2.11.3 Baseline, Promotion, and Demotion Procedures

The vendor shall provide a description of the procedures and naming conventions used to address the specific requirements of Volume I, Section 8.5 of the Standards. These requirements pertain to:

a. Establishing a particular instance of a system component as the starting baseline;

b. Promoting subsequent instances of a component to baseline throughout the system development process for the first complete version of the system submitted for qualification testing; and

c. Promoting subsequent instances of a component to baseline status as the component is maintained throughout its life cycle.

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, Section 8.6 of the Standards. These requirements pertain to:

a. Developing and maintaining internally developed items;

b. Developing and maintaining third-party items;

c. Resolve internally identified defects; and

d. Resolve 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 ITAs and customers to address the specific requirements of Volume I, Section 8.7 of the Standards. These requirements pertain to:

a. A first release of the system to an ITA;

b. A subsequent maintenance or upgrade release of a system, or particular components, to an ITA;

c. The initial delivery and installation of the system to a customer; and

d. 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, Section 8.8 of the Standards. These requirements pertain to:

a. Physical configuration audit that verifies the voting system components submitted for qualification to the vendor's technical documentation; and

b. 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, Section 8.9 of the Standards. These requirements pertain to information regarding:

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

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

c. 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 7. 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 test authority. A well-organized, robust and detailed Quality Assurance Program will enable the test authority 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:

a. Scope and nature of QA activities; and

b. Breadth of application of vendor's policy and practices to the voting system.

2.12.2 Parts and Materials Special Tests and Examinations

The vendor shall provide a description of its practices for parts and materials tests and examinations that meet the requirements of Volume I, Section 7.3 of the Standards.

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, Section 7.4 of the Standards. For each test performed, the record of tests provided shall include:

a. Test location;

b. Test date;

c. Individual who conducted the test; and

d. 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, Section 7.5 of the Standards.

2.13 System Change Notes

Vendors submitting a system for testing that has been tested previously by the test authority and issued a qualification number shall submit system change notes. These will be used by the test authority to assist in developing and executing the test plan for the modified system. The system change notes shall include the following information:

a. Summary description of the nature and scope of the changes, and reasons for each changes;

b. A listing of the specific changes made, citing the specific system configuration items changed and providing detailed references to the sections of documentation changed;

c. The specific sections of the documentation that are changed (or complete revised documents, if more suitable to address a large number of changes);

d. 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.

Volume II, Section 3

Table of Contents

3 Functionality Testing

3.1 Scope

This section contains a description of the testing to be performed by the ITAs to confirm the functional capabilities of a voting system submitted for qualification. 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 compliment the diversity of the voting systems industry, the qualification testing process is not rigidly defined. Although there are basic functionality testing requirements, additions or variations in testing are appropriate in order to complement the system's use of specific technologies and configurations, the system capabilities, and the outcomes of previous testing.

3.2.1 Basic Functionality Testing Requirements

ITAs shall design and perform procedures to test a voting system against the functional requirements outlined in Volume I, Section 2. Tests procedures shall be designed and performed by the ITA that address:

a. Overall system capabilities;
b. Pre-voting functions;
c. Voting functions;
d. Post-voting functions;
e. System maintenance; and
f. Transportation and storage.

The specific procedures to be used shall be identified in the Qualification Test Plan prepared by the ITA. 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 functionality testing performed by the ITA.

Recognizing variations in system design and the technologies employed by different vendors, the ITAs shall design test procedures that account for such variations and reflect the system-specific functional capabilities in Volume I, Section 2.

3.2.2 Variation of System Functionality Testing to Reflect Voting System Technologies and Configurations

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 by the ITA for a particular system shall reflect the specific technologies and design configurations used by that system.

3.2.3 Variation of System Functionality Testing to Reflect Additional Voting System 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 that are submitted for qualification testing 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, ITAs shall design and perform system functionality testing for additional functional capabilities as well as the capabilities required by Volume I, Section 2 of the Standards.

3.2.4 Variation of System Functionality Testing to Reflect Voting Systems That Incorporate Previously Tested Functionality

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 qualification testing are designed to address this scope, and are tested accordingly.

However, some new systems seek qualification using a combination of new subsystems or system components interfaced with the components of a previously qualified system. For example, a vendor can submit a voting system for qualification testing that has a new DRE voting device, but that integrates the election management component from a previously qualified system.

In this situation, the vendor is strongly encouraged to identify in its TDP the functional capabilities supported by new subsystems/components and those supported by subsystems/components taken from a previously qualified system. The vendor is also encouraged to indicate in its system design documentation and configuration management records the scope and nature of any modifications made to the reused subsystems or components. Following these suggestions will assist the ITA in developing efficient test procedures that rely in part on the results of testing of the previously qualified subsystems or components.

In this situation the ITA may design and perform a test procedure that draws on the results of testing performed previously on reused subsystems or components. However, the scope of testing shall include, irrespective of previous testing, certain functionality tests:

a. All functionality performed by new subsystems/modules;
b. All functionality performed by modified subsystems/modules;
c. Functionality that is accomplished using any interfaces to new modules, or that shares inputs or outputs from new modules;
d. All functionality related to vote tabulation and election results reporting; and
e. All functionality related to audit trail maintenance.

3.3 General Test Sequence

There is no required sequence for performing the system qualification tests. For a system not previously qualified, the ITA 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 qualification testing process shall include functionality testing for all system functions of a voting system, minus the exceptions noted in Section 3.2. Generally, in depth functionality testing will follow testing of the systems hardware and the source code review of the system's software. ITAs will usually conduct functionality testing as an integral element of system level integration testing described in Volume II, Section 6.

Some functionality tests for the voting functions defined in Volume I, Section 2.4 and 2.5 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 Functionality Testing in Parallel With Hardware Testing for Precinct Count Systems

For testing voting functions defined in Volume I, Sections 2.4 and 2.5, the following procedures shall be performed during the functionality tests of voting equipment and precinct counting equipment.

a. The procedure to prepare election programs shall:

(1) Verify resident firmware, if any;

(2) Prepare software (including firmware) to simulate all ballot format and logic options for which the system will be used;

(3) Verify program memory device content; and

(4) Obtain and design test ballots with formats and voting patterns sufficient to verify performance of the test election programs.

b. The procedures to program precinct ballot counters shall:

(1) Install program and data memory devices, or verify presence if resident; and

(2) Verify operational status of hardware as in Volume II, Section 4.

c. The procedures to simulate opening of the polls shall:

(1) Perform procedures required to prepare hardware for election operations;

(2) Obtain ''zero'' printout or other evidence that data memory has been cleared;

(3) Verify audit record of pre-election operations; and

(4) Perform procedure required to open the polling place and enable ballot counting.

d. 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 4.

e. The procedure to simulate closing of polls shall:

(1) Perform hardware operations required to disable ballot counting and close the polls;

(2) Obtain data reports and verify correctness; and

(3) Obtain audit log and verify correctness.

They need not be performed in the sequence listed, provided the necessary precondition of each procedure has been met.

3.3.2 Functionality Testing in Parallel With Hardware Testing for Central Count Systems

For testing voting functions defined in Volume I, Sections 2.4 and 2.5, the following procedures shall be performed during the functional tests.

a. The procedure to prepare election programs shall:

(1) Verify resident firmware, if any;

(2) 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;

(3) Verify program memory device content; and

(4) Procure test ballots with formats, voting patterns, and format identifications sufficient to verify performance of the test election programs;

b. 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 4; and

c. The procedure to simulate election reports shall:

(1) Obtain reports at polling places or precinct level;

(2) Obtain consolidated reports;

(3) Provide query access, if this is a feature of the system;

(4) Verify correctness of all reports and queries; and

(5) 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

As indicated in Volume I, Section 2.2.7, voting systems shall provide accessibility to individuals with disabilities, meeting the specific requirements of this Section. ITAs shall design and perform test procedures that verify conformance with each of these requirements.

3.5 Functionality 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, ITAs shall conduct functionality tests using hardware provided by the vendor that meets the minimum configuration specifications defined by the vendor.

Volume II, 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.

Volume II, Section 4

Table of Contents

4 Hardware Testing

4.1 Scope

This section contains a description of the testing to be performed by the ITAs to confirm the proper functioning of the hardware components of a voting system submitted for qualification testing. 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

ITAs shall design and perform procedures that test the voting system hardware requirements identified in Volume I, Section 3. Test procedures shall be designed and performed by the ITA 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; and
- 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 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 manufacturers specifications and evidence that the equipment has been tested to the equivalent of the Standards.

The specific testing procedures to be used shall be identified in the Qualification Test Plan prepared by the ITA. 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 ITA.

4.2.2 Hardware Provided by Vendor

The hardware submitted for qualification 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

Qualification 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:

a. Temperature of +/−4 degrees F; and

b. Electrical supply voltage +/−2 VAC.

4.4 Test Log Data Requirements

The ITA 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 ITA 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 qualification 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 site.

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 site. 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 and are not subjected 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 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–STD810D, 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 in the preceding chart.

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 vac.

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 4.7.11 have been met.

4.7.1.1 Data Accuracy

As indicated in Volume I, Section 3, 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, Section 3.2.1 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 it 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).

Volume II, Appendix C, Section C.5 provides further details of the calculation for this testing volume.

4.7.2 Maintainability Test

The ITA shall test for maintainability based on the provisions of Volume I, Section 3 for maintainability, including both physical attributes and additional attributes regarding the ease of performing maintenance activities. These tests include:

a. Examine 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 (part of the TDP).

b. 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 ITA shall include such findings in the qualification test results of the qualification test report.

4.7.3 Reliability Test

The ITA shall test for reliability based on the provisions of Volume I, Section 3 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. Volume II, Appendix C, Section C.4 provides further details of the calculation for this testing period.

4.7.4 Availability Test

The ITA shall assess the adequacy of system availability based on the provisions of Volume I, Section 3. 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 ITA.

The model shall reflect the equipment used for a typical system configuration to perform the following system functions:

a. For all paper-based systems:

(1) Recording voter selections (such as by ballot marking or punch);

(2) Scanning the punches or marks on paper ballots and converting them into digital data;

b. For all DRE systems:

(1) Recording and storing the voter's ballot selections.

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

(1) 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; and

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

(1) 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

4.8.1 Power Disturbance

The test for power disturbance disruption shall be conducted in compliance with the test specified in in IEC 61000–4–11 (1994–06).

4.8.2 Electromagnetic Radiation

The test for electromagnetic radiation shall be conducted in compliance with the FCC Part 15 Class B requirements by testing per ANSI C63.4.

4.8.3 Electrostatic Disruption

The test for electrostatic disruption shall be conducted in compliance with the test specified in IEC 61000–4–2 (1995–01).

4.8.4 Electromagnetic Susceptibility

The test for electromagnetic susceptibility shall be conducted in compliance with the test specified in IEC 61000–4–3 (1996).

4.8.5 Electrical Fast Transient

The test for electrical fast transient protection shall be conducted in compliance with the test specified in IEC 61000–4–4 (1995–01).

4.8.6 Lightning Surge

The test for lightning surge protection shall be conducted in compliance with the test specified in IEC 61000–4–5 (1995–02).

4.8.7 Conducted RF Immunity

The test for conducted RF immunity shall be conducted in compliance with the test specified in IEC 61000–4–6 (1996–04).

4.8.8 Magnetic Fields Immunity

The test for AC magnetic fields RF immunity shall be conducted in compliance with the test specified in IEC 61000–4–8 (1993–06).

Volume II, Section 5

Table of Contents

5 Software Testing

5.1 Scope

This section contains a description of the testing to be performed by the ITA to confirm the proper functioning of the software components of a voting system submitted for qualification 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:

a. Volume II, Section 3, for specific tests of voting system functionality; and

b. Volume II, 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

ITAs shall design and perform procedures that test the voting system software requirements identified in Volume I. 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 ITA 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 ITA.

The ITA may inspect COTS source code units to determine testing requirements or to verify the code is unmodified.

The ITA 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 Qualification Test Plan prepared by the ITA. 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 ITA.

Recognizing variations in system design and the technologies employed by different vendors, the ITAs shall design test procedures that account for these variations.

5.3 Initial Review of Documentation

Prior to initiating the software review, the ITA shall verify that the documentation submitted by the vendor in the TDP is sufficient to enable:

a. Review of the source code; and

b. Design and conducting of 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 standards.

5.4 Source Code Review

The ITA 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 4.

5.4.1 Control Constructs

Voting system software shall use the control constructs identified in this section as follows:

a. 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;

b. 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); and

c. 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.

Illustrations of control construct techniques are provided in Figures 4–1 through 4–6.

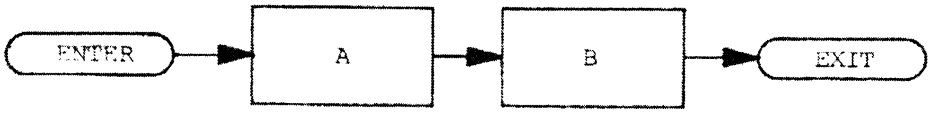
- Fig. 4–1 Sequence
- Fig. 4–2 If-Then-Else
- Fig. 4–3 Do-While
- Fig. 4–4 Do-Until
- Fig. 4–5 Case
- Fig. 4–6 General loop, including the special case FOR loop

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.

BILLING CODE 6820–KF–P

5.4.1.2 Figures



Control flows from "Process A" to the next in sequence, "Process B."

Figure 4-1, "SEQUENCE"

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.

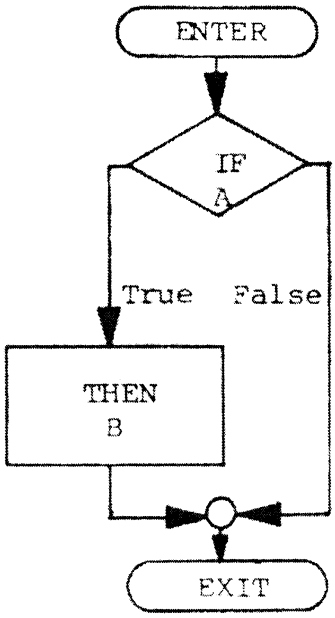


Figure 4-2, "IF-THEN-ELSE"

*In Figure 4-2, Flow of control will skip a process pending the condition of "A."

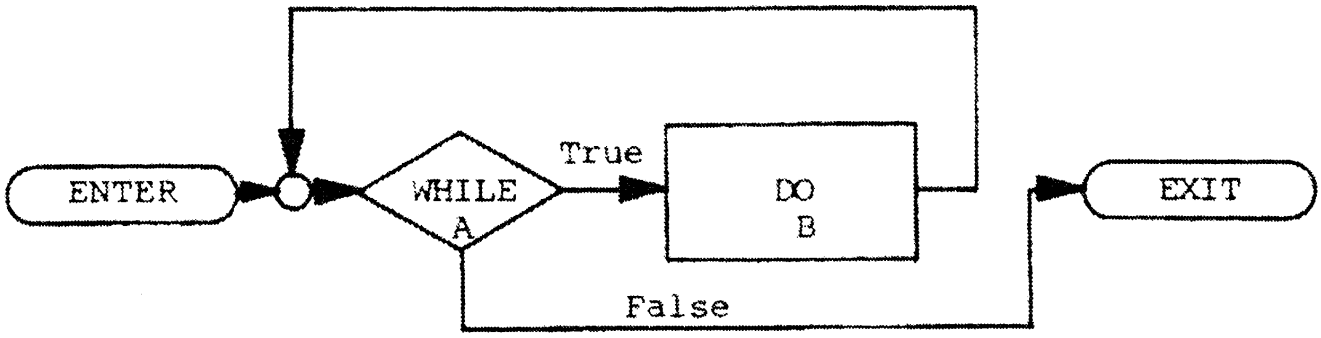


Figure 4-3, "DO-WHILE"

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.

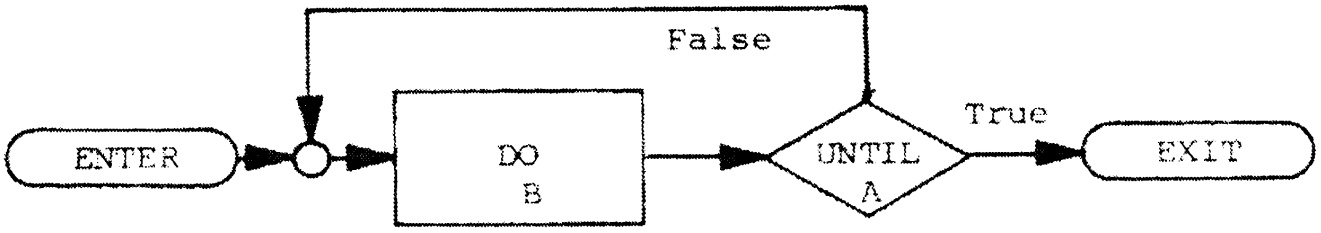


Figure 4-4, "DO-UNTIL"

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.

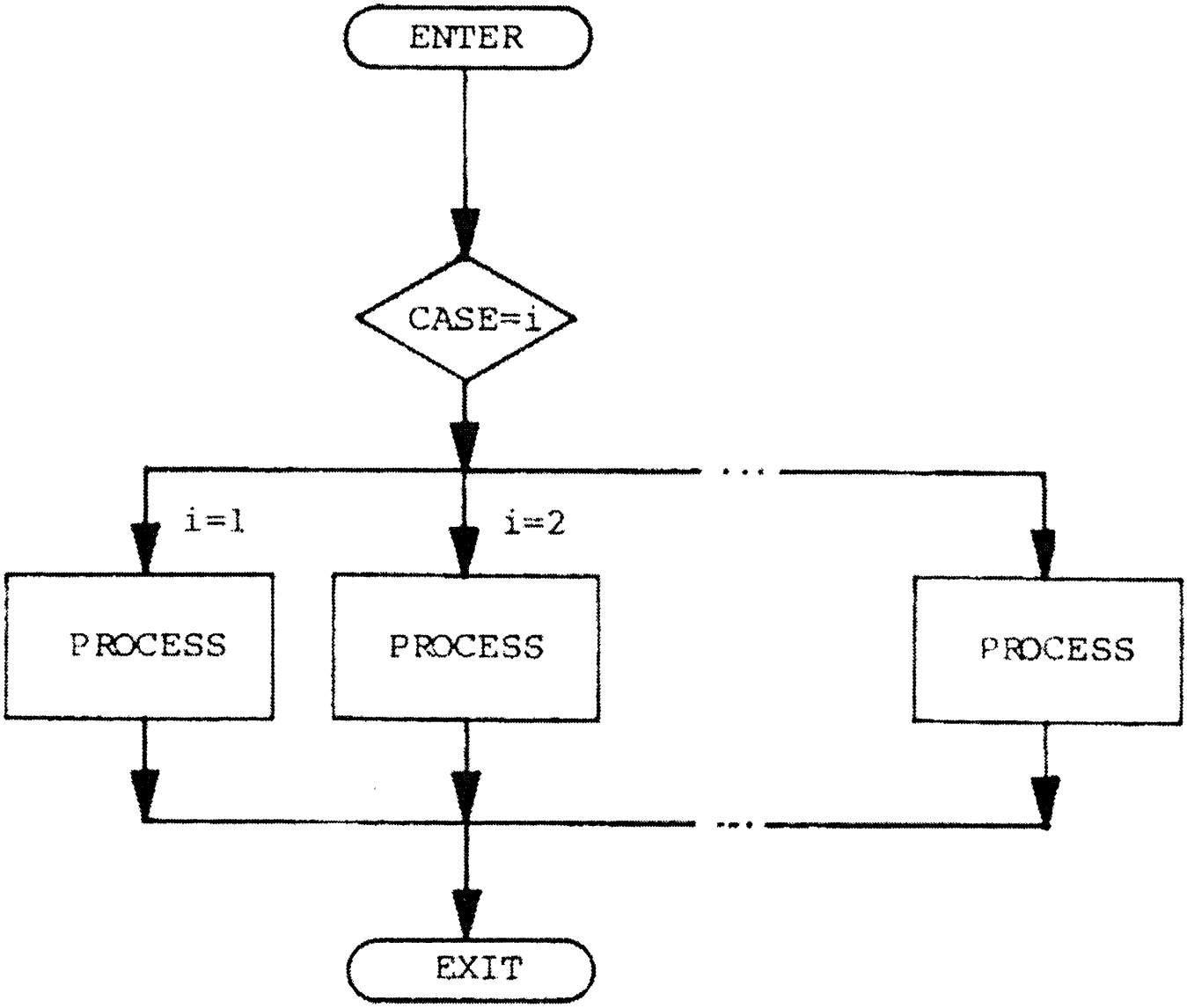


Figure 4-5, "CASE"

Control is passed to a Process based on the value of i.

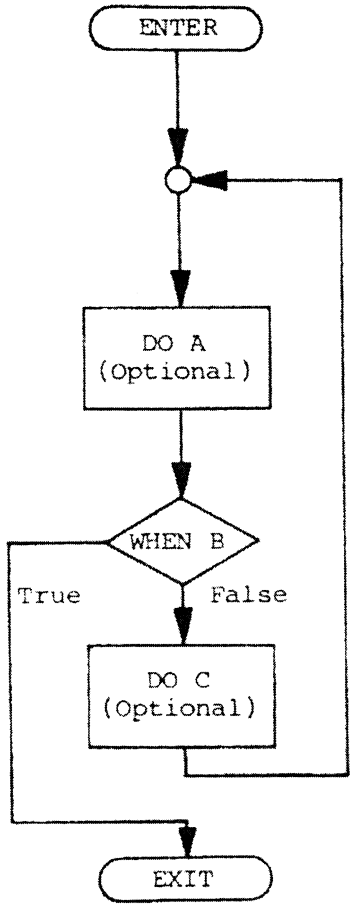


Figure 4-6, "General LOOP"

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 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 the 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 too 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 ITA 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, section 4.2.6.a, the ITA shall review the code to ensure that it:

a. 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;

b. For C based language and others to which this applies, has the return explicitly defined for callable units such as functions or procedures (do not drop through by default) and, in the case of functions, have 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;

c. Does not use macros that contain returns or pass control beyond the next statement;

d. For those languages with unbound arrays, provides controls to prevent writing beyond the array, string, or buffer boundaries;

e. 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;

f. For those languages supporting case statements, has a default choice explicitly defined to catch values not included in the case list;

g. 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;

h. Is indented consistently and clearly to indicate logical levels;

i. 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;

j. 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 ITA with the generated source code replaced with an unexpanded macro call or its equivalent;

k. Has no line of code exceeding 80 columns in width (including comments and tab expansions) without justification;

l. Contains no more than one executable statement and no more than one flow control statement for each line of source code;

m. 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;

n. Avoids mixed-mode operations. If mixed mode usage is necessary, then all uses shall be identified and clearly explained by comments;

o. Upon exit() at any point, presents a message to the user indicating the reason for the exit().

p. 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.

q. References variables by fewer than five levels of indirection (i.e. a.b.c.d or a[b].c->d).

r. 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
                                        }
                                }
                }
        }
}
}
```

s. Initializes every variable upon declaration where permitted

t. Specifies explicit comparisons in all if() and while() conditions. For instance,

i. if(flag)

is prohibited, and shall be written in the format

ii. if (flag == TRUE)

for both single and multiple conditions.

u. 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.

v. Only contains the minimum implementation of the ''a = b ? c : d'' syntax. Expansions such as ''j=a?(b?c:d):e;'' are prohibited.

w. 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 enable and active as a test version.

Volume II, Section 6

Table of Contents

6 System Level Integration Testing

6.1 Scope

This section contains a description of the testing to be performed by the ITAs to confirm the proper functioning of the fully integrated components of a voting system submitted for qualification 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 qualification tests address the integrated operation of both hardware and software, along with any telecommunications capabilities. The system-level qualification tests shall include the tests (functionality, volume, stress, usability, security, performance, and recovery) indicated in the ITAs' Qualification 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

ITAs 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, 5, 6 and 8.

These procedures shall also address the requirements for testing system functionality provided in Volume II, Section 3. Where practical, the ITA 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 ITA will use the coverage report to identify any portions of the source code that were not covered and determine:

a. The additional functional tests that are needed;

b. Where more detailed source code review is needed; or

c. Both of the above.

The specific procedures to be used shall be identified in the Qualification Test Plan prepared by the ITA. 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 ITA.

Recognizing variations in system design and the technologies employed by different vendors, the ITAs shall design test procedures that account for these variations.

6.2.2 System Baseline for Testing

The system level qualification tests are conducted using the version of the system as it is intended to be sold by the vendor and delivered to jurisdictions. To ensure that the system version tested is the correct version, the ITA 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 qualification testing process, the ITA shall require the vendor conduct a new ''build'' of the system to ensure that the qualified 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 ITA 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 ITA's Qualification 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 the Standards.

Some voting systems may use components or subsystems from previously tested and qualified systems, such as ballot preparation. For these scenarios, the ITA shall, at a minimum,

a. Confirm that the version of previously approved components and subsystems are unchanged; and

b. 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 as defined in Section 5. For those systems that do use such capabilities, components that are located at the poll site or separate vote counting site 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 vendor (e.g., public telephone networks), the ITA 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 ITA shall design and perform test procedures that test the security capabilities of the voting system against the requirements defined in Volume I, Section 6. These procedures shall focus on the ability of the system to detect, prevent, log, and recover from a broad range of security risks as identified in Section 6 and system capabilities and safeguards, claimed by the vendor in its TDP that go beyond the risks and threats identified in Volume I, Section 6.

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, including the Internet, to transmit election management data or official election results (such as ballots or tabulated results), the ITAs 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 qualification.

The ITA 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 ITA may conduct or simulate attacks on the system to confirm the effectiveness of the system's security capabilities, employing test procedures approved by the NASED Voting Systems Board.

6.4.1 Access Control

The ITA shall conduct tests of system capabilities and review the access control policies and procedures and 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 ITA shall design tests to confirm that these security elements work as specified.

Specific activities to be conducted by the ITA shall include:

a. A review of the vendor's access control policies, procedures and system capabilities to confirm that all requirements of Volume I, Section 6.2 have been addressed completely; and

b. Specific tests designed by the ITA 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:

(1) 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 (including firmware) installation (as described in Volume I, Section 6.4); and

(2) 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 ITA shall review, and conduct tests of, the data interception and prevention safeguards specified by the vendor in its TDP. The ITA 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 ITA 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:

a. Identification of new threats and their impact;

b. Development or acquisition of effective countermeasures;

c. System testing to ensure the effectiveness of the countermeasures;

d. Notification of client jurisdictions that use the system of the threat and the actions that should be taken;

e. Distribution of new system releases or updates to current system users; and

f. Confirmation of proper installation of new system releases.

6.5 Accessibility Testing

The ITA shall design and perform procedures that test the capability of the voting system to assist voters with disabilities. ITA test procedures shall confirm that:

a. Voting machines intended for use by voters with disabilities provide the capabilities required by Volume I, Section 2.2.7;

b. Voting machines intended for use by voters with disabilities operate consistent with vendor specifications and documentation; and

c. Voting machines intended for use by voters with disabilities meet all other functional requirements required by Volume I, Section 2.

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:

a. 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;

b. 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 test agency shall verify that the vendor's engineering and test data are for the software version submitted for qualification;

c. 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;

d. 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-level functional and performance tests; and

e. All subsequent changes to the baseline software configuration made during the course of qualification testing shall be subject to reexamination. All changes to the system hardware that may produce a change in software operation shall also be subject to reexamination.

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.):

a. The test agency 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; and

b. The test agency 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 ITA shall design and conduct all appropriate module and integrated functional tests. The functional configuration audit may be performed in the facility either of the test agency 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.

Volume II, Section 7

Table of Contents

7 Examination of Vendor Practices for Configuration Management and Quality Assurance

7.1 Scope

This section contains a description of the examination performed by the ITAs to confirm 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

ITAs shall design and perform procedures that examine documented vendor practices for quality assurance and configuration management as addressed by Volume I, Sections 7 and 8, and complemented by Volume II, Section 2.

Examination procedures shall be designed and performed by the ITA that address:

a. Conformance with the requirements to provide information on vendor practices required by the Standards;

b. Conformance of system documentation and other information provided by the vendor with the documented practices for quality assurance and configuration management.

The Standards do not require on-site examination of the vendor's quality assurance and configuration management practices during the system development process. However, the ITAs 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 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.

It is recognized that examinations of vendor practices, and determinations of conformance, entail a significant degree of professional judgement. These standards for vendor practices identify specific areas of focus for the ITAs, while at the same time relying on their expertise and professional judgement, as evaluated in the certification of the ITAs.

The specific procedures used by the ITA shall be identified in the Qualification Test Plan. Recognizing variations in vendors' quality assurance and configuration management practices and procedures, the ITAs 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 within the overall qualification testing process 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 other elements of the qualification test process.

7.3.1 Examination of Vendor Practices in Parallel With Other Qualification Testing

While not required, ITAs are encouraged to initiate the examinations of quality assurance and configuration management practices early in the overall qualification testing sequence, and 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 qualification process,

7.3.2 Performance of Functional Configuration Audit as an Element of Integrated System Testing

As described in Volume I, Section 8, 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 ITAs as an element of integrated system testing that confirms the proper functioning of the system as a whole. Integrated system testing is described in more detail in Volume II, Section 6.

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 8, and the documentation requirements described in Volume II, Section 2. In addition to confirming that all required information has been submitted, the ITAs shall determine the vendor's conformance with the documented configuration management practices.

7.4.1 Configuration Management Policy

The ITAs shall examine the vendor's documented configuration management policy to confirm that it:

a. Addresses the full scope of the system, including components provided by external suppliers; and

b. Addresses the full breadth of system documentation;

7.4.2 Configuration Identification

The ITAs shall examine the vendor's documented configuration identification practices policy to confirm that they:

a. Describe clearly the basis for classifying configuration items into categories and subcategories, for numbering of configuration items; and for naming of configuration items; and

b. Describe 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 ITA shall examine the vendor's documented baseline, promotion and demotion procedures to confirm that they:

a. Provide a clear, controlled process that promotes components to baseline status when specific criteria defined by the vendor are met; and

b. 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 ITA shall examine the vendor's configuration control procedures to confirm that they:

a. Are capable of providing effective control of internally developed system components; and

b. Are capable of providing effective control of components developed or supplied by third parties.

7.4.5 Release Process

The ITA shall examine the vendor's release process to confirm that it:

a. Provides clear accountability for moving forward with the release of the initial system version and subsequent releases;

b. Provides the means for clear identification of the system version being replaced;

c. Confirms that all required internal vendor tests and audits prior to release have been completed successfully;

d. Confirms that each system version released to customers has been qualified by a the appropriate ITA prior to release;

e. Confirms that each system release has been received by the customer; and

f. Confirms that each system release has been installed successfully by the customer;

7.4.6 Configuration Audits

The ITA shall examine the vendor's configuration audit procedures to confirm that they:

a. Are sufficiently broad in scope to address the entire system, including system documentation;

b. Are conducted with appropriate timing to enable effective control of system versions; and

c. Are sufficiently rigorous to confirm that all system documentation prepared and maintained by the vendor indeed matches the actual system functionality, design, operation and maintenance requirements.

7.4.7 Configuration Management Resources

The ITA 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 7, and the documentation requirements described in Volume II, Section 2. The ITA shall confirm that all required information has been submitted, and assess whether the vendor's quality assurance program provides for:

a. Clearly measurable quality standards;

b. An effective testing program throughout the system development life cycle;

c. Application of the quality assurance program to external providers of system components and supplies;

d. Comprehensive monitoring of system performance in the field and diagnosis of system failures;

e. Effective record keeping of system failures to support analysis of failure patterns and potential causes; and

f. 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 ITA shall focus on the specific elements of the vendor's quality assurance program indicated below.

7.5.1 Quality Assurance Policy

The ITA shall examine the vendor's quality assurance policy to confirm that it:

a. Addresses the full scope of the voting system;

b. Clearly designates a senior level individual accountable for implementation and oversight of quality assurance activities;

c. Clearly designates the individuals, by position within the vendor's organization, who are to conduct each quality assurance activity; and

d. Provides procedures that determine compliance with, and correct deviations from, the quality assurance program at a minimum annually.

7.5.2 Parts & Materials Special Tests and Examinations

The ITA shall examine the vendor's parts and materials special tests and examinations to confirm that they:

a. 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;

b. Are designed in a manner appropriate to determine suitability; and

c. Have been conducted and documented for all applicable parts and materials.

7.5.3 Quality Conformance Inspections

The ITAs shall examine the vendor's quality conformance plans, procedures and inspection results to confirm that:

a. All components have been tested according to the test requirements defined by the vendor;

b. All components have passed the requisite tests; and

c. For each test, the test documentation identifies:

(1) Test location;

(2) Test date;

(3) Individual who conducted the test; and

(4) Test outcome.

7.5.4 Documentation

The ITAs shall examine the vendor's voting system documentation to confirm that it meets the content requirements of Volume I, Section 7.5, and Volume I Section 2, and is written in a manner suitable for use by purchasing jurisdictions.

Volume II, Appendix A

Table of Contents

A Qualification Test Plan

A.1 Scope

This Appendix contains a recommended outline for the Qualification Test Plan, which is to be prepared by the test agency. The primary purpose of the test plan is to document the test agency's development of the complete or partial qualification test. A sample outline of a Qualification Test Plan is illustrated in Figure A–1 at the end of this Appendix.

It is intended that the test agency use this Appendix as a guide in preparing a detailed test plan, and that the scope and detail of the requirements for qualification 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 prequalification tests and information available on the specific software's physical and functional configuration.

Prior to development of any test plan, the test agency must obtain the Technical Data Package (TDP) from the vendor submitting the voting system for qualification. The TDP contains information necessary to the development of a Qualification Test Plan, such as the vendor's Hardware Specifications, Software Specifications, System Operating Manual and System Maintenance Manual.

It is foreseen that vendors may submit some voting systems in use at the time the standards are issued to partial qualification tests. It is also specified by the standards that voting systems incorporating the vendor's software and COTS hardware need only be submitted for software and system-level tests. Requalification of systems with modified software or hardware is also anticipated. The test agency shall alter the test plan outline as required by these situations.

The following sections describe the individual sections of the recommended Qualification Test Plan.

The test agency 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 agency shall list all documents that contain material used in preparing the test plan. This list shall include specific reference to applicable portions of the standards, and to the vendor's TDP.

A.1.2 Terms and Abbreviations

The test agency shall list and define all terms and phrases relevant to the hardware, the software, or the test plan.

A.2 Prequalification Tests

The test agency shall evaluate vendor tests, or other agency tests in determining the scope of testing required for system qualification. Prequalification test activities may be particularly useful in designing software functional test cases and tests of system security.

The ITA shall summarize prequalification test results that support the discussion of the preceding section.

A.3 Materials Required for Testing

The following materials must presented to the ITA in order to facilitate testing of the voting system:

- Software;
- Equipment;
- Test materials;
- Deliverable materials; and
- Proprietary Data.

A.3.1 Software

The ITA shall list all software required for the performance of hardware, software, telecommunications, security and integrated system 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 ITA shall list all equipment required for the performance of the hardware, software, telecommunications, security and integrated system 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 ITA 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 ITA shall list all documents and materials to be delivered as a part of the system, such as:

- Hardware specification;
- Software specification;
- Voter, operator, and hardware and software maintenance manuals;
- Program listings, facsimile ballots, tapes; and
- Sample output report formats.

A.3.5 Proprietary Data

The ITA shall list and describe all documentation and data that are the private property of the vendor, and hence are subject to restrictions with respect to ITA use, release, or disclosure.

A.4 Test Specifications

The ITA shall cite the pertinent hardware qualitative examinations and quantitative tests that follow from Volume I, Sections 3 and 9. The ITA shall also describe the specific test requirements that follow from the design of the software and telecommunications capabilities under test.

The qualification test shall include ITA consideration of hardware, software and telecommunications, design; and ITA 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 ITA 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 ITA shall describe the software functions in sufficient detail to provide a foundation for selecting the test case designs and conditions contained in Subsections A.4.4.3, A.4.4.4, and A.4.4.5, below. On the basis of this test case design, the ITA shall prepare a table delineating software functions and how each shall be tested.

A.4.3 Test Case Design

The ITA 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; and
- System-level Test Case Design.

A.4.3.1 Hardware Qualitative Examination Design

The ITA 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 standards concerning the requirements for:

- Overall system capabilities;
- Pre-voting functions;
- Voting functions; and
- Post-voting functions.

In the event that a review of the results of previous examinations indicates problem areas, the test agency 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 ITA 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 qualification tests described in Volume I, Section 9 of the standards. The test agency shall cite any additional tests required, based on this review and those tests requested by the vendor or the state. The test agency shall also cite any environmental tests of Section 9 that are not to be conducted, and note the reasons why.

For complete qualification, environmental tests shall include the following tests, depending upon the design and intended use of the hardware.

a. Non-operating tests, including the:
(1) Bench handling test;
(2) Vibration test;
(3) Low temperature test;
(4) High temperature test; and
(5) Humidity test; and

b. 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 agency shall review the vendor's program analysis, documentation, and, if available, module test case design. The test agency 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 qualification test.

If the vendor's module test case design does not provide conclusive coverage of all program paths, then the test agency shall perform an independent analysis to assess the frequency and consequence of error of the untested paths. The ITA shall design additional module test cases, as required, to provide coverage of all modules containing untested paths with potential for untrapped errors.

The test agency 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 agency 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 agency shall review the vendor's test plans and data to verify that the individual performance requirements described in Volume II, Section 2, Subsection 2.5.3.5, are reflected in the software.

As a part of this process, the test agency shall review the vendor's functional test case designs. The test agency shall prepare a detailed matrix of system functions and the test cases that exercise them. The test agency 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 agency shall define ACCEPT/REJECT criteria for qualification using the Software Specifications and, if the software runs on special hardware, the associated Hardware Specifications to determine acceptable ranges of performance.

The test agency 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.

a. Ballot preparation subsystem;

b. Test operations performed prior to, during, and after processing of ballots, including:

(1) Logic tests to verify interpretation of ballot styles, and recognition of precincts to be processed;

(2) Accuracy tests to verify ballot reading accuracy;

(3) Status tests to verify equipment statement and memory contents;

(4) Report generation to produce test output data; and

(5) Report generation to produce audit data records;

c. Procedures applicable to equipment used in the polling place for:

(1) Opening the polling place and enabling the acceptance of ballots; (b) maintaining a count of processed ballots;

(2) Monitoring equipment status;

(3) Verifying equipment response to operator input commands;

(4) Generating real-time audit messages;

(5) Closing the polling place and disabling the acceptance of ballots;

(6) Generating election data reports;

(7) Transfer of ballot counting equipment, or a detachable memory module, to a central counting location; and

(8) Electronic transmission of election data to a central counting location; and

d. Procedures applicable to equipment used in a central counting place:

(1) Initiating the processing of a ballot deck or PMD for one or more precincts;

(2) Monitoring equipment status;

(3) Verifying equipment response to operator input commands;

(4) Verifying interaction with peripheral equipment, or other data processing systems;

(5) Generating real-time audit messages;

(6) Generating precinct-level election data reports;

(7) Generating summary election data reports;

(8) Transfer of a detachable memory module to other processing equipment;

(9) Electronic transmission of data to other processing equipment; and

(10) Producing output data for interrogation by external display devices.

A.4.3.5 System-Level Test Case Design

The test agency shall provide a description of system tests of both the software and hardware. For software, these tests shall be designed according the stated design objective without consideration of its functional specification. The test agency 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:* These tests are designed to exercise system capabilities and features intended for use by voters with disabilities in accordance with Volume I, Section 2.2.5;
- *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; and
- *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 agency shall identify all data recording requirements (e.g.; what is to be measured, how tests and results are to be recorded). The test agency shall also design or approve the design of forms or other recording media to be employed. The test agency shall supply any special instrumentation (pulse measuring device) needed to satisfy the data requirements.

A.5.2 Test Data Criteria

The test agency 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 3, Hardware Standards.
- *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 nontest 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 agency 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 shall have been shown 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 agency 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 agency 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 agency 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 agency shall state any restrictions on the grouping or sequence of tests in this section.

A.6.4 Test Operations Procedures

The test agency 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 agency 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 agency shall also provide a description of the procedures to be followed by the test personnel.

Figure A–1

Test Plan Outline

1 Introduction

1.1 References
1.2 Terms and Abbreviations

2 Prequalification Tests

2.1 Prequalification Test Activity

B Qualification Test Report

B.1 Scope

This Appendix contains a recommended outline for the Qualification Test Report to be prepared by the test agency. 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 Voting System Qualification Test Report

A full report is prepared for the initial qualification testing of a voting system. This document consists of five main sections: Introduction, Qualification Test Background, System Identification, System Overview, and Qualification 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.8 describe the contents of the individual sections of this report.

B.1.2 Changes to Previously Qualified Voting System Qualification Test Report

This report addresses a wide range of scenarios. After a preliminary review of the submitted changes, the test agency may determined that:

a. A review of all change documentation against the baseline materials was sufficient for recommendation for qualification; or

b. All changes must be retested against the previously qualified baseline; or

c. The scope of the changes are substantial enough such that a complete retest of the software is required.

The format of this report varies, based on the type of review that was performed. If only a review of change documentation against the baseline materials was 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 Qualification Test Background

This section contains the following information:

a. General information about the qualification test process; and

b. 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:

a. System name and major subsystems (or equivalent);

b. System Version;

c. Test Support Hardware; and

d. 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 Qualification 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:

a. 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;

b. The degree to which the hardware and software meet the vendor's specifications and the standards, and the acceptability of the vendor's technical and user documentation;

c. General findings on the maintainability of the system including, where applicable, notation of specific maintenance activities that are determined to be difficult to perform;

d. Identification and description of any deficiencies that remain uncorrected after completion of the qualification test and that has caused or is 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); and

e. A specific recommendation to the NASED ITA Committee 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, Sections 3 and 4 of the Standards, or failure to fully implement formal programs for quality assurance and configuration management described in Volume I, Sections 7 and 8. The nature of the deficiency is described in detail sufficient to support the recommendation either to accept or to reject the system, and 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 Qualification 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.

Volume II, Appendix C

Table of Contents

C Appendix C: Qualification Test Design Criteria

C.1 Scope

This appendix describes the guiding principles used to design the voting system qualification testing process conducted by ITAs.

Qualification tests are designed to demonstrate that the system meets or exceeds the requirements of the Standards. The tests are also used to demonstrate compliance with other levels of performance claimed by the manufacturer.

Qualification 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 and statistical methods of the test designs contained in the Standards are discussed below. Technical descriptions of their design can be found in any of several books on testing and statistical analysis.

C.2 Approach To Test Design

The qualification tests specified in the Standards 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 preselection of some test parameter, such as the number of failures or other detectable factor. 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 Standards, 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 Standards 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

An 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, Hardware Testing, 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 of the Standards.

In this case, the null hypothesis is that the Mean Time Between Failure (MTBF), as defined in Volume I, Subsection 3.4.3 of the Standards, 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 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 an 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.

Qualification 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 Standards 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:

- 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; and
- 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. 06–3101 Filed 4–11–06; 8:45 am]
BILLING CODE 6820–KF–C