



FEDERAL ELECTION COMMISSION  
WASHINGTON, D.C. 20463



RECEIVED  
FEDERAL ELECTION COMMISSION  
COMMUNICATIONS SECTION

JUN 15 12 06 PM '01

**AGENDA ITEM**  
For Meeting of: 6-28-01

June 14, 2001

**MEMORANDUM**

**TO:** The Commission  
**THROUGH:** James Pehrkon, Staff Director   
**FROM:** Penelope Bonsall, Director Office of Election Administration   
**SUBJECT:** Release for Public Comment of Voting Systems Standards Materials

Please find attached the following items which we submit for your review and approval prior to their release to the general public for a 60-day comment period:

- Federal Register Notice
- An Overview of Volume 1
- Voting System Performance Standards: Volume 1

These revised Standards and accompanying documents have been developed by American Management Systems (AMS) in conjunction with FEC staff and NASED's Voting Systems Board which has, over the past 22 months and 5 public meetings, reviewed much of the draft material. Voting system vendors, the U.S. Access Board, the Disability Section of the Department of Justice, computer security experts, and other interested parties have also participated in this deliberative process.

These are technical standards that relate to voting system performance. As such, they do not include the administrative or management functions, nor do they address all the problems encountered in the Florida 2000 elections, such as what constitutes a vote, lack of uniform recount procedures, or human engineering considerations. While the Commission receives public comments, work will proceed on the final draft of the system test plans and criteria which we are scheduled to deliver for review at the end of October.

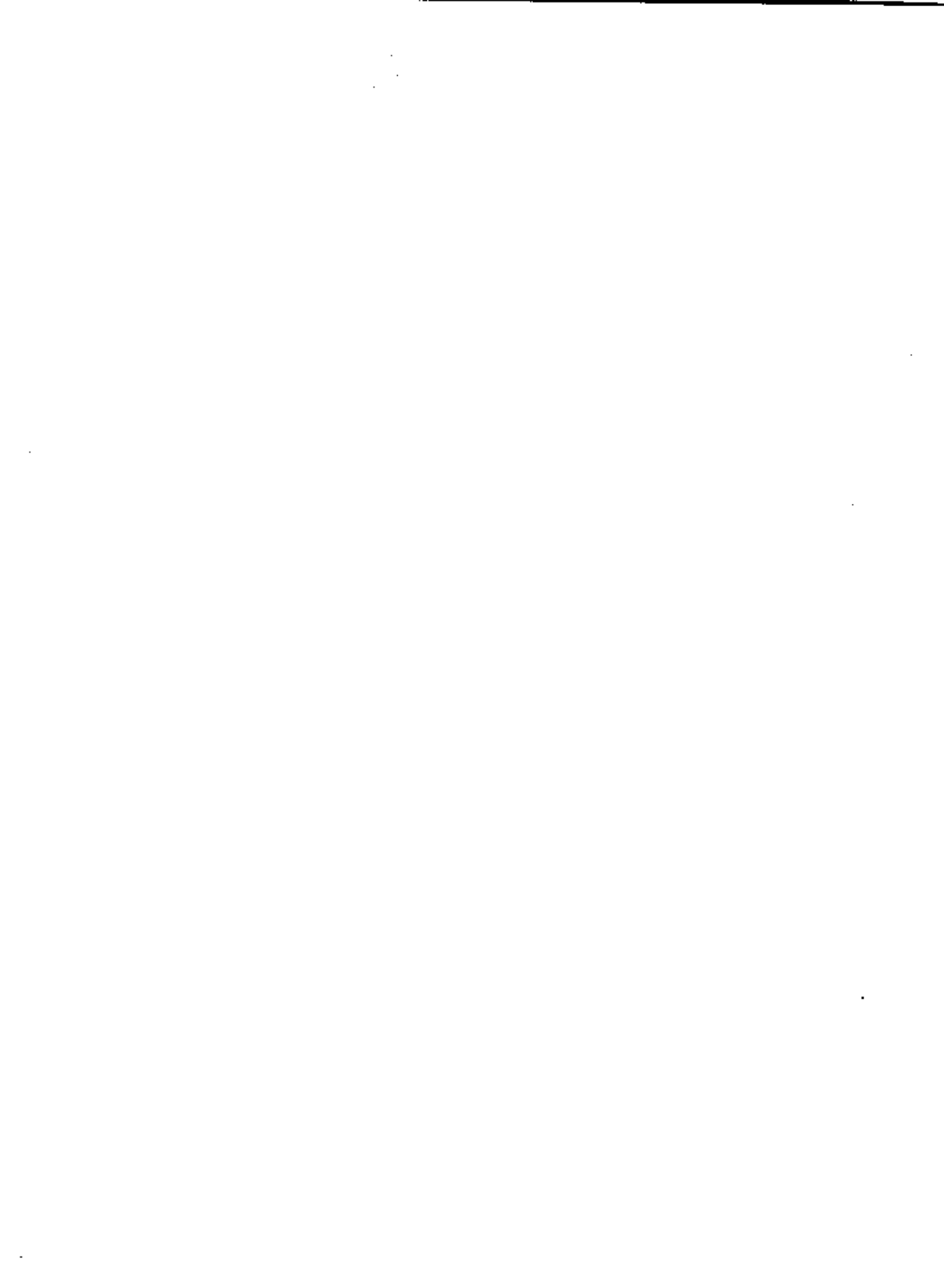


These standards remain voluntary, but NASED and many States will look to these specifications as they procure new electronic voting systems in the next 2 to 4 years.

#### RECOMMENDATIONS:

The Office of Election Administration recommends that the Commission:

1. Approve the Federal Register Notice
2. Approve the release of the Overview document
3. Approve the release of Volume 1 of the Voting System Standards



1  
2  
3  
4  
5  
6  
7  
8  
9  
0  
1  
2  
3  
4  
5  
6  
7  
8  
9  
0  
1  
2

**FEDERAL ELECTION COMMISSION**

[Notice 2001 - ]

**Voluntary Standards for Computerized Voting Systems**

**AGENCY:** Federal Election Commission

**ACTION:** Notice with request for comments.

**SUMMARY:** The Federal Election Commission (the "FEC") requests comments on proposed revisions to the 1990 national voluntary performance standards for computerized voting systems. Please note that the draft revised standards do not represent a final decision by the Commission, nor do they include proposed revised test standards. The FEC will publish a notice when the proposed revised test standards are available for comment, and another notice when the final revised performance and test standards are issued. Note also that the text of the final documents will not become part of the Code of Federal Regulations because they are intended only as guidelines for States and voting system vendors. States may mandate the specifications and procedures through their own statutes, regulations, or administrative rules. Voting system vendors may voluntarily adhere to the standards to ensure the reliability, accuracy, and integrity of their products. Further information is provided in the supplementary information that follows.

**DATE:** Comments must be received on or before [insert date 60 days after date of publication in the Federal Register].

1 **ADDRESSES:** Copies of the draft revised performance standards may be found on the  
2 Federal Election Commission's web site at [www.fec.gov/elections.html](http://www.fec.gov/elections.html), or  
3 may be requested by contacting the Office of Election Administration,  
4 Federal Election Commission, 999 E Street, NW, Washington, DC 20463.  
5 They may also be picked up at the Office of Election Administration, 800  
6 N. Capital St. NW, Washington, DC, Suite 600. All comments should be  
7 addressed to Ms. Penelope Bonsall, Director, Office of Election  
8 Administration, and must be submitted in either written or electronic form.  
9 Written comments should be sent to the Office of Election Administration,  
0 Federal Election Commission, 999 E Street, NW, Washington, DC 20463.  
1 Faxed comments should be sent to (202)219-8500, with printed copy  
2 follow-up to insure legibility. Electronic mail comments should be sent to  
3 [VSS@fec.gov](mailto:VSS@fec.gov). See the Supplementary Information that follows for file  
4 formats and other information about filing comments electronically.

5 **FOR FURTHER**  
6 **INFORMATION**  
7 **CONTACT:**

8 Ms. Penelope Bonsall, Director, Office of Election Administration, 999 E  
9 Street, NW, Washington, DC 20463; Telephone: (202) 694-1095; Toll  
0 Free.(800) 424-9530, extension 1095.

1 **SUPPLEMENTARY INFORMATION:** The FEC issued the first national voluntary voting  
2 system standards in response to the States' requests for assistance, after a number of voting  
3 system failures in the field. The FEC's Office of Election Administration undertook this activity  
4 pursuant to its responsibilities under 2 U.S.C. 438(a)(10), which requires the FEC to "serve as a

1 national clearinghouse for the compilation of information and review of procedures with respect  
2 to the administration of Federal elections.”

3 The FEC began developing the first performance standards and test criteria for computer  
4 based voting systems in 1984, subsequent to two studies. The first study was the 1975  
5 publication entitled “Effective Use of Computing Technology in Vote Tallying”, which was  
6 prepared jointly by the National Bureau of Standards (now the National Institute of Standards  
7 and Technology) and the FEC’s predecessor at the General Accounting Office. This report  
8 concluded that one of the basic causes for computer-related election problems was the lack of  
9 appropriate technical skills at the State and local level for developing or implementing  
10 sophisticated and complex written standards, against which voting system hardware and software  
11 could be tested. The second report was a congressionally mandated feasibility study published in  
12 1982? 1983? and entitled “Voting System Standards: A Report to the Congress on the  
13 Development of Voluntary Engineering and Procedural Performance Standards for Voting  
14 Systems”. This document, produced by the FEC in cooperation with the National Bureau of  
15 Standards, cited a substantial number of technical and management problems that affected the  
16 integrity of the vote counting process. It also detailed the need and desirability of having a  
17 federal agency develop voluntary national technical standards and test criteria for voting systems  
18 other than mechanical lever or hand-counted paper ballot systems.

19 The original standards took six-years to develop. A series of public meetings were held.  
20 State and local election officials, representatives of voting system vendors, technical consultants,  
21 and others reviewed drafts of the proposed criteria. A notice soliciting comments from the  
22 public was published in the Federal Register on August 8, 1989. 54 FR 32479. The FEC  
23 meticulously reviewed all responses to the notice and incorporated corrections and suitable

suggestions. Notice of the final standards was published in the Federal Register on February 5, 1990. 55 FR 3764.

Thirty-seven States now report that they have implemented, or intend soon to adopt, the standards. The National Association of State Election Directors ("NASED") oversees the national testing of voting systems by independent test authorities using the standards. The Election Center, a private membership association of election officials, serves as Secretariat for the NASED testing program.

Today, election officials are better assured that the voting systems they procure will work accurately and reliably. Voting system failures are on the decline, and now tend to involve pre-standard equipment, untested equipment configurations, or the mismanagement of tested equipment.

Nevertheless, after ten years of use, the standards needed revision. The technologies used to develop voting systems and way the voting process is administered had evolved and continue to evolve. The needs of the disabled community have been widely recognized. In addition, voting system vendors, NASED independent test authorities, States, and local jurisdictions have gained much experience in using the standards and have identified areas for refinement.

The FEC initiated this particular revision process in the fall of 1999, after conducting an analysis to pinpoint where revisions were needed and to estimate associated costs. The production of draft revised standards involved technical consultants, representatives of the two NASED certified independent test authorities, State and local election officials who are members of the NASED committee that oversees the testing process, and the Executive Director of The Election Center. Voting system vendors also were given the opportunity to comment on



1 problems with the current standards, the focus of and framework for the revised standards, and an  
2 early draft of the functional requirements for the revised standards.

3 The proposed revised standards separate the original performance standards and test criteria,  
4 which had been presented together as one large volume, into two volumes to better suit the needs  
5 of different user groups. "Volume I: Voting System Performance Standards" provides an  
6 introduction to the standards, describes the functional and technical requirements for voting  
7 systems, and includes a summary of the testing process. "Volume II: Voting System Test  
8 Standards" will provide details of the test process in terms of information to be submitted by the  
9 vendor, testing conducted by the independent test authorities, and criteria for passing the  
10 individual tests of the test process.

11 To improve readability, the revised performance standards also have been reorganized to  
12 clearly identify individual elements as either mandatory requirements or recommended guidelines  
13 or practices. They focus on voting system functionality, identifying requirements common to all  
14 types of voting systems and those that apply only to subclasses of voting systems (e.g.; paper  
15 based versus all electronic, central count versus precinct count).

16 The proposed performance standards provide expanded coverage of certain automated  
17 election management functions that interface with vote recording and tabulating systems; both on  
18 the front end during the preparation of ballots and the election-specific coding of software and on  
19 the back end during vote consolidation and reporting. They augment coverage of system  
20 requirements for feedback to the voter, audit trails, telecommunications, security, and the  
21 documentation of vendor quality assurance practices. They also provide new coverage for  
22 Internet voting, the accessibility aspects of voting systems, and the documentation of the  
23 vendor's process for managing voting system development and changes.

1 The proposed performance standards no longer describe fundamental professional systems  
2 development processes. They do not address election practices and procedures that are not under  
3 the control of the vendor, although vendors will be required to document actions, materials, and  
4 environmental considerations necessary to properly secure, use, transport, and maintain their  
5 specific voting systems. This version of the standards also does not address many specific  
6 human interface considerations, except for the accessibility of information technology  
7 components to the disabled and some general provisions for ballot presentation, feedback to the  
8 voter, and warning signals. The FEC has requested funds to enhance existing documents and  
9 develop new ones to address these matters.

0 The proposed performance standards also do not cover election administration databases and  
1 information technology that are not involved in ballot preparation, election coding of software,  
2 vote recording and tabulation, or vote consolidation and reporting (e.g.; databases used to  
3 manage voter registration, absentee balloting requests, precinct boundaries, poll worker  
4 remuneration, etc.). Further discussion of the reasons for these exclusions is contained in the  
5 Overview document that accompanies the proposed standards.

6 The FEC is now making the draft "Volume I: Voting System Performance Standards"  
7 available for comment. This fall, the Commission plans to publish a notice in the Federal  
8 Register to announce when the draft "Volume II: Voting System Test Standards" is available for  
9 comment. The Commission will evaluate comments received to both volumes to determine what  
0 additional refinements are warranted. Following this process, a notice will be published in the  
1 Federal Register announcing the availability of the final documents. Assuming a continuous  
2 funding stream, the Commission anticipates a final issuance date no later than April 2002 and

1 will recommend to the States, voting system vendors, and independent test authorities an  
2 effective date of July 1, 2002.

3 Electronic Access and Filing Addresses

4 Comments may be submitted by sending electronic messages to VSS@fec.gov. The FEC  
5 also accepts comments in electronic mail attachments and on disk that are in Word 5.0, or earlier  
6 version, file format. Commenters should avoid the use of special characters or encryption.

7 Persons sending comments by electronic mail must include their full name, electronic mail  
8 address and postal service address within the text of their comments. Comments that do not  
9 contain the full name, electronic mail address and postal service address of the commenter will  
10 not be considered.

11  
12  
13  
14 Danny L. McDonald  
15 Chairman  
16 Federal Election Commission  
17

18 DATED: \_\_\_\_\_  
19 BILLING CODE: 6715-01-P





# NASED

## Updating the Voting Systems Performance and Test Standards: An Overview

### Background

The program to develop and implement performance and test standards for electronic voting equipment is over 25 years old. National interest in this program has been renewed recently as a result of the circumstances surrounding the 2000 Presidential election.

In 1975, the National Bureau of Standards (now the National Institute of Standards and Technology) and the Federal Election Commission's (FEC's) predecessor at the General Accounting Office produced a joint report entitled *Effective Use of Computing Technology in Vote Tallying*. This report concluded that one of the basic causes of computer-related election problems was the lack of appropriate technical skills at the state and local level to develop or implement sophisticated and complex written standards, against which voting system hardware and software could be tested. A subsequent Congressionally-mandated feasibility study and report, produced by the FEC and the National Bureau of Standards, cited a significant number of technical and management problems affecting the integrity of the vote-counting process. It 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 their testing, certification, and procurement of computer-based voting systems.

In 1984, Congress appropriated funds directing the FEC to begin development of voluntary national standards for computer-based voting systems. Subsequently, more than 130 state and local election officials, independent technical experts, election systems vendors, Congressional staff, and others attended numerous public hearings and reviewed the proposed criteria for the draft standards. Prior to final issuance, the FEC published the draft standards in the *Federal Register* and requested interested parties to submit their final comments. After reviewing all responses and incorporating corrections and suitable suggestions, the FEC formally approved the Performance and Test Standards for Punchcard, Marksense and Direct Recording Electronic Voting Systems<sup>1</sup> in January 1990.

---

<sup>1</sup> This document is generally referred to as the *Voting Systems Standards (VSS or Standards)*

Following publication of the Standards, the National Association of State Election Directors (NASED) established a process by which vendors could submit their equipment to Independent Test Authorities (ITAs) for evaluation against the national standards. Wyle Laboratories and Metamore Technologies were certified by NASED to serve as program ITAs for testing hardware and examining software. NASED also continues to encourage other qualified testing facilities to request ITA certification. The national testing effort is overseen by NASED's Voting Systems Board (*See Attachment A,*) which is composed of election officials and independent technical advisors. The FEC's Director of the Office of Election Administration (OEA) and representatives from Wyle and Metamore serve as ex-officio members. The Executive Director of the Election Center, a non-governmental membership organization, serves as Secretariat to the Board.

Since its initiation in 1994, more than 30 voting systems, or components of voting systems, have gone through the NASED testing and qualification process. In addition, many systems have been certified at the state level using the VSS outside the boundaries of the formal NASED program.

As the qualification process matured and tested systems were used in the field, the Voting Systems Board, in consultation with the ITAs, identified certain testing issues that needed to be resolved. At the same time, technological advancements introduced new scenarios not contemplated by the original standards. Internet voting systems, in particular, and the accompanying challenges to voter privacy, security and overall system integrity, commanded specific attention in the standards.

During a 1997 briefing, NASED members urged FEC Commissioners to authorize the OEA to address the issues raised by the ITAs and to update the Standards. Following a 1998-1999 Requirements Analysis, the Commission approved the first revision of the Voting System Standards and dedicated resources from other programs to ensure its timely completion.

## **Issues Addressed by the Revised Standards**

The primary goal of the VSS—to provide a vehicle for state and local election officials to assure the public of the integrity of computer-based election systems—has remained unchanged since 1990. The methods for achieving this goal have, however, broadened over the last decade.

The updated Standards provide a common set of requirements across all voting technologies, using technology-specific requirements only where essential to address impacts on voting accuracy, integrity, and reliability unique to a particular technology. The original VSS classified systems as either Punchcard and Marksense (P&M) or Direct Recording Electronic (DRE) and defined separate standards for each technology. The revised Standards focus on technology specific standards for two separate categories: *paper-based* voting systems and *electronic-based* voting systems.

Paper-based systems encompass both punchcards and optically marked and scanned ballots. Electronic systems include a broad range of systems that directly record votes electronically, such as those that use touch screens and/or keyboards to record votes. Internet voting systems are addressed as a subcategory of electronic systems that transmit individual votes over the Internet.

The revised Standards provide new or expanded coverage of the following functional and technical system capabilities:

### **Election Management Functions**

Performance requirements are specified for 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.

### **Feedback to Voter**

Performance requirements are defined for electronic voting devices and for precinct-based vote counting devices that provide direct feedback to the voter, indicating contests where an under-vote or over-vote is detected.

### **Accessibility**

Performance requirements are defined for systems that use electronic information technology to enable voters with disabilities to cast ballots and election officials with disabilities to operate systems without assistance. These requirements are based on the accessibility standards for Electronic and Information Technology (EIT) established in *36 CFR Part 1194 - Electronic and Information Technology Accessibility Standards*, which implement Section 508 of the Rehabilitation Act Amendments of 1998. The requirements apply to all electronic voting systems, including Internet voting systems, and ballot scanning and counting equipment for paper-based systems. Of particular note, precinct-based electronic voting devices and ballot scanning and counting equipment for paper-based ballots are subject to the specific requirements of Subpart B, Section 1194.25 for self-contained closed products.

### **Audit Trails**

Performance requirements for audit trails are strengthened to address the full range of election management functions, including such functions as ballot definition and election programming.

### **Telecommunications**

Performance requirements are defined for hardware and software components of voting systems that carry voting related information between devices at a single site (e.g., individual voting machine and vote-counting device for a direct recording electronic voting system), as well as between sites (e.g., between poll sites and central vote count facilities). Specific prohibitions are included for various types of information that are not permitted to be communicated/transferred via telecommunications at any time due to the limits of existing technology to prevent unauthorized use of data. Systems must be designed to provide the secure transfer of information, such as: requests for Internet voting submitted by individual voters to a jurisdiction; registry of voter keys and/or voter PINs to any person, including the voter (such as to authenticate himself/herself to cast a ballot over the Internet); the Election Management Database; ballot definition programs and databases; ballot installation and programming; system programming and software installation; pre-election test programs; and voting device or system audit logs.

### **Broadcasting of Unofficial Results**

Performance requirements are defined for the content and labeling of data provided to the media and other organizations (in reports, data files, or postings to election office Web sites) prior to the canvass and certification of election results.

### **Internet Voting**

Performance requirements for systems that provide for casting ballots over the Internet are defined for poll site systems which enable casting ballots only from locations and equipment controlled by election officials, and for remote site systems that enable voters to cast ballots using the Internet. Requirements for Internet voting systems are set to assure that these systems are as accurate, reliable and secure as other forms of voting systems, and will likely require advanced technology to be achieved. Specific requirements are defined for attributes such as system availability, vote accuracy and integrity, vote privacy, ballot presentation, ballot acceptance and storage at the server, and security.

### **Time Limited Qualification**

Generally, a voting system remains qualified as long as no modifications are made to the system that have not been submitted to, and tested by, a certified ITA. The qualification remains valid for as long as the voting system remains unchanged. However, voting systems that transmit live system data using public networks, including all forms of Internet voting systems, are subject to an additional requirement that recognizes that the risks and threats to system availability and



integrity increase over time, and system capabilities that may have been adequate at one point in time may no longer be sufficient. For systems that transmit live data using public networks (as defined in Section 5) the qualification is valid only for a single year, and the system must be re-qualified annually. The re-qualification tests will focus on whether the system provides sufficient capabilities to fully meet the security requirements of Section 5 with respect to risks and threats that have been identified since the previous qualification testing for the system.

The revised VSS also provide a restructured and expanded description of the tests performed by the ITAs, addressing:

### **Expanded Testing Standards**

Additional tests are defined to address the expanded functional and technical requirements for voting systems.

### **Stages in the Test Process**

The test process is re-defined in terms of pre-testing, testing, and post-testing activities.

### **Distinction Between Initial Tests and Testing of Modifications to Previously Tested Systems**

The extent of testing required for system changes depends on the nature of the changes. Criteria for determining the scope of testing for modifications are defined.

### **Documentation Submitted by Vendors**

The description of documentation provided by vendors as part of the Technical Data Package is refined to support the collection of all information required by the ITAs to conduct the expanded testing.

Finally, the standards have been reorganized and edited to better suit the needs of different user groups and to improve readability. These changes include:

### **Multiple Volumes**

While the original VSS was published as a single document, the update is divided into two distinct volumes. *Volume I, Voting System Performance Standards*, provides an introduction to the Standards, describes the functional and technical

requirements for voting systems, and provides a summary of the testing process. This volume is intended for a general audience, including the public, the press, state and local election officials and prospective vendors, as well as the ITAs and current vendors already familiar with the Standards and the testing process. *Volume II, Voting System Test Standards*, is written more specifically for jurisdictions purchasing a new system, vendors and ITAs. This volume provides details of the test process in terms of the information to be submitted by the vendor to support testing, the development of test plans by the ITAs for initial system testing and the testing of modifications to the system, the conduct of system qualification tests by the ITAs and the test reports generated by the ITAs.

### **Standards, Guidelines and Fundamental System Development Techniques**

The revised Standards clearly identify individual elements as mandatory requirements or recommended guidelines or practices. Volumes I and II no longer provide descriptions of basic professional system development and management techniques included in the current version of the VSS. They do, however, provide references to common industry practices and, for some topics, such as quality assurance and configuration management, require vendors to submit documentation of their processes.

### **Inclusion of Selected Test Procedure Details**

Although the details of test procedures continue to be developed by the ITAs, consistent with the test process and standards defined in VSS Volumes I and II, the standards continue to specify the procedure for certain hardware tests for voting and vote-counting devices in Volume II.

## **Issues Not Addressed by the Revised Standards**

A number of important issues are not addressed by the revised Standards. As indicated below, some are outside the scope of the VSS. Others will be addressed in the future. Each issue, and the reason for its exclusion, is discussed below.

### **Administrative Functions**

The revised Standards do not address administration and management practices, other than those under the direct control of the vendor. Election officials have long recognized that adequate standards and test criteria are only part of the formula for ensuring that votes are cast and counted in an accurate manner. The other key

component, and one that is often overlooked in the rush to embrace technological solutions to election problems, is administration and management. While effective administration at the local level requires the adoption and implementation of consistent and effective procedures for acquiring, securing, operating and maintaining a voting system, such procedures are not properly included in a standards document focusing on the system itself. Subject to Congressional funding, the FEC intends to fill this void by producing a companion document outlining recommended procedural guidelines for the administration of computerized voting systems.

### **Integration with the Voter Registration Database**

Local and statewide automated voter registration databases have become more common in recent years as election officials throughout the country attempt to harness innovations in network computing to solve the problems posed by increasingly complex voter registration information requirements. In some instances, a voter registration database will contain many data fields common to other election administration applications. These applications can include campaign finance recording, election worker management, and the reporting of election results. Although many of these applications are co-dependent, the testing of the design and interface, if it exists, between the voting system and the voter registration database has been specifically excluded from this update of the Standards. This decision was made for practical reasons. Because there is such a variety of databases and interfaces being used, not only among the various states, but often within individual states as well, there appeared to be no practical and systematic way such testing could be accomplished. In addition, many of the voting systems being used today still do not include an electronic interface with the voter registration database. If and when the majority of voting systems and voter registration databases become more seamlessly integrated, a module will be added to the VSS covering their performance, functionality and testing.

### **Commercial Off-the-Shelf (COTS) Products**

The exclusions described for COTS products have two purposes: (1) to make use of existing professional standards that meet the requirements for voting systems, and minimize the cost and time that would be required for duplicative system testing; and (2) to avoid prescribing standards for system components that have no material impact on the ability of the system to support voting functions.

**HARDWARE** - Like the original VSS, the update continues to exclude from parts of the testing process certain commercially-available hardware that is commonly used and has proven reliable over a period of time. The update re-defines these products as 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. Also excluded are 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. A final hardware testing exclusion is permitted for 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 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).

**SOFTWARE** - Also excluded from certain aspects of software testing are general purpose non-voting software (e.g., operating systems, programming language compilers, database management systems, web browsers) and other software components that are resident on a vote recording or counting device but which do not operationally support any voting related activities, including components that are bypassed or disabled during processing for any voting related activities.

#### **Detailed Human Interface and Usability Standards**

The recent controversy over the design of the Presidential ballot in certain jurisdictions has highlighted the importance of ballot design and system usability to both election officials and the general public. As mentioned earlier, the updated VSS cover design and usability in a detailed manner as it pertains to disabled voters. Human interface and usability issues for the general voting public are addressed in standards for ballot formatting, which require such things as the uniform allocation of space and fonts, the simultaneous display of all choices for a single contest on one page, and easy navigation of multi-page ballots. Both NASED and the FEC recognize, however, that neither the original VSS, nor the update, do an adequate job of developing detailed test standards for interface and usability. It is contemplated that the next module to be added to the VSS will focus on interface and usability issues, including, but not limited to, such things as typography, layout, use of graphic elements, sequencing, screen flow (for electronic and internet systems), language simplification, and user testing.

#### **Human Error Rate**

The term "error rate", as defined by the VSS, does not apply to the accuracy of a voting system or components of that system with respect to the incidence of voter error, such as the failure to mark a ballot in accordance with instructions. The updated accuracy standard is defined in terms of a character error rate, that is, the

acceptable error rate for letters, numbers, symbols and other markings that are recorded, stored and reported by the voting system. For example, each contest on a ballot, each candidate's name, and the text of a ballot proposition consist of multiple letters or characters. Each location on a paper ballot card or electronic ballot image where a vote may be entered represents a character. The minimum acceptable error rate for all hardware components is one in one million characters. This system error rate applies to data that is entered into the system, or a particular component, in conformance with the applicable instructions and specifications. Further research on human interface and usability issues is needed to enable the specification of standards for system error rates that encompass human error.

## Summary of VSS Content

The summary provided below addresses the content of *Volume 1*, only. It is intended to provide an overview of the subject matter in each section of the volume, to identify the most significant revisions and to provide information about individual standards of particular interest. A summary of the content of *Volume 2* will be included upon completion of that document.

### Section 1- Introduction

This section provides an introduction to the VSS, addressing the following topics:

- Objectives and usage of the VSS;
- Development history for initial VSS;
- Update of the VSS;
- Accessibility for individuals with disabilities;
- Definitions of key terms;
- Application of the standards and test specifications; and
- Outline of contents.

### Section 2 - Functional Capabilities

This section describes the functional capabilities required of all voting systems. These capabilities are predominantly independent of technology. They represent acceptable levels of combined hardware and software function, commensurate with overall system requirements for functionality, speed, accuracy, reliability, and audit capability. The functional capabilities are defined in terms of specific standards that include all operations necessary to support the following three phases of election activity and specify more general requirements:

**Pre-voting** - Standards are defined for ballot preparation; the preparation of election-specific software or firmware; the production of ballots or ballot pages; the installation of ballots and ballot counting software or firmware; and system and equipment tests. The updated VSS expand and address in greater detail the

requirements for pre-voting processing. As in the original version, the revised VSS do not address activities related to candidate nomination and inclusion on the ballot, or voter registration.

**Voting** - Standards are defined for all operations conducted at the polling place by voters and officials, including the generation of status messages.

**Post-voting** - Standards are defined for closing the polling place; obtaining reports by voting machine, polling place, and precinct (central count systems); obtaining consolidated reports; and obtaining reports of audit trails.

**General Requirements** - Standards are defined for: accessibility; security; accuracy and integrity; election management activities; the vote tabulating program; telecommunications; and data retention and audit trails. Standards are also defined for the capabilities necessary to maintain voting system equipment and, for precinct count systems, to transport and store the equipment.

Recognizing the diversity of voting systems and the technologies they employ, the functional capabilities are structured to apply specific standards to the appropriate technologies. Some of these standards apply only if the system incorporates certain optional functions (for example, voting systems employing telecommunications to transmit voting data.). Internet voting systems are addressed as a form of electronic voting system and are subject to the Standards for an electronic voting system and additional standards that address unique characteristics of casting individual ballots over the Internet.

The requirement that voting systems provide access to individuals with disabilities is one of the most significant VSS revisions. The specific requirements are based on the accessibility standards for electronic and information technology (EIT) established in *36 CFR Part 1194 - Electronic and Information Technology Accessibility Standards*, which implement Section 508 of the Rehabilitation Act Amendments of 1998. Of particular note, electronic voting devices are subject to the specific requirements of Subpart B, Section 1194.25 for self-contained closed products.

### **Section 3 - Hardware Standards**

This section describes the performance characteristics, physical characteristics, and design, construction and maintenance characteristics for the hardware and selected related components of voting systems. 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 and ballots—ballot displays, ballot recorders, and precinct vote control units;

- Voting devices—including punching and marking devices and electronic recording devices;
- Voting booths and enclosures;
- Computers 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.

For vote recording devices used as part of an Internet voting system, the standards contained in this section also apply to:

- General purpose devices (such as personal computers) acquired by the jurisdiction for the purpose of poll-site Internet voting;
- General purpose devices acquired by others (such as school systems, libraries, military installations and other public organizations) for the purpose of voting at sites supervised by election officials; and
- Devices designed solely for remote Internet voting by individuals.

This section is not intended to apply to multi-purpose devices, such as personal computers (PCs) and personal data assistants (PDAs) owned by the voter or third persons (e.g., employer, library, hotel, college,) which are utilized for remote Internet voting at uncontrolled locations. However, these devices, as well as those utilized at controlled voting locations, are subject to the security requirements of Section 6.

The standards defined in this section specify the minimum values for the relevant attributes of hardware. These attributes include: 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; controls; susceptibility to interference from static electricity and magnetic fields; human engineering; product marking; and safety.

#### **Section 4- Software/Firmware Standards**

This section describes the design and performance characteristics of the software embodied in voting systems, addressing both system-level software, such as operating systems, 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 standards described also influence hardware design for 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;
- Software furnished by an external provider (for example, providers of commercial off-the-shelf (COTS) operating systems and web browsers) where the software is potentially used in any way during voting system operation; and
- Software developed by the voting jurisdiction.

This section provides general requirements and specific requirements. The general requirements apply to software used to support the broad range of voting system activities, including pre-voting, voting and post-voting activities. The specific standards encompass ballot counting, vote processing, the creation of an unalterable audit trail, and the generation of output reports and files.

In addition to the standards defined in this section, voting system software is subject to the security requirements of Section 6.

### **Section 5 - Telecommunications Standards**

This section describes the performance, design and maintenance characteristics of the telecommunications components of voting systems and defines the acceptable levels of performance against these characteristics. For VSS purposes, telecommunications is defined as the capability to transmit and receive data electronically over a distance using hardware and software components, including data transmission between a voting device and a central vote processing unit.

The requirements specified in this section represent acceptable levels of function and performance for the transmission of data that is used to operate the system and report official election results. This section, where applicable, specifies minimum values for critical performance and functional attributes involving telecommunications hardware and software components, addressing attributes such as accuracy/integrity, availability, privacy, confirmation, reliability, durability, maintainability, and response time.

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.

This section addresses telecommunications hardware and software across a broad range of technologies including, but not limited to, dial-up communications technologies, high-speed telecommunications lines (public and private), various



cabling technologies, communications routers, modems, modem drivers, dial-up networking software, channel service units (CSU)/data service units (DSU), and dial-up networking applications software.

This section applies to transmissions over public networks, such as those provided by regional telephone companies and long distance carriers, as well as private networks that may be employed by a jurisdiction. This section also applies to private networks that transmit data between facilities (e.g., polling place and central office) regardless of whether the network is owned and operated by the election jurisdiction or by a third party, such as a telecommunications company under contract to the jurisdiction.

For systems that transmit data over public networks, including Poll Site Internet Voting Systems, this section applies to telecommunications components that are to be installed and operated at settings supervised by election officials, such as traditional polling places, and the central office.

### **Section 6 - Security Standards**

This section describes the essential security capabilities for a voting system, encompassing the system's hardware, software, communications, and documentation. The standards of this section recognize that no predefined set of security capabilities is capable of defeating all conceivable or theoretical threats, while focusing on achieving an acceptable level of confidence in the integrity, reliability, and inviolability of the election process. Ultimately, the objectives of the security standards for voting systems are to:

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

The security 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, these 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;
- Maintaining 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 individual.

### **Section 7 - Quality Assurance**

The VSS views quality assurance as a vendor function with associated practices that confirm throughout the system development and maintenance life cycle that a voting system conforms with the Standards and state and local requirements. 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 and submitting documentation for a quality assurance program to ensure that the design, workmanship, and performance requirements of this standard are achieved in all delivered systems and components. These responsibilities:

- Include procedures for specifying and procuring parts and raw materials of the requisite quality, and for their inspection, acceptance, and control.
- Require the documentation of the hardware and software development process.
- Identify and enforce all requirements for in-process inspection and testing which the manufacturer deems necessary to ensure proper fabrication and assembly of hardware; and installation and operation of software or firmware.
- Include a procedure for maintaining all data and records required to document and verify the quality inspections and tests.
- Include a procedure for maintaining records of errors and defects reported by state authorities and local jurisdictions.

### **Section 8 - Configuration Management**

This section contains specific requirements for configuration management of voting systems. For VSS purposes, configuration management is defined as a set of activities and associated practices that assures 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 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, auditing, and reporting activities that 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.

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 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 VSS 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 which, 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 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 for the testing of modifications and re-qualification after a system has been qualified.

The testing described in this section is performed by an ITA that is 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 ITAs at any point in time. Five types of focuses guide the overall testing process:

- Absolute logical 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 character error rate (for which the maximum acceptable error rate is one in one million characters);
- Operational failure(s) 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.

The scope of system testing during re-qualification will often be less extensive than that for initial qualification. The ITA will determine the types of tests necessary for re-qualification 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.

## Conclusion

Thirty-seven States have adopted, or intend to adopt, the Voting Systems Standards. While the Commission recognizes that State adoption has taken various forms of implementation, it continues to recommend that individual States need to decide how best these performance standards be applied to future procurements.

Adoption of the VSS by the states, coupled with NASED's national testing program, will ensure accurate and reliable voting systems nation-wide. As the requirements for voting systems and the technologies used to build them have evolved over the past decade, the revised VSS have effectively closed the gaps in the Standards for system performance and testing. In order to prevent technology gaps in the future, the FEC and NASED are committed to making the VSS an ongoing project, capable of being updated in an expedited manner to respond to constantly changing technology which will invariably be incorporated into automated voting systems.

---

**NASED**  
**VOTING SYSTEMS/INDEPENDENT TEST AUTHORITY**  
**ACCREDITATION BOARD**

**Thomas R. Wilkey, Chair**  
Executive Director  
New York State Board of Elections  
Albany, New York

**David Elliott, Asst. Director of Elections**  
Office of the Secretary of State  
Olympia, Washington

**Robert Naegels, President**  
Granite Creek Technology  
Pacific Grove, California

**James Hendrix, Executive Director**  
State Election Commission  
Columbia, South Carolina

**Brit Williams, Professor**  
CSIS Dept, Kennesaw State College  
Kennesaw, Georgia

**Denise Lamb, Director**  
State Bureau of Elections  
Santa Fe, New Mexico

**Paul Craft, Computer Audit Analyst**  
Florida State Division of Elections  
Tallahassee, Florida

**Sandy Steinbach, Director of Elections**  
Office of Secretary of State  
Des Moines, Iowa

**Steve Freeman, Software Consultant**  
League City, Texas

**Donetta Davidson,**  
Secretary of State  
Denver, Colorado

**Jay W. Nispel, Senior Principal Engineer**  
Computer Sciences Corporation  
Annapolis Junction, Maryland

**Connie Schmidt, Commissioner**  
Johnson County Election Commission  
Olathe, Kansas

**Yvonne Smith (Member Emeritus)**  
Former Assistant to the Executive Director  
Illinois State Board of Elections  
Chicago, Illinois

**Ex Officio:**

**Penelope Bonsall, Director**  
Office of Election Administration  
Federal Election Commission  
Washington, D.C.

**Jim Dearman**  
Wyle Laboratories  
Huntsville, Alabama

**Shawn Southworth**  
**Jennifer Price**  
Metamore  
Huntsville, Alabama

**Committee Secretariat:**

**The Election Center**  
**R. Doug Lewis, Executive Director**  
Houston, Texas  
Tele: 281-293-0101  
Fax: 281-293-0453  
email: [electioncent@pdq.net](mailto:electioncent@pdq.net)



# **Voting System Standards Volume 1: Performance Standards**

**June 13, 2001  
DRAFT**



**Federal Election Commission  
United States of America**





# Table of Contents

---

<b>1 Introduction</b> .....	<b>1-1</b>
1.1 Objectives and Usage of the Voting System Standards .....	1-1
1.2 Development History for Initial Standards.....	1-2
1.3 Update of the Standards.....	1-3
1.4 Accessibility for Individuals with Disabilities.....	1-4
1.5 Definitions .....	1-5
1.5.1 Voting System .....	1-5
1.5.2 Paper Vote Based Voting System .....	1-5
1.5.3 Electronic Voting System.....	1-6
1.5.4 Internet Voting System.....	1-7
1.6 Application of the Standards and Test Specifications.....	1-8
1.6.1 Qualification Tests.....	1-9
1.6.2 Certification Tests.....	1-10
1.6.3 Acceptance Tests.....	1-11
1.7 Outline of Contents .....	1-11
<b>2 Functional Capabilities</b> .....	<b>2-1</b>
2.1 Scope.....	2-1
2.2 Overall System Capabilities .....	2-2
2.2.1 Security .....	2-2
2.2.2 Accuracy and Integrity .....	2-3
2.2.2.1 Vote Accuracy Measures.....	2-3
2.2.2.1.1 Common Standards.....	2-3
2.2.2.1.2 Electronic System Standards.....	2-4
2.2.2.2 Integrity Measures .....	2-4
2.2.2.2.1 Common Standards.....	2-4
2.2.2.2.2 Electronic Systems Standards .....	2-4
2.2.3 System Audit .....	2-5
2.2.3.1 System Audit Purpose and Context.....	2-5
2.2.3.2 Operational Requirements.....	2-6
2.2.3.2.1 Time, Sequence, and Preservation of Audit Records .....	2-6

- 2.2.3.2.2 Error Messages.....2-7
      - 2.2.3.2.3 Status Messages.....2-7
    - 2.2.4 The Election Management System.....2-8
    - 2.2.5 Accessibility .....2-8
      - 2.2.5.1 Scope and Applicability .....2-9
      - 2.2.5.2 Technical Standards .....2-10
      - 2.2.5.3 Functional Performance Criteria.....2-10
      - 2.2.5.4 Information, Documentation and Support.....2-10
    - 2.2.6 Vote Tabulating Capabilities .....2-10
    - 2.2.7 Telecommunications.....2-11
    - 2.2.8 Retention of Data.....2-12
  - 2.3 Pre-voting Functions .....2-14
    - 2.3.1 Ballot Preparation .....2-14
      - 2.3.1.1 General Capabilities.....2-14
        - 2.3.1.1.1 Common Standards .....2-15
        - 2.3.1.1.2 Paper Based System Standards .....2-15
      - 2.3.1.2 Ballot Formatting.....2-15
      - 2.3.1.3 Ballot Production.....2-16
    - 2.3.2 Election Programming .....2-17
    - 2.3.3 Ballot and Program Installation.....2-17
    - 2.3.4 Readiness Testing.....2-18
    - 2.3.5 Verification at the Polling Place .....2-18
    - 2.3.6 Verification at the Central Location.....2-19
      - 2.3.6.1 Verification Standards.....2-19
      - 2.3.6.2 Test Data .....2-19
      - 2.3.6.3 Data Verification Reporting .....2-19
  - 2.4 Voting Functions .....2-19
    - 2.4.1 Opening the Polls .....2-20
      - 2.4.1.1 Paper Based System Standards .....2-20
      - 2.4.1.2 Electronic System Standards .....2-20
    - 2.4.2 Activating the Ballot (Electronic Systems) .....2-21
    - 2.4.3 Casting a Ballot.....2-21
      - 2.4.3.1 Common Standards.....2-21
      - 2.4.3.2 Paper Based Systems Standards .....2-22
        - 2.4.3.2.1 All Paper-Based Systems.....2-22
        - 2.4.3.2.2 Precinct Count Paper-Based Systems .....2-22
      - 2.4.3.3 Electronic Systems Standards .....2-22

2.4.3.4 Internet Voting Systems Standards .....	2-23
2.4.4 Augmenting the Election Counter (for Paper-based Systems) .....	2-24
2.4.5 Augmenting the Life Cycle Counter (for Paper-based Systems) .....	2-25
2.5 Post-Voting Functions .....	2-25
2.5.1 Closing the Polling Place (Precinct Count) .....	2-25
2.5.2 Closing the Polling Place (Internet Voting Systems) .....	2-26
2.5.3 Obtaining Polling Place Reports (Precinct Count) .....	2-26
2.5.4 Obtaining Precinct Reports Jurisdiction-wide (Central Count) .....	2-27
2.5.5 Obtaining Consolidated Reports or Results .....	2-27
2.5.6 Consolidation of Absentee Ballots .....	2-27
2.5.7 Consolidation of Internet Ballots .....	2-28
2.5.8 Broadcasting Results .....	2-28
2.6 Maintenance .....	2-28
2.7 Transportation and Storage (Precinct Count) .....	2-28
<b>3 Hardware Standards .....</b>	<b>3-1</b>
3.1 Introduction .....	3-1
3.1.1 Scope .....	3-1
3.1.2 Organization of this Section .....	3-2
3.2 Performance Requirements .....	3-3
3.2.1 Environmental Requirements .....	3-4
3.2.1.1 Shelter Requirements .....	3-4
3.2.1.2 Space Requirements .....	3-4
3.2.1.3 Furnishings and Fixtures .....	3-4
3.2.1.4 Electrical Supply .....	3-4
3.2.1.5 Environmental Control .....	3-5
3.2.1.6 Data Networks Guidelines .....	3-5
3.2.2 Control Requirements .....	3-5
3.2.2.1 Equipment Preparation .....	3-6
3.2.2.2 Pre-Election Testing .....	3-6
3.2.2.3 Tests at the Polling Place .....	3-6
3.2.2.4 Tests at Central Counting Facilities .....	3-7
3.2.2.5 Opening the Polling Place (Precinct Count Systems) .....	3-7
3.2.2.6 Activating a Ballot (Electronic Systems) .....	3-7
3.2.2.7 Error Recovery (Precinct Count System) .....	3-8
3.2.2.8 Closing the Polling Place .....	3-8
3.2.2.9 Polling Place Reports .....	3-8

3.2.3 Election Management System Requirements .....	3-9
3.2.3.1 Recording Accuracy .....	3-9
3.2.3.2 Memory Stability .....	3-9
3.2.4 Vote Recording Requirements .....	3-10
3.2.4.1 Paper Based Recording Requirements .....	3-10
3.2.4.1.1 Ballot Standards .....	3-10
3.2.4.1.2 Punching Devices .....	3-10
3.2.4.1.3 Marking Devices .....	3-11
3.2.4.1.4 Frames or Fixtures for Punchcard Ballots .....	3-11
3.2.4.1.5 Frames or Fixtures for Printed Ballots .....	3-12
3.2.4.1.6 Voting Booths .....	3-12
3.2.4.1.7 Ballot Boxes and Ballot Transfer Boxes .....	3-13
3.2.4.2 Electronic Systems Recording Requirements .....	3-13
3.2.4.2.1 Enclosure .....	3-13
3.2.4.2.2 Activity Indicator .....	3-14
3.2.4.2.3 Vote Recording .....	3-14
3.2.4.2.4 Recording Accuracy .....	3-15
3.2.4.2.5 Recording Reliability .....	3-15
3.2.4.2.6 Public Counter .....	3-15
3.2.4.2.7 Protective Counter .....	3-16
3.2.5 Paper Based Conversion Requirements .....	3-16
3.2.5.1 Ballot Handling .....	3-16
3.2.5.1.1 Outstacking .....	3-17
3.2.5.1.2 Multiple Feed Prevention .....	3-17
3.2.5.2 Ballot Reading .....	3-17
3.2.5.2.1 Reading Accuracy .....	3-18
3.2.5.2.2 Reading Reliability .....	3-18
3.2.6 Processing Requirements .....	3-18
3.2.6.1 Paper Based System Processing Requirements .....	3-19
3.2.6.1.1 Processing Accuracy .....	3-19
3.2.6.1.2 Memory Stability .....	3-19
3.2.6.2 Electronic System Processing Requirements .....	3-20
3.2.6.2.1 Processing Speed .....	3-20
3.2.6.2.2 Processing Accuracy .....	3-20
3.2.6.2.3 Memory Stability .....	3-20
3.2.7 Reporting Requirements .....	3-21
3.2.7.1 Removable Storage Media .....	3-21

3.2.7.2 Communication Devices .....	3-21
3.2.7.3 Printers .....	3-21
3.2.8 Vote Data Management Requirements .....	3-22
3.2.8.1 Data File Management .....	3-22
3.2.8.2 Data Report Generation .....	3-22
3.3 Physical Characteristics .....	3-22
3.3.1 Size .....	3-23
3.3.2 Weight .....	3-23
3.3.3 Transport and Storage of Portable Systems .....	3-23
3.3.4 Security .....	3-24
3.3.5 Transportability .....	3-24
3.4 Design, Construction, and Maintenance Characteristics .....	3-24
3.4.1 Materials, Processes and Parts .....	3-24
3.4.1.1 Ballot Cards .....	3-25
3.4.1.2 Ballot Printing .....	3-25
3.4.1.2.1 Punchcard Ballots .....	3-25
3.4.1.2.2 Marksense Ballots .....	3-25
3.4.1.3 Punching Stylus .....	3-26
3.4.1.4 Vote Recorder .....	3-26
3.4.2 Durability .....	3-26
3.4.3 Reliability .....	3-26
3.4.4 Maintainability .....	3-27
3.4.4.1 Elements of Maintainability .....	3-27
3.4.4.2 Mean Time to Repair (MTTR) Guidelines .....	3-28
3.4.5 Availability (Ai) .....	3-28
3.4.6 Environmental Conditions .....	3-28
3.4.7 Electromagnetic Radiation .....	3-29
3.4.8 Electrostatic Test (ESD) .....	3-29
3.4.9 Magnetic Susceptibility Test .....	3-29
3.4.10 Product Marking .....	3-30
3.4.11 Workmanship .....	3-30
3.4.12 Interchangeability .....	3-30
3.4.13 Safety .....	3-30
3.4.14 Human Engineering—Controls and Displays .....	3-31
<b>4 Software/Firmware Standards .....</b>	<b>4-1</b>
4.1 Scope .....	4-1

4.1.1 Software Types .....	4-1
4.1.2 Software Sources .....	4-2
4.1.3 Location and Control of Software and Hardware on Which it Operates .....	4-2
4.1.4 Exclusions.....	4-3
4.2 Software Design and Coding Standards .....	4-3
4.3 Data Quality Assessment.....	4-4
4.4 Data and Document Retention.....	4-4
4.5 Audit Record Data.....	4-4
4.5.1 Pre-election Audit Records .....	4-5
4.5.2 System Readiness Audit Records .....	4-5
4.5.3 In-Process Audit Records .....	4-6
4.5.4 Vote Tally Data .....	4-7
4.6 Software for Internet Voting Systems.....	4-8
4.6.1 System Availability and Risk of Failure .....	4-8
4.6.2 Vote Accuracy and Integrity.....	4-9
4.6.3 Vote Privacy.....	4-9
4.6.4 Ballot Presentation.....	4-10
4.6.5 Ballot Acceptance and Storage at the Vote Server.....	4-10
<b>Telecommunications.....</b>	<b>5-1</b>
5.1 Scope.....	5-1
5.1.1 Types of Components.....	5-1
5.1.2 Telecommunications Operations and Providers .....	5-2
5.1.3 Data Transmissions .....	5-3
5.1.4 Organization of Standards .....	5-4
5.2 Performance Requirements .....	5-4
5.2.1 Accuracy/Integrity .....	5-5
5.2.2 Availability.....	5-5
5.2.3 Privacy .....	5-6
5.2.4 Confirmation .....	5-6
5.2.5 Reliability .....	5-6
5.2.6 Durability.....	5-7
5.2.7 Maintainability .....	5-7
5.2.7.1 Elements of Maintainability.....	5-7
5.2.7.2 Mean Time to Repair (MTTR) Guidelines.....	5-8
5.2.8 Response Time.....	5-8

5.3 Prohibitions (Pre-Voting, Voting, and Post Voting) .....	5-9
<b>6 Security Standards.....</b>	<b>6-1</b>
6.1 Scope.....	6-1
6.1.1 System Components and Sources.....	6-2
6.1.2 Location and Control of Software and Hardware on Which it Operates.....	6-2
6.1.3 Application to Internet Voting Systems and Public Telecommunications Networks.....	6-3
6.1.4 Exclusions .....	6-3
6.1.5 Other Elements an Effective Security Program .....	6-4
6.1.6 Organization of this Section.....	6-4
6.2 Access Control.....	6-5
6.2.1 Penetration Analysis.....	6-6
6.2.2 Access Control Policy.....	6-6
6.2.2.1 General Access Control Policy .....	6-6
6.2.2.2 Individual Access Privileges .....	6-7
6.2.3 Access Control Measures.....	6-7
6.3 Equipment and Data Security .....	6-8
6.3.1 Physical Security Measures .....	6-8
6.3.1.1 Polling Place Security.....	6-8
6.3.1.2 Central Count Location Security.....	6-9
6.4 Software and Firmware Installation.....	6-9
6.5 Telecommunications and Data Transmission.....	6-10
6.5.1 Access Control .....	6-10
6.5.2 Data Interception and Prevention .....	6-10
6.5.3 Virus Protection for Third Party Products and Services.....	6-11
6.5.3.1 Identification of Potentially Vulnerable Third Party Products.....	6-11
6.5.3.2 Virus Forms.....	6-11
6.5.3.3 Use of Antivirus Software .....	6-12
6.5.3.4 Update and Maintenance of Antivirus Software.....	6-12
6.5.4 Shared Operating Environment.....	6-12
6.5.5 Access to Incomplete Election Returns and Interactive Queries.....	6-13
6.6 Internet Voting System Security.....	6-14
6.6.1 General Security Requirements for Internet Voting Systems .....	6-14
6.6.2 Vote Server Data Center Requirements for Internet Voting Systems.....	6-15
6.6.3 Voting Process Security for Poll Site Internet Voting Systems .....	6-16
6.6.3.1 Documentation of Security Activities at Poll Site.....	6-16

6.6.3.2 Capabilities to Operate During Denial of Service Attack (Poll Site Internet System Only) .....	6-16
6.6.4 Voting Process Security for Remote Site Internet Voting Systems.....	6-17
6.6.4.1 Request for Internet Balloting.....	6-17
6.6.4.2 Authorization for Internet Ballot.....	6-17
6.6.4.3 Voter Authentication.....	6-18
6.6.4.4 Casting of Votes .....	6-18
6.6.4.5 Transmitting a Ballot to the Vote Server.....	6-19
6.6.4.6 Receipt of a Ballot by the Vote Server.....	6-19
6.6.4.7 Vote Authentication and Separation from Voter Identification .....	6-20
<b>Quality Assurance .....</b>	<b>7-1</b>
7.1 General Requirements .....	7-1
7.1.1 Guidelines.....	7-2
7.2 Responsibility for Tests.....	7-2
7.3 Parts & Materials Special Tests and Examinations.....	7-3
7.4 Quality Conformance Inspections .....	7-3
7.5 Documentation.....	7-3
7.6 Error Notification Reporting Process & Issues Management .....	7-4
<b>Configuration Management .....</b>	<b>8-1</b>
8.1 Introduction .....	8-1
8.1.1 Configuration Management Scope .....	8-1
8.1.2 Configuration Management Benefits .....	8-2
8.1.3 Organization of Configuration Management Standards.....	8-3
8.2 Application of Configuration Management Requirements.....	8-4
8.3 Configuration Management Policy .....	8-4
8.4 Configuration Identification.....	8-5
8.4.1 Structuring and Naming Configuration Items .....	8-5
8.4.2 Versioning Conventions.....	8-5
8.5 Baseline, Promotion, and Demotion Procedures .....	8-5
8.6 Configuration Control Procedures.....	8-6
8.7 Release Process .....	8-6
8.8 Configuration Status Accounting.....	8-7
8.9 Configuration Audits.....	8-7
8.9.1 Physical Configuration Audit.....	8-7
8.9.2 Functional Configuration Audit.....	8-8



8.10 Interface Control .....	8-8
8.11 Configuration Management Resources .....	8-9
<b>9 Overview of Qualification Tests .....</b>	<b>9-1</b>
9.1 Introduction .....	9-1
9.2 Testing Scope .....	9-2
9.2.1 Test Categories .....	9-3
9.2.1.1 Focus of Hardware Tests .....	9-3
9.2.1.2 Focus of Software Evaluation .....	9-4
9.2.1.3 Focus of Telecommunications Tests .....	9-4
9.2.1.4 Focus of Security Tests .....	9-5
9.2.1.5 Focus of Integration Tests .....	9-5
9.2.1.6 Focus of Useability/Accessibility Tests .....	9-5
9.2.1.7 Tests of Ballot Counting Accuracy .....	9-6
9.2.1.8 Sequence of Tests and Audits .....	9-6
9.2.2 Test System .....	9-6
9.3 Applicability .....	9-7
9.3.1 General Applicability .....	9-7
9.3.1.1 Exclusions .....	9-7
9.3.1.2 Software .....	9-8
9.3.2 Modifications to Qualified Systems .....	9-8
9.3.2.1 General Requirements for Modifications .....	9-8
9.3.2.2 Potential for Limited Testing of Modifications .....	9-9
9.3.2.3 Utility Software and/Device Handlers .....	9-10
9.4 Documentation Submitted by Vendor .....	9-10
9.5 Qualification Test Process .....	9-11
9.5.1 Pretest Activities .....	9-11
9.5.1.1 Initiation of Testing .....	9-11
9.5.1.2 Pretest Preparation .....	9-12
9.5.2 Qualification Testing .....	9-12
9.5.2.1 Qualification Test Plan .....	9-12
9.5.2.2 Qualification Test Practices .....	9-13
9.5.2.3 Qualification Test Conditions .....	9-14
9.5.2.4 Qualification Test Data Requirements .....	9-14
9.5.2.5 Qualification Test Fixtures .....	9-15
9.5.2.6 Witness of System Build and Installation .....	9-15
9.5.3 Qualification Report Issuance and Post Test Activities .....	9-15

9.5.4 Time Limited Qualification for Data Transmission Using Public Networks.....9-16

**A Glossary..... A-1**

**B Appendix B ..... B-1**

B.1 Applicable Documents .....B-1

# Table of Contents

---

<b>1 Introduction</b> .....	<b>1-1</b>
1.1 Objectives and Usage of the Voting System Standards .....	1-1
1.2 Development History for Initial Standards .....	1-2
1.3 Update of the Standards .....	1-3
1.4 Accessibility for Individuals with Disabilities.....	1-4
1.5 Definitions .....	1-5
1.5.1 Voting System.....	1-5
1.5.2 Paper Vote Based Voting System.....	1-5
1.5.3 Electronic Voting System .....	1-6
1.5.4 Internet Voting System.....	1-6
1.6 Application of the Standards and Test Specifications.....	1-8
1.6.1 Qualification Tests .....	1-9
1.6.2 Certification Tests .....	1-10
1.6.3 Acceptance Tests .....	1-11
1.7 Outline of Contents .....	1-11



# 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 the risk of voting system failures. The U.S. Congress, responding to calls for assistance from the states, authorized the Federal Election Commission (FEC) to develop national voting systems standards for computer-based systems, but mandated that they be voluntary. The resulting FEC Voting System Standards Project seeks 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, or reject them. States may also choose to enact stricter performance requirements for systems to be used in their jurisdictions.

The standards specify minimum functional requirements, performance characteristics, documentation requirements, and test evaluation criteria. Essentially, they address what a voting system should reliably do, not how the system should meet this requirement. It is not the intent of the standards to impede the design and development of new, innovative equipment by vendors. Furthermore, the standards should not force vendors to price their voting systems out of the range of local jurisdictions.

The standards are not intended to define appropriate election administration practices. The total integrity of the election process, however, can be assured only when the 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:

- a. 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
- b. State or local agencies evaluating voting systems to be procured within their jurisdiction

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

Following the release of this report, the U.S. 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." (See P.L. 96-187.) The resulting 1983 study cited a substantial number of technical and management problems that affected the integrity of the vote counting process. It also detailed the need and desirability of having a federal agency develop national performance standards that might be used as a tool by state and local election officials in their testing, certification, and procurement of computer-based voting systems. In 1984, Congress approved initial funding for the Standards project.

A series of public hearings were held as the initial standards were being developed. State and local election officials, representatives of election system vendors, pro bono technical consultants, and others reviewed drafts of the proposed criteria. The FEC considered their many comments and, where appropriate, made corresponding 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 persons submit their final comments. The FEC meticulously reviewed all responses to the notice and incorporated corrections and suitable suggestions. The final product, therefore, is the result of considerable deliberation, close consultation with election officials, and careful consideration of comments from other interested persons.

In January 1990, the FEC approved for issuance the performance standards and testing procedures for punchcard, marksense, and direct recording electronic voting systems. The Standards did not cover paper ballot and mechanical lever systems. The FEC also did not incorporate requirements for mainframe computer hardware within the hardware standards, since it was reasonable to assume that other engineering and performance criteria govern the operation of mainframe computers. Vote tally software installed on mainframes, however, is covered by the Standards.

## 1.3 Update of the Standards

---

Today, over two thirds of the States have adopted the Standards. As a result, the voting systems now marketed are (even according to their designers) greatly improved. Election officials are better assured that the voting systems they procure will work accurately and reliably. Voting system failures are on the decline, and now tend to involve pre-standard equipment, untested equipment configurations, or the mismanagement of tested equipment. Overall, election process and systems integrity has improved markedly.

However, advances in technology and requirements imposed by new legislation have generated a need to update the Standards. Specifically, electronic voting systems are being purchased in increasing number, and are introducing new hardware and software with the general advancement of information technology. We are now seeing the use of personal computer technology and non-mainframe servers marketed as integral elements of electronic voting systems.

Further, the marketplace is beginning to consider the use of Internet Voting Systems to conduct elections, and the challenges to voting privacy, security and overall system integrity posed by Internet voting. While it is not the purpose of these Standards to advocate the relative merits and risks of different technologies, the Standards are intended to address the operating environment and risks posed by each technology. In part, this update is intended to address current election system technologies that did not exist or were first emerging during the development of the initial Standards.

As new information technologies are introduced to voting systems, the application of quality assurance practices to the design and manufacture of voting systems takes on greater importance to assure that errors are found and corrected prior to system deployment. Similarly the application of rigorous configuration management practices takes on increasing importance to assure that the configuration of components in each voting system is well documented; configurations are changed subject to specific controls; and the version of each system delivered to customers has met state qualification and or certification requirements. This update of the Standards substantially strengthens the provisions for quality assurance and configuration management.

In addition, voting systems now need to be responsive to the provisions of Section 504 of the Americans with Disabilities Act (ADA) of 1990 and guidelines developed to assist in implementing ADA. This update of the Standards is intended to address the need to provide voters with disabilities effective access to the voting system and the ability to vote without assistance.

## 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, or find it impossible, to use traditional voting systems. This updated version of the Standards requires that voting systems provide accessibility to individuals such that they may vote or serve in an election administration capacity without assistance. The requirements address a broad range of disabilities, including those relating to vision, hearing, cognitive abilities, physical mobility, and fine motor skills.

The specific requirements for voting systems accessibility are based on the accessibility standards for electronic and information technology (EIT) established in *36 CFR Part 1194—Electronic and Information Technology Accessibility Standards*, which implement Section 508 of the Rehabilitation Act of 1973 as amended by Title II of the Rehabilitation Act Amendments of 1998 (29 U.S.C. 794d). These standards apply, with limited exclusions, to all federal agencies for the procurement of electronic and information technology. They were developed under the leadership of the Access Board, an independent federal agency established by the Rehabilitation Act to promote accessibility for individuals with disabilities.

Although the EIT accessibility standards were not designed specifically with voting systems in mind, they were designed to provide accessibility to systems that display, record and otherwise process information utilizing many of the same technologies that are used, or could be used, by voting systems today. For example, they apply to systems that process forms and textual information using display screens, keyboards, and audio devices.

Although they apply directly to systems purchased by Federal agencies, the users of these systems (i.e., federal employees and members of the public seeking information or services from a Federal agency) are very representative of the users of voting systems: election officials (both paid and volunteer) and voters. Indeed, a very significant proportion of the individuals who use systems governed by Section 508 are also voters.

The accessibility requirements for voting systems defined in the VSS address:

- ◆ Applicability
- ◆ Technical Standards
- ◆ Functional Performance Criteria; and
- ◆ Information, Documentation and Support.

Section 2.2.5 provides the specific requirements.



## 1.5 Definitions

---

The standards contain terms describing function, design, documentation, and testing attributes of equipment and computer programs. In most cases, the intended sense is that commonly used by the information technology industry. In some cases the usage is more restrictive, and it applies specifically to voting system computer programs. A glossary of these terms is contained in Appendix A. Terms not listed in Appendix A shall be interpreted according to their standard dictionary definitions.

The following particularly important terms are defined below:

- ◆ Voting System
- ◆ Paper Vote Based System
- ◆ Electronic Voting System
- ◆ Internet Voting Systems

### 1.5.1 Voting System

---

A voting system is a total combination of mechanical, electromechanical or electronic equipment, including the software, firmware, and documentation required to program, control, and support the equipment that is used to define ballots; to cast and count votes; to report and/or display election results; and to maintain and produce all audit trail information. By definition, a voting system also includes the practices and associated documentation used identify system components and their versions, test the system during its development and maintenance, maintain records of system errors and defects, and determine specific system changes to be made to a system after initial system qualification. By definition, this includes all documentation required in Section 9.4.

### 1.5.2 Paper Vote Based Voting System

---

*A Paper Vote Based 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, using one or more ballot cards. The punchcard voting system records votes by means of holes punched in designated voting response locations; the marksense voting system records votes by means of marks made in imprinted voting response locations. There are two types of paper based voting systems, classified according to the intended use, and to the manner in which votes are tabulated.

- ◆ **Precinct Count Systems**—tabulate ballot cards at the polling place. These systems are typically used to tabulate ballots as they are cast, and are programmed to print the results of the tabulation after the close of polling. The systems may also provide a means for electronic storage of the tabulation, either in a magnetic medium (on disk or tape) or in a non-volatile semiconductor memory component; for transmitting the results to a central location over public telecommunication networks; for consolidating and reporting results from precincts at the central location; for transmitting the results from the central location to a higher election authority (such as county to State) over public telecommunication networks; and for electronic distribution of election results for on-site or remote display.
- ◆ **Central Count Systems**—tabulate ballot cards at a central counting place (or at designated regional sites). Voted ballot cards are typically placed into secure containers at the polling place. After the close of polling, these containers are transported to a central counting place. The systems produce either a printed report of the vote count, a report stored on a magnetic medium or in a semiconductor memory component, or both. These systems may also provide a parallel means for transmitting the results to a higher election authority (such as county to State) over public telecommunication networks and for electronic distribution of election results for on-site or remote display.

### 1.5.3 Electronic Voting System

---

An *Electronic Voting System* (referred to in the initial standards as a Direct Recording Electronic (DRE) Voting System) is one 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 ballot images in internal and/or external memory components. It produces a tabulation of the voting data as hard copy or stored in a removable memory component, or both.

The system may also provide a means for transmitting the results to a central location over public telecommunication networks; for consolidating and reporting results from precincts at the central location; for transmitting the results from the central location to a higher election authority (such as county to State) over public telecommunication networks, and for electronic distribution of election results for on-site or remote display.

### 1.5.4 Internet Voting System

---

An *Internet Voting System* is defined as an election system that uses electronic ballots that would allow voters to transmit their voted ballot to election officials over the

Internet. For purposes of these standards, Internet voting systems are considered a category of systems within Electronic Voting Systems and, due to their design, are subject to many of the standards applicable to Electronic Voting Systems. However, because Internet voting relies on equipment beyond the control of the election authority, and is subject to additional threats to system integrity and availability, additional requirements apply.

The VSS address Internet voting to assure that as these systems are developed they provide the same level of integrity, security, performance and availability as other voting systems. The VSS do not promote Internet voting, but instead recognize the need for standards to assure that Internet Voting Systems, when they are developed, are examined and tested using standards that recognize the unique design and operating characteristics, and inherent risks, of Internet Voting Systems.

Internet voting is a complex undertaking with no room for error. In particular, the acceptance of Internet voting, and approval of Internet Voting Systems, must be accomplished in a manner that precludes three risks to the election process: automated large scale casting of fraudulent votes, automated manipulation of vote counts, and disruption of the voting process such that the system is unavailable to voter during the time periods authorized for system use.

The first implementations of Internet voting systems are expected to be utilized in parallel with the operation of other voting systems. Two scenarios reflect the approaches envisioned by the VSS for Internet Voting Systems:

- a. *Polling Place Internet Voting*, defined as the use of Internet Voting Machines at traditional polling places staffed by election officials who conduct authentication of voters before ballots are cast. In this scenario, voters would not gain the advantage of voting from any place at any time, but the integrity of the voting and tabulation technology will be verified through the use of Internet Voting Machines, a device and associated software that allows an electronic ballot to be cast over the Internet.
- b. *Remote Internet Voting*, defined as the unsupervised use of an Internet Voting Machine to cast a ballot over the Internet using a computer not necessarily owned and operated by election personnel, with no election officials present during voting to assist in voter authentication. This scenario allows voters to cast remote Internet ballots from uncontrolled machines at uncontrolled locations. These machines may be owned by the voter or third persons (e.g., employer, library, hotel, college, military installation, etc.), and may be located anywhere an Internet connection can be provided. Authentication of the voter's identity would take place with a combination of manual and electronic procedures that would provide at least the same level of security as existing voting processes.

The VSS are defined to apply to each of the Internet Voting System scenarios defined above, provided that the system is operated in parallel with another voting system. Recognizing the risks and research needs cited in studies of Internet voting conducted to date, including *the Report of the National Workshop on Internet Voting: Issues*

*and Research Agenda, March 2001* (sponsored by the National Science Foundation), the Standards do not address a standalone Internet voting system.

## **1.6 Application of the Standards and Test Specifications**

---

The standards apply to all system hardware, software, firmware, 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 quantitative tests and qualitative examination, to determine system suitability for election use.

Some voting systems utilize one or more commercial, readily available devices (such as card readers, printers, personal computers) and software products (such as operating systems, programming language compilers, database management systems). A device is defined as a functional unit that performs its assigned tasks as an integrated whole. These devices and software are exempted from certain portions of the Standards and test processes as defined therein, so long as they are not modified for use in a voting system.

Voting system are subject to the following three testing phases prior to being purchased or leased:

- ◆ National qualification tests
- ◆ State certification tests
- ◆ State and/or local acceptance tests

## 1.6.1 Qualification Tests

---

*Qualification tests* validate that a voting meets the requirements of these 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.

Qualification tests for voting systems are performed by Independent Test Authorities (ITAs) certified by NASED. ITAs may be certified for the full scope of qualification testing, or for distinct subsets of the total scope of testing. To date, ITAs have been certified 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. 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 national test standards and qualifies for the certification process of states that have adopted the national standards. The Qualification Number applies to the system as a whole, and does not apply to individual system components.

Further examination of a system is required after the system has completed qualification testing if modifications are made to hardware, software, communications or documentation, including the installation of software on different hardware. Vendors will request review of modifications by the appropriate ITAs based on the nature and scope of changes made and the scope of the ITAs NASED certification. The ITA will determine the extent to which the modified system should be resubmitted for qualification testing. In the case of software modifications, as distinct from other changes, detailed re-testing is likely.

Generally a voting system remains qualified as long as no modifications are made to the system that have not been submitted to, and tested by, a certified ITA. The qualification test report remains valid for as long as the voting system remains unchanged. However, all systems that transmit official or live data using public networks are subject to an additional requirement that the system be retested periodically even if no modifications have been made. This requirement applies to Internet voting systems, and also to precinct count systems (paper based and electronic) that transmit official or live data using public networks as defined in Section 5. The requirement for periodic retesting recognizes that the risks and threats to availability and integrity for these systems increase over time, and system capabilities that may have been adequate at one point in time may no longer be sufficient. These systems are therefore given a VSS Qualification Number that is valid for only a single year, and which is renewed upon successful system review by a certified ITA.

Qualification testing differs from the vendor's developmental testing. The ITA will be 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 systems performance specifications. The ITA will undertake sample testing of the vendor's test modules and also design 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, the test conditions are, in most cases, less severe. This reflects commercial and industrial, rather than military and aerospace, practice.

## 1.6.2 Certification Tests

---

*Certification tests* should be 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 at the national level;
- ◆ 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 state laws, election practices, and specific environment in mind. It is recommended, however, that they not duplicate qualification tests, but include 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 in addition to those defined in the VSS. By design, the VSS, and qualification testing of voting systems for compliance with the VSS, do not address these additional requirements. However, qualification testing does address all capabilities of a voting system stated by the vendor in the system documentation submitted to the ITA, including capabilities that are not required by the VSS but which may be in response to state requirements.

### 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 as delivered is state certified and/or nationally qualified;
- ◆ 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 would be repeated during acceptance testing. If a voting system is modified after acceptance, it is recommended that it be reevaluated to determine if further acceptance testing is warranted.

The original version of the VSS issued January 1990 provided information and guidelines in *Section 8, Acceptance Tests*, concerning acceptance testing of voting systems by purchasing jurisdictions. The reorganization of the VSS for this version will provide expanded information and guidance on best practices to states and jurisdictions for acceptance testing in additional volumes of the VSS. Accordingly, Volumes I and II of the VSS do not contain updated guidelines concerning acceptance testing.

## 1.7 Outline of Contents

---

The organization of the standards has been simplified to facilitate their 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.

- a. Section 2 describes the functional capabilities required of voting systems.
- b. Sections 3 through 6 describe specific performance standards for election system hardware, software, telecommunications and security, respectively.
- c. Sections 7 and 8 describe recommended practices for quality assurance and configuration management, respectively, to be utilized 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.

- d. Section 9 provides an overview of the test and measurement process used by test authorities for qualification and re-qualification of voting systems.
- e. Appendix A provides a glossary of important terms used in Volume I.
- f. Appendix B lists the publications used for guidance in the preparation of the Standards and which also contain information which is useful in interpreting and complying with the requirements of the Standards.

*Volume II, Voting System Qualification Testing Standards*, is intended for primary use by independent test authorities, state organizations state organizations that certify a system, and vendors. This volume complements the content of Volume I, describing the standards for the technical information submitted by the vendor to support testing; the development of test plans by the independent test authority (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.



# Table of Contents

---

<b>2 Functional Capabilities</b> .....	<b>2-1</b>
2.1 Scope.....	2-1
2.2 Overall System Capabilities .....	2-2
2.2.1 Security.....	2-2
2.2.2 Accuracy and Integrity.....	2-3
2.2.2.1 Vote Accuracy Measures.....	2-3
2.2.2.1.1 Common Standards.....	2-3
2.2.2.1.2 Electronic System Standards.....	2-4
2.2.2.2 Integrity Measures.....	2-4
2.2.2.2.1 Common Standards.....	2-4
2.2.2.2.2 Electronic Systems Standards.....	2-4
2.2.3 System Audit.....	2-5
2.2.3.1 System Audit Purpose and Context.....	2-5
2.2.3.2 Operational Requirements.....	2-6
2.2.3.2.1 Time, Sequence, and Preservation of Audit Records .....	2-6
2.2.3.2.2 Error Messages .....	2-7
2.2.3.2.3 Status Messages .....	2-7
2.2.4 The Election Management System.....	2-8
2.2.5 Accessibility .....	2-8
2.2.5.1 Scope and Applicability .....	2-9
2.2.5.2 Technical Standards.....	2-9
2.2.5.3 Functional Performance Criteria .....	2-10
2.2.5.4 Information, Documentation and Support.....	2-10
2.2.6 Vote Tabulating Capabilities.....	2-10
2.2.7 Telecommunications .....	2-11
2.2.8 Retention of Data .....	2-12
2.3 Pre-voting Functions .....	2-14
2.3.1 Ballot Preparation .....	2-14
2.3.1.1 General Capabilities .....	2-14
2.3.1.1.1 Common Standards.....	2-14
2.3.1.1.2 Paper Based System Standards.....	2-15
2.3.1.2 Ballot Formatting .....	2-15

2.3.1.3 Ballot Production .....	2-16
2.3.2 Election Programming .....	2-16
2.3.3 Ballot and Program Installation .....	2-17
2.3.4 Readiness Testing .....	2-17
2.3.5 Verification at the Polling Place .....	2-18
2.3.6 Verification at the Central Location .....	2-18
2.3.6.1 Verification Standards .....	2-19
2.3.6.2 Test Data .....	2-19
2.3.6.3 Data Verification Reporting .....	2-19
2.4 Voting Functions .....	2-19
2.4.1 Opening the Polls .....	2-20
2.4.1.1 Paper Based System Standards .....	2-20
2.4.1.2 Electronic System Standards .....	2-20
2.4.2 Activating the Ballot (Electronic Systems) .....	2-21
2.4.3 Casting a Ballot .....	2-21
2.4.3.1 Common Standards .....	2-21
2.4.3.2 Paper Based Systems Standards .....	2-21
2.4.3.2.1 All Paper-Based Systems .....	2-21
2.4.3.2.2 Precinct Count Paper-Based Systems .....	2-22
2.4.3.3 Electronic Systems Standards .....	2-22
2.4.3.4 Internet Voting Systems Standards .....	2-23
2.4.4 Augmenting the Election Counter (for Paper-based Systems) .....	2-24
2.4.5 Augmenting the Life Cycle Counter (for Paper-based Systems) .....	2-24
2.5 Post-Voting Functions .....	2-25
2.5.1 Closing the Polling Place (Precinct Count) .....	2-25
2.5.2 Closing the Polling Place (Internet Voting Systems) .....	2-25
2.5.3 Obtaining Polling Place Reports (Precinct Count) .....	2-26
2.5.4 Obtaining Precinct Reports Jurisdiction-wide (Central Count) .....	2-26
2.5.5 Obtaining Consolidated Reports or Results .....	2-27
2.5.6 Consolidation of Absentee Ballots .....	2-27
2.5.7 Consolidation of Internet Ballots .....	2-27
2.5.8 Broadcasting Results .....	2-27
2.6 Maintenance .....	2-28
2.7 Transportation and Storage (Precinct Count) .....	2-28

## Functional Capabilities

---

### 2.1 Scope

---

This section contains the functional capabilities required of all voting systems. The requirements specified herein represent acceptable levels of combined hardware and software function, commensurate with overall system requirements for functionality, speed, accuracy, reliability, and audit capability. Functional capabilities are defined in terms of specific standards. *Standards* are mandatory requirements and are designated by use of the term *shall*.

These functional capabilities include all operations necessary to support the following three phases of election activity:

- ◆ **Pre-voting:** ballot preparation; the preparation of election-specific software or firmware; the production of ballots or ballot pages; the installation of ballots and ballot counting software or firmware; and system and equipment tests.
- ◆ **Voting:** all operations conducted at the polling place by voters and officials including the generation of status messages.
- ◆ **Post-voting:** closing the polling place; obtaining reports by voting machine, polling place, and precinct (central count systems); obtaining consolidated reports; and obtaining reports of audit trails.

They also include overall system capabilities relating to security; accuracy and integrity; the election management system; the vote tabulating program; telecommunications; and data retention and audit trails.

Finally, they include the capabilities necessary to maintain voting system equipment, and, for precinct count systems, to transport and store the equipment.

Recognizing the diversity of voting systems and the technologies they employ, these functional capabilities are structured to apply specific standards to the appropriate technologies. Some of these standards apply only if the system incorporates certain optional functions (for example, voting systems employing telecommunications to transmit voting data.). For each scenario, *Common Standards* are specified first, followed, where necessary, by standards applicable to specific technologies (i.e., paper based systems and electronic systems and intended use (i.e., central or precinct



count). For purposes of these Standards, Internet voting systems are considered a form of electronic voting system, and are subject to the standards for electronic voting systems, with specific exceptions noted due to fundamental differences of system design. Internet voting systems are also subject to additional standards deemed necessary due to unique characteristics and risks of Internet-based technology.

## 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 functional capabilities that address standards for:

- ◆ security;
- ◆ accuracy and integrity;
- ◆ system auditability,
- ◆ Election Management System;
- ◆ vote tabulating program;
- ◆ telecommunications; and
- ◆ retention of Data.

*Technical* standards for these capabilities are described Sections 3 through 6 of these Standards.

### 2.2.1 Security

---

All systems shall meet the following standards:

- ◆ Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality and accountability
- ◆ Provide system functions that are executable only in the intended manner and order, and only under the intended conditions.
- ◆ Use the system's control logic to preclude a system function from executing if any preconditions to the function have not been met.

- ◆ Provide security provisions that are compatible with the procedures and administrative tasks involved in equipment preparation and testing, and in operation by the public in a polling place.
- ◆ If access to a system function is to be restricted or controlled, then the system shall incorporate a means of implementing this capability.

## 2.2.2 Accuracy and Integrity

---

The reliability and quality of memory hardware such as semiconductor devices and magnetic storage media must be high. The overall design of equipment in all voting systems shall provide for the highest possible levels of protection against mechanical, thermal, and electromagnetic (EMI) stress. Section 3 provides additional information on required susceptibility capabilities.

### 2.2.2.1 Vote Accuracy Measures

---

All systems shall incorporate accuracy measures that apply to data recorded by the system, including data entered by election officials and data entered by voters.

#### 2.2.2.1.1 Common Standards

---

All systems shall:

- ◆ Record the election contests, candidates and issues precisely as defined by election officials
- ◆ Record the appropriate options for casting and recording votes;
- ◆ Record each vote precisely as cast and be able to produce an accurate report of all votes cast;
- ◆ 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
- ◆ 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.

#### 2.2.2.1.2 Electronic System Standards

---

As a means of assuring accuracy in electronic machines, the unit shall incorporate a means of providing redundant copies of the original ballot objects or data as entered by the voter (ballot image). (Examples include, but are not limited to, ray to ray and multiple memories).

#### 2.2.2.2 Integrity Measures

---

Integrity measures assure the integrity of the vote recording and counting processes.

##### 2.2.2.2.1 Common Standards

---

All systems shall:

- a. Protect against the interruption of electronic power;
- b. Protect against generated or induced electromagnetic radiation;
- c. Protect against ambient temperature and humidity fluctuations;
- d. Protect against the failure of any data input or storage device;
- e. Protect against any attempt at improper data entry or retrieval;
- f. Provide capabilities for recording and reporting the date and time of normal and abnormal events;
- g. Provide capabilities for maintaining a permanent record of audit information that cannot be turned off;
- h. Provide capabilities for detecting and recording significant events (e.g., casting a ballot), occurrence of an error conditions which cannot be disposed of by the system itself, time-dependent or programmed events which occur without the intervention of the voter or a polling place operator; and
- i. Include built-in test self test, measurement and diagnostic software and hardware for detecting and reporting the system's status and degree of operability.

##### 2.2.2.2.2 Electronic Systems Standards

---

In addition to the common standards indicated above, electronic systems shall maintain a record of each ballot cast, in a manner independent and distinct from the main vote detection, interpretation, processing and reporting path, while protecting the anonymity of each voter ( for example, by means of storage location scrambling).

The system shall be capable of reproducing these ballot images in human readable form.

## 2.2.3 System Audit

---

### 2.2.3.1 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 in the event of litigation.

The following audit trail requirements are based on the premise that system-generated creation and maintenance of audit records reduces the chance of human error. Since most of the 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 these 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 test authorities 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.

Also part of the election audit trail, but not covered in these technical standards, is the documentation of such items as paper ballots delivered and collected, administrative procedures for system security, and maintenance performed on voting equipment. Future new volumes of the Standards are intended to address these and other system operations practices. In the interim, *Innovations in Election Administration #10, Ballot Security and Accountability*, provides useful guidance.



### 2.2.3.2 Operational Requirements

---

Audit records shall be prepared for all phases of elections operations performed using devices controlled by the jurisdiction or its contractor(s). 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.

#### 2.2.3.2.1 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. The purpose of the real-time record is to provide the operator or precinct official with continuous updates on machine status. This information allows effective operator intervention during an error condition, and contributes to the reconstruction of election-related events necessary for recounts or litigation.
- b. All systems shall incorporate a real-time clock as part of system 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 in use 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 interfered with 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 contents of the audit record shall be preserved during any interruption of power to the system until processing and data reporting have been completed.
- g. The system shall be capable of producing a printed 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 hardcopy output device 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.
- 3) The physical security of the audit record entries can be ensured.

#### 2.2.3.2.2 Error Messages

---

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

- a. Error message entries shall be made and reported as they occur. Except for error messages which require resolution by a trained technician, all other 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.
- b. When numerical codes are used for trained technician maintenance or repair, the text corresponding to the code shall be self-contained, or an instructional sheet shall be affixed inside the unit device. This is intended to reduce inappropriate reactions to error conditions, and to allow for ready and effective problem correction.
- c. The message cue for all systems shall clearly state the action to be performed in the event that voter or operator response is required.
- d. System design shall ensure that erroneous responses will not lead to irrecoverable error.
- e. Nested error conditions shall be corrected in a controlled sequence such that system status shall be restored to that initial state existing before the first error occurred.

#### 2.2.3.2.3 Status Messages

---

These Standards provide latitude in software design so that consideration can be given to various user processing and reporting needs. The user may require some status and information messages to be displayed and reported in real-time. Other messages, which do not require operator intervention, may be stored in memory to be recovered after ballot processing has been completed.

Depending on their nature, and at the discretion of the jurisdiction, status messages may or may not become part of the real-time audit record. Non-critical status messages need not be displayed at the time of occurrence. It is acceptable to 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.

Critical status messages will be defined by the jurisdiction. Depending on the critical nature of the message, and the particular jurisdiction's needs, critical status messages

shall be displayed and reported by suitable, unambiguous indicators or English language text.

## 2.2.4 The Election Management System

---

The *Election Management System* is used, on the front end, to prepare ballots and programs for use in casting and counting votes, and on the back end to consolidate, report, and display election results. Election Management Systems shall generate and maintain a database, or one or more interactive databases, that enables the election official or his or her designee to perform the following functions:

- a. Define political subdivision boundaries and multiple political districts;
- 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; and
- h. Generate reports.

## 2.2.5 Accessibility

---

All automated voting systems that utilize electronic and information technology (EIT) shall be accessible to individuals with disabilities. Most voting systems use one or more forms of EIT. Specific definitions of the terms 'electronic and information technology' and 'information technology' are provided in *36 CFR Part 1194—Electronic and Information Technology Accessibility Standards*, which implement Section 508 of the Rehabilitation Act of 1973 as amended by Title II of the Rehabilitation Act Amendments of 1998 (29 U.S.C. 794d).

- ◆ **Electronic and information technology.** Includes information technology and any equipment or interconnected system or subsystem of equipment, that is used in the creation, conversion, or duplication of data or information. The term electronic and information technology includes, but is not limited to, telecommunications products (such as telephones), information kiosks and transaction machines, World Wide Web sites, multimedia, and office equipment such as copiers and fax machines. The term does not include any

equipment that contains embedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For example, HVAC (heating, ventilation, and air conditioning) equipment such as thermostats or temperature control devices, and medical equipment where information technology is integral to its operation, are not information technology.

- ◆ *Information technology.* Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

The full text of *36 CFR Part 1194—Electronic and Information Technology Accessibility Standards*, can be found at the Access Board's Internet site (<http://www.access-board.gov/sec508/508standards.htm>).

### 2.2.5.1 Scope and Applicability

---

All voting systems shall provide accessibility to individuals consistent with *36 CFR Part 1194* for all voting system component products defined as EIT, including self contained, closed products, that are used to support:

- a. System operations activities performed by voters. These activities include, but are not limited to, indicating the voter's selections in individual races and ballot propositions, and submitting the voter's ballot for processing.
- b. System operations activities performed by election officials to accomplish the full range of pre-voting, voting and post voting functions defined in Sections 2.3 through 2.5 of the VSS. These activities include, but are not limited to, performing ballot design, operating vote counting equipment, consolidating vote count information, and conducting audits of voting results.

Products that record votes without the use of EIT (e.g., vote recording devices for paper-based ballots) are excluded from these requirements. However, paper-based ballot scanners and counting devices that use EIT shall meet these requirements.

### 2.2.5.2 Technical Standards

---

All voting systems shall meet the technical standards specified in *Subpart B—Technical Standards of 36 CFR Part 1194*. Of particular note, electronic voting

devices and paper ballot scanning and counting devices, are subject to the specific requirements of Subpart B, Section 1194.25 for self contained closed products.

### 2.2.5.3 Functional Performance Criteria

---

All voting systems shall meet the functional performance criteria specified in *Subpart C - Functional Performance Criteria of 36 CFR Part 1194*.

### 2.2.5.4 Information, Documentation and Support

---

All voting systems shall meet the Information, Documentation and Support requirements of *Subpart D - Information, Documentation and Support of 36 CFR Part 1194*.

## 2.2.6 Vote Tabulating Capabilities

---

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.

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 Technical Data Package accompanying the system shall specifically identify which of the following items that *can* be accommodated by the system:

- 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 options;
- i. Cross-party endorsement;
- j. Split precincts;
- k. Vote for N of M;
- l. Recall issues, with options;
- m. Overvotes;
- n. Undervotes; and
- o. Totally blank ballots.

## 2.2.7 Telecommunications

---

For all voting systems that employ telecommunications for the transmission of data during pre-voting, voting or post-voting activities, capabilities shall be provided which assure data are transmitted with no alteration or unauthorized disclosure during transmission. Section 5 of these Standards describes standards that apply to, at a minimum, the following types of data transmissions:

- a. **Voter Registration Information (Pre-voting, Voting and Post-voting)**—Information that identifies the name and eligibility of a voter;
- b. **Ballot Definition Transmission (Pre-voting)**—Information that describes to a voting machine the content and appearance of the ballots to be used in an election;
- c. **Voter Key Distribution (Pre-voting)**—For Internet voting systems, a code that consists typically (but not always) of secret numbers that are used to verify the identity and eligibility of a potential voter;
- d. **Authentication of Security Information (Pre-voting, Voting)**—For Internet voting systems, a code provided to a voter by the jurisdiction that is combined with a personal identification number that will allow a voter to authenticate himself/herself to the system;
- e. **Ballot Transmission to Voter (Voting)**—For Internet voting systems, the transmission of the appropriate ballot image to an authenticated voter;
- f. **Vote Transmission to County (Voting)**—For Internet voting systems, the transmission of a single voted ballot to the central location for consolidation with other county vote data;

- g. **Vote Count Transmission (Voting and Post-Voting)**—Information representing the transmission of tabulated votes among or between any of several levels: polling place, precinct, or central count;
- h. **List of Voters (Voting and Post-Voting)**—A listing of the individual voters who have cast ballots in a specific election; and

## 2.2.8 Retention of Data

---

United States Code Title 42, Sections 1974 through 1974e, states that election administrators are required to preserve for 22 months “all records and paper which came into (their) possession relating to an application, registration, payment of poll tax, or other act requisite to voting.” This retention requirement applies to systems that will be used at any time for voting of candidates for Federal offices (e.g., Member of Congress, United States Senator, and/or Presidential Elector). Therefore, all 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.

Since 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. As such, all documentation that may be relevant to the detection and prosecution of federal civil rights or election crimes are required to be maintained intact for the 22-month federal retention period, as long as it was generated in connection with an election which 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 play and requires that the record be retained for 22 months if it falls into one or more of the categories listed below.

For 22-month document retention, the general rule is that all hard-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 contained in a database file. In precinct count systems, this data is used to program each machine, establish ballot layout and generate tallying files. The preliminary thinking is that it is not necessary to retain this information on electronic media if there is documented producible hard copy of all final database information. It is recommended, however, that electronic storage of the aggregate summary data for each device be retained in addition to hard-copy records so that reconstruction of an

election is possible without data re-entry. The same requirement and recommendation shall apply to vote results generated by each precinct device or system.

Specifically, the Department of Justice considers Section 1974 to include the following items relevant to automated voting systems:

- a. Copies of operating procedures, including security measures, established for system preparation, operation and data extraction;
- b. Election database(s);
- c. Election programming and ballot formatting records;
- d. Records of the installation of election programs and ballots;
- e. Records of pre-election testing of electronic vote counting systems;
- f. Test deck(s) and test program(s);
- g. Printed list of zero totals for precinct count devices (or memory registers in central count systems);
- h. All voted ballots, paper or machine-read, including absentee ballots (Section 1974 requires the retention of the ballots themselves in those jurisdictions where a voter's preference is manifested by marking a piece of paper or punching holes in a computer card);
- i. Records of ballot images produced by electronic voting devices;
- j. Strips or sheets mounted on electronic voting machines (ballot faces), each identified by machine number and precinct;
- k. Assembled vote recorder pages (applicable to Votomatic systems), each identified by precinct;
- l. Any record reflecting the identity of those who cast ballots, if automated;
- m. Official canvass records, if automated;
- n. All Statements of Votes;
- o. Removable data storage component (PROM, memory pack, cartridge, chip, etc.) [*Either the storage component itself is saved, or save, on electronic medium, record of programming the device, and the post-election hard copy of its output plus the program used to read the component.*];
- p. Reports produced by voting devices at the opening and closing of polls;
- q. Records of service and maintenance to voting equipment at the polling place;
- r. All vote-counting software; and
- s. All audit trail records;

The above listing does not include other items required that are of an administrative nature and not elements of the voting system itself.



## 2.3 Pre-voting Functions

---

This section defines capabilities required of voting systems 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;
- ◆ Readiness Testing;
- ◆ Verification at the Polling Place; and
- ◆ Verification at the Central Counting Place.

These 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.

- ◆ General Capabilities;
- ◆ Ballot Formatting; and
- ◆ Ballot Production.

#### 2.3.1.1 General Capabilities

---

The general capabilities for *Ballot Preparation* define common standards and also standards specific to all paper based systems.

##### 2.3.1.1.1 Common Standards

---

All systems shall be capable of:

- ◆ Enabling the automatic formatting of ballots in accordance with the requirements for offices, candidates, and measures qualified to be placed upon the ballot for each political jurisdiction;
- ◆ Generating ballots that contain identifying codes or marks uniquely associated with each format;
- ◆ Supporting at least 500 potentially active voting positions, which can be arranged so as to identify party affiliations in a primary election; and
- ◆ Collecting and maintaining the following data:
  - Offices and their associated labels and instructions;
  - Candidate names and their associated labels; and
  - Issues or measures and their associated text.
- ◆ Ensure 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

---

Paper Based Systems also shall meet the following standards applicable to the technology utilized:

- a. Enable voters to make selections by punching a hole or by making a mark in fields (regions) 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.
- d. For marksense ballots, ensure that vote selections are read for only a single ballot at a time, without detection of marks from multiple ballots concurrently (e.g., reading of bleed-through from other ballots)

#### 2.3.1.2 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 to be contained on the ballot and to present them in a layout permitted by state law. All systems shall provide a capability for the:

- 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 all choices for a single contest on the same page, with no splitting across multiple pages or displays;
- e. Easy navigation of multi-page ballots by voters, with no way to get lost or leave the balloting process except deliberately;
- f. Retention of previously defined formats in that election;
- g. Prevention of unauthorized modification of ballot formats subsequent to an election; and
- h. 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. The voting system shall provide a means of printing or otherwise generating a ballot display, which 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 hardcopy 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 hardcopy document on which the user views the ballot shall not show any advertising or commercial logos of any kind, whether public service, commercial, or political, unless specifically provided for in State law; and for electronic displays shall not provide connection to same via hyperlink; and
- c. Conformance to vendor specifications for type of paper, stock, weight, size, shape, and ink for printing if paper ballot documents or paper displays are part of the system.

### 2.3.2 Election Programming

---

*Election Programming* is the process by which election officials or their designees use election databases and vendor system software/firmware to logically define to the

system's software the voter choices associated with the contents of the ballot(s). All systems shall provide for the:

- a. Logical definition of the ballot(s), 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 may vary among polling places;
- c. Activation or exclusion of any portion of the ballot(s) upon which the entitlement of a voter to vote may vary by reason of place of residence, or other such administrative or geographical criteria;
- d. Ability to select from a range of voting options to enable conformance with the laws in 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 ballot(s) for each voting device and polling place, and for each tabulating device.

### 2.3.3 Ballot and Program Installation

---

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* at the jurisdiction:

- a. 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;
- b. A method for validating that software (whether nonresident or resident) has been properly selected and installed in the equipment or in a programmable memory device; and
- c. A method for validating that software correctly matches the ballot formats that it is intended to process.

### 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.

All systems shall contain appropriate and necessary provisions for:

- a. Verifying that voting machines or vote recording and data processing devices, precinct count ballot-counting devices, and central counting equipment are properly prepared for an election;
- b. Obtaining status and data reports from each set of equipment;
- c. Verifying the effective integration of all system equipment;
- d. Verifying that hardware and software function correctly; and
- e. Generating consolidated data reports at the polling place and higher jurisdictional levels.

### 2.3.5 Verification at the Polling Place

---

Jurisdiction election officials perform *Verification at the Polling Place* to ensure 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 commands:

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

### 2.3.6 Verification at the Central Location

---

Jurisdiction election officials perform *Verification at the Central Location* to ensure that vote counting devices and software function properly before and after an election.

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.

### 2.3.6.1 Verification Standards

---

Verification shall include the use of tests needed to assure the readiness of the equipment and to accommodate administrative reporting requirements.

### 2.3.6.2 Test Data

---

Test data shall be segregated from actual voting data, either procedurally or by hardware/software features.

### 2.3.6.3 Data Verification Reporting

---

Any paper based system used in a central count environment shall provide a printed record of the following upon verification of the authenticity of the commands:

- a. The election's identification data;
- b. The contents of each active candidate register by office and of each active measure register (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 provide capabilities to support the following voting functions:

- ◆ Opening the polls; and
- ◆ Casting a ballot.

All electronic systems also shall provide capabilities to support:

- ◆ Enabling the Ballot.
- ◆ Augmenting the Election Counter; and
- ◆ Augmenting the Life-Cycle Counter.

## 2.4.1 Opening the Polls

---

The standards for *Opening the Polls* are specific to individual voting system technologies. The vendor shall provide, at a minimum, systems with the functional capabilities indicated below.

### 2.4.1.1 Paper Based System Standards

---

All paper based systems shall include:

- a. a means of verifying that ballot punching or marking devices are properly prepared and ready for 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.

In addition, precinct count equipment shall include a means of:

- d. activating the ballot counting device;
- e. verifying that the device has been correctly activated and is functioning properly; and
- f. identifying device failure and corrective action needed.

### 2.4.1.2 Electronic System Standards

---

All electronic systems shall provide a means of opening the polling place and activating the equipment for voting that incorporates:

- 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 device has been activated correctly; and
- d. a means of identifying device failure and corrective action needed.

## 2.4.2 Activating the Ballot (Electronic Systems)

---

Electronic systems shall provide capabilities for:

- a. Accomplishing the recording of votes and the casting of a ballot by each eligible voter;
- b. Preventing the voter from voting on a ballot to which he or she is not entitled; and
- c. Preventing a voter from casting more than one ballot in the same election.

## 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. All systems must provide capabilities that enable voters with disabilities to cast a ballot unassisted.

Systems must provide additional functional capabilities that enable accessibility to disabled voters as defined in Section 2.2.5 of these Standards.

### 2.4.3.1 Common Standards

---

All systems shall provide the means for:

- a. the voter's selection of candidates whose names do not appear on the ballot, if applicable under State law, and the recording of as many write in votes as the number of candidates the voter is allowed to select; and
- b. protecting the secrecy of the vote such that the content of the voted ballot may not be viewed and associated with the voter at any time, unless specifically required by State law (for example, Arkansas).

### 2.4.3.2 Paper Based Systems Standards

---

#### 2.4.3.2.1 All Paper-Based Systems

---

All paper based systems shall provide the means for the voter to:



- a. Easily identify the voting field that is associated with each candidate or ballot measure response;
- b. Either directly punch or mark the ballot to register votes, or punch or mark the ballot to reflect choices made on the basis of separate ballot pages;
- c. Place the voted ballot, or cause it to be placed, into the ballot counting device (precinct count systems) or into a secure receptacle (central count systems); and
- d. Protecting the secrecy of the vote while making selections and while the voted ballot is being handled, either by the voter or by a polling place official, if the voter must leave the voting booth to place the ballot in a secure receptacle or ballot counting device.

#### 2.4.3.2.2 Precinct Count Paper-Based Systems

---

Precinct count paper based systems shall provide the means to:

- a. Provide feedback to the voter that identifies specific contests or ballot issues for which an over-vote or under-vote is detected;
- b. Allow the voter, at the voter's choice, to vote a corrected ballot or submit the ballot 'as is' without correction; and
- c. Allow a voting official, with appropriate access control, to turn off the capabilities defined in 'a' and 'b' above.

#### 2.4.3.3 Electronic Systems Standards

---

Electronic systems shall provide the means for:

- a. 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.
- b. Allowing the voters to be able to select their preferences on the ballot in any legal number and combination;
- c. Indicating that a selection has been made or canceled;
- d. Preventing voters from over-voting (i.e., voting for more candidates than permitted for a single office);
- e. Signifying to each voter that the selection of candidates and measures has been completed;
- f. Allowing the voters, before the ballot is cast, to review their choices and, if they desire, to delete or change their choices before the ballot is cast;

- g. Prompting the voter to confirm the voter's choices before casting their 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;
- h. Signifying to the voter that the ballot has been cast after the vote is stored successfully;
- i. Ensuring that the votes stored accurately represent the actual votes cast;
- j. Preventing modification of the voter's vote after the ballot is cast;
- k. Recording an image of the ballot cast in human readable form (in accordance with the requirements of 2.2.2.2.2 and 2.2.8);
- l. Incrementing the proper ballot position registers or counters (not applicable to Internet systems);
- m. Protecting the secrecy of the vote such that the vote may not be observed during the voter's selection of preferences, during the casting of the ballot, and as the voted ballot is transmitted for recording on a storage device; and
- n. Prohibiting voted ballots from being accessed by anyone until after the close of polls.

#### 2.4.3.4 Internet Voting Systems Standards

---

In addition to the standards for electronic systems listed above, Internet voting systems shall provide the means for:

- a. Using a unique personal identifier assigned to the voter for voting;
- b. Using a unique voter identifier, such as a password, assigned to the voter during the election official's authentication of the voter;
- c. Providing only deliberate selections for exiting the voting process, with no ability to link to other sites or processes;
- d. Encrypting the voted ballot as it travels over the Internet to protect the secrecy and integrity of each vote;
- e. Providing sufficient computational performance to provide responses back to voters in ten seconds even if some vote servers are down;
- f. The vote server only accepting a voted ballot in its entirety.
- g. Providing a means to communicate to the voting device and voter that a voted ballot has not been accepted by the server (due to non-receipt or other problem), and enabling the voter to try to vote again by Internet or other means;
- h. Providing a means to count only the initial ballot cast when a ballot has been successfully received by the vote server but confirmation has been received

by the voting device, thus avoiding double counting or voter changes to the initial ballot;

- i. Avoiding the storage of keys or other tools for decrypting ballots on the vote server for votes that are managed by persons other than the election officials;
- j. Providing high-bandwidth connections to the Internet sufficient to support peak voter activity during the last hours Internet voting is permitted;
- k. Providing high-bandwidth connections to the Internet sufficient to support peak voter activity aggregated across the jurisdiction, and aggregated across all jurisdictions and elections supported by the same vote server data center.
- l. Maintaining high system availability, detecting and defeating denial of service attacks during allowable voting periods;
- m. Recording a maximum allowable time period for voting hours to be extended;
- n. Casting of test ballots for use in verifying end-to-end integrity of the entire voting system; and
- o. Isolating 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.

#### 2.4.4 Augmenting the Election Counter (for Paper-based Systems)

---

Vote counting equipment for all paper-based systems shall provide a counter that:

- a. Can be set to zero prior to opening of the polling place;
- b. Records the number of ballots cast during that particular election;
- c. Adds incrementally only by the input of a ballot;
- d. Prevents or disables resetting the count by other than authorized persons after the polls close; and
- e. Is visible to all designated polling place officials.

#### 2.4.5 Augmenting the Life Cycle Counter (for Paper-based Systems)

---

Vote counting equipment for all paper-based systems shall provide a counter that:

- a. Records all of the test and election ballots input since the unit was built;

- b. Cannot be reset and cannot be changed by any cause other than the casting of a ballot; and
- c. Is visible at all times when the device is configured for test, maintenance, or election use.

## 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 of closing 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. Incorporating a visible indication of system status; and
- c. Precluding the unauthorized reopening of the polls once the poll closing has been completed for that election.

### 2.5.2 Closing the Polling Place (Internet Voting Systems)

---

The standards for *closing the polling place* are specific to Internet voting systems. These systems shall provide the means to:

- a. Provide automatic termination of the ability to cast ballots system-wide at a time specified by an authorized central office election official.
- b. Enable an authorized local election official, for poll site Internet voting systems, to extend voting time at the specified poll site for a specific duration, and terminate voting at the time specified by the official;
- c. Enable an authorized central office election official to monitor whether ballots are being cast at poll sites during extended voting hours and terminate voting at any poll site (for example, if an authorized local official specifies a voting time extension determined to be unduly long by the central office official);

### 2.5.3 Obtaining Polling Place Reports (Precinct Count)

---

The standards for *obtaining polling place reports* are specific to precinct count systems. These systems shall provide a means to:

- a. Prevent the printing of reports or the extraction of data, until the proper sequence of events associated with closing the polling place has been completed;
- b. Produce a printed report of the votes counted upon each voting machine or precinct tabulator;
- c. Produce all reports or electronic memory that contains all system audit information required in Section 4.5;
- d. Extract information from a transportable programmable memory device or data storage medium;
- e. If more than one voting machine or precinct tabulator is used, consolidate and report the data contained in each unit into a single report for the polling place; and
- f. Prevent memory data from being altered or destroyed by report generation, or by the electronic transmission of results over telecommunications lines.

### 2.5.4 Obtaining Precinct Reports Jurisdiction-wide (Central Count)

---

For all central counting equipment, the equipment shall provide a means for, at a minimum:

- a. Extracting data from transportable memory devices and storage media;
- b. Allowing the data to be used to produce a printed report of the vote for each precinct;
- c. Producing a printed report of the vote counted by each counting machine if multiple machines are used;
- d. Producing reports that contain all information required for audits, as defined in Sections 2.2.3 and 4.5; and
- e. Preventing memory data in portable media from being altered or destroyed by report generation.

## 2.5.5 Obtaining Consolidated Reports or Results

---

All systems shall provide a means for:

- a. Consolidating into one report the data and/or results from all polling places; and
- b. Consolidating the data at one or more intermediate levels.

## 2.5.6 Consolidation of Absentee Ballots

---

All systems shall provide a means for:

- a. Consolidating into one report the data from all polling places with that from absentee ballots; and
- b. Consolidating the data at one or more intermediate levels.

## 2.5.7 Consolidation of Internet Ballots

---

For all systems that are intended to operate in combination with an Internet voting system, the system shall provide a means for:

- a. Consolidating into one report the data from all polling places with that from Internet ballots
- b. Consolidating the data at one or more intermediate levels

## 2.5.8 Broadcasting Results

---

Some voting systems offer a capability to make interim, unofficial results available to external organizations such as the news media, political party officials, and others in the form of paper reports or electronic reports or data files. Although this capability is not required, systems that make unofficial results available shall:

- a. Provided only aggregated results, and not data for individual ballots;
- b. Provide no access path from unofficial electronic reports or data files to the storage devices for official data; and

- c. Provide prominent labeling of all reports and data files indicating they contain unofficial election results.

## **2.6 Maintenance**

---

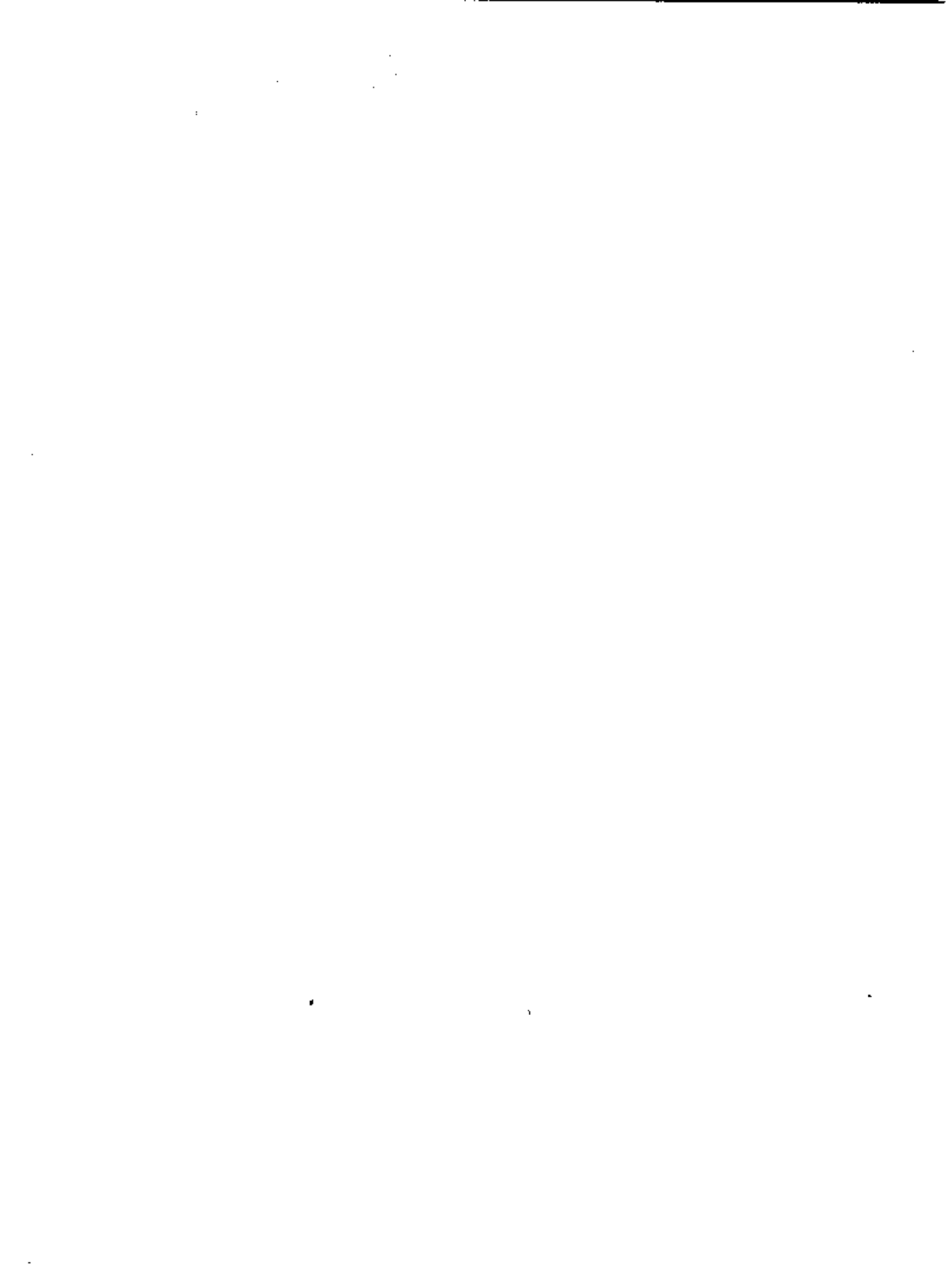
All systems shall be designed and manufactured to facilitate preventive and corrective maintenance, conforming to the standards described in Section 3, Hardware Standards.

## **2.7 Transportation and Storage (Precinct Count)**

---

All precinct count devices shall be capable of:

- a. Functioning without degradation in capabilities after transit to and from the polling place, as demonstrated by meeting the performance standards described in Section 3; and
- b. Functioning without degradation in capabilities after storage between elections, as demonstrated by meeting the performance standards described in Section 3.





# Table of Contents

---

<b>3 Hardware Standards</b> .....	<b>3-1</b>
3.1 Introduction.....	3-1
3.1.1 Scope.....	3-1
3.1.2 Organization of this Section .....	3-2
3.2 Performance Requirements .....	3-3
3.2.1 Environmental Requirements.....	3-4
3.2.1.1 Shelter Requirements.....	3-4
3.2.1.2 Space Requirements.....	3-4
3.2.1.3 Furnishings and Fixtures .....	3-4
3.2.1.4 Electrical Supply.....	3-4
3.2.1.5 Environmental Control.....	3-5
3.2.1.6 Data Networks Guidelines .....	3-5
3.2.2 Control Requirements .....	3-5
3.2.2.1 Equipment Preparation.....	3-6
3.2.2.2 Pre-Election Testing .....	3-6
3.2.2.3 Tests at the Polling Place .....	3-6
3.2.2.4 Tests at Central Counting Facilities .....	3-7
3.2.2.5 Opening the Polling Place (Precinct Count Systems) .....	3-7
3.2.2.6 Activating a Ballot (Electronic Systems) .....	3-7
3.2.2.7 Error Recovery (Precinct Count System).....	3-8
3.2.2.8 Closing the Polling Place.....	3-8
3.2.2.9 Polling Place Reports .....	3-8
3.2.3 Election Management System Requirements.....	3-9
3.2.3.1 Recording Accuracy .....	3-9
3.2.3.2 Memory Stability .....	3-9
3.2.4 Vote Recording Requirements .....	3-10
3.2.4.1 Paper Based Recording Requirements .....	3-10
3.2.4.1.1 Ballot Standards .....	3-10
3.2.4.1.2 Punching Devices .....	3-10
3.2.4.1.3 Marking Devices .....	3-11
3.2.4.1.4 Frames or Fixtures for Punchcard Ballots.....	3-11
3.2.4.1.5 Frames or Fixtures for Printed Ballots .....	3-12

3.2.4.1.6 Voting Booths .....	3-12
3.2.4.1.7 Ballot Boxes and Ballot Transfer Boxes.....	3-12
3.2.4.2 Electronic Systems Recording Requirements.....	3-13
3.2.4.2.1 Enclosure .....	3-13
3.2.4.2.2 Activity Indicator.....	3-14
3.2.4.2.3 Vote Recording.....	3-14
3.2.4.2.4 Recording Accuracy .....	3-14
3.2.4.2.5 Recording Reliability .....	3-15
3.2.4.2.6 Public Counter.....	3-15
3.2.4.2.7 Protective Counter .....	3-16
3.2.5 Paper Based Conversion Requirements .....	3-16
3.2.5.1 Ballot Handling .....	3-16
3.2.5.1.1 Outstacking .....	3-16
3.2.5.1.2 Multiple Feed Prevention .....	3-17
3.2.5.2 Ballot Reading.....	3-17
3.2.5.2.1 Reading Accuracy .....	3-17
3.2.5.2.2 Reading Reliability.....	3-18
3.2.6 Processing Requirements .....	3-18
3.2.6.1 Paper Based System Processing Requirements.....	3-18
3.2.6.1.1 Processing Accuracy .....	3-19
3.2.6.1.2 Memory Stability.....	3-19
3.2.6.2 Electronic System Processing Requirements .....	3-19
3.2.6.2.1 Processing Speed .....	3-19
3.2.6.2.2 Processing Accuracy .....	3-20
3.2.6.2.3 Memory Stability.....	3-20
3.2.7 Reporting Requirements .....	3-20
3.2.7.1 Removable Storage Media .....	3-20
3.2.7.2 Communication Devices.....	3-21
3.2.7.3 Printers.....	3-21
3.2.8 Vote Data Management Requirements .....	3-21
3.2.8.1 Data File Management.....	3-22
3.2.8.2 Data Report Generation .....	3-22
3.3 Physical Characteristics .....	3-22
3.3.1 Size.....	3-22
3.3.2 Weight .....	3-22
3.3.3 Transport and Storage of Portable Systems .....	3-23
3.3.4 Security.....	3-23
3.3.5 Transportability .....	3-23

3.4 Design, Construction, and Maintenance Characteristics .....	3-24
3.4.1 Materials, Processes and Parts.....	3-24
3.4.1.1 Ballot Cards.....	3-24
3.4.1.2 Ballot Printing .....	3-25
3.4.1.2.1 Punchcard Ballots.....	3-25
3.4.1.2.2 Marksense Ballots .....	3-25
3.4.1.3 Punching Stylus.....	3-25
3.4.1.4 Vote Recorder.....	3-26
3.4.2 Durability.....	3-26
3.4.3 Reliability.....	3-26
3.4.4 Maintainability .....	3-26
3.4.4.1 Elements of Maintainability.....	3-27
3.4.4.2 Mean Time to Repair (MTTR) Guidelines .....	3-27
3.4.5 Availability (Ai).....	3-28
3.4.6 Environmental Conditions .....	3-28
3.4.7 Electromagnetic Radiation .....	3-29
3.4.8 Electrostatic Test (ESD).....	3-29
3.4.9 Magnetic Susceptibility Test.....	3-29
3.4.10 Product Marking.....	3-29
3.4.11 Workmanship.....	3-30
3.4.12 Interchangeability.....	3-30
3.4.13 Safety.....	3-30
3.4.14 Human Engineering—Controls and Displays .....	3-31



# 3

## Hardware Standards

---

### 3.1 Introduction

---

#### 3.1.1 Scope

---

This section contains the performance characteristics, physical characteristics, and design, construction and maintenance characteristics for the hardware and selected related components of all voting systems, specifying the minimum values for key attributes of these characteristics. This section focuses predominantly on the devices utilized in the design and manufacture of voting systems, encompassing components such as:

- ◆ Ballot printers;
- ◆ Ballot cards;
- ◆ Ballot displays;
- ◆ Voting devices, including punching and marking devices and electronic recording devices;
- ◆ Voting booths and enclosure;
- ◆ 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.

For electronic vote recording devices used as part of an Internet Voting system, the standards contained in this section also apply to:

- ◆ General purpose devices (such as personal computers) acquired by the jurisdiction for the purpose of poll site Internet voting;
- ◆ General purpose devices acquired by others (such as school systems, libraries, military installations and other public organizations) for the purpose of voting at sites supervised by election officials; and
- ◆ Devices designed solely for remote Internet voting by individuals.

This section is not intended to apply to multi-purpose devices such as personal computers (PCs) and personal data assistants (PDAs) owned by the voter or third persons (e.g., employer, library, hotel, college,) which are utilized for remote Internet voting at uncontrolled locations. However, these devices, as well as those utilized at controlled voting locations, are subject to the security requirements of Section 6 of these Standards.

This section describes the requirements for voting devices that are intended for use by individuals without disabilities. Section 2.2.5 describes the functional and performance requirements for voting devices intended for use by individuals with disabilities.

This section also applies to the combination of software with hardware to accomplish specific performance and system control requirements. Standards that are specific to software alone are provided in Section 4 of these Standards.

### 3.1.2 Organization of this Section

---

The standards presented in this section are organized as follows:

- a. *Performance Requirements*, which represent the combined operational capability of both system hardware and software across a broad range of parameters (see below);
- b. *Physical Requirements*, which address the size, weight and transportability of voting systems; and
- c. *Design, Construction and Maintenance Requirements*, which address the reliability and durability of materials, product marking, quality of system workmanship, safety and other attributes to assure smooth system operation in the voting environment.

The *Performance Requirements* address a broad range of parameters, encompassing:

- a. Environmental requirements, where no distinction is made between requirements for paper based and electronic systems, but requirements for precinct and central count are described;
- b. Control requirements, where no distinction is made between requirements for paper based and electronic systems;
- c. Vote recording requirements, where separate and distinct requirements are delineated for paper based and electronic systems;
- d. Conversion requirements, which apply only to paper based systems;
- e. Processing requirements, where separate and distinct requirements are delineated for paper based and electronic systems;
- f. Reporting requirements, where no distinction is made between requirements for paper based and electronic systems, but where differences between precinct and central count systems are readily apparent based on differences of their reporting; and
- g. Vote data management requirements, where no differentiation is made between requirements for paper based and electronic systems.

The *Performance Requirements* include such attributes as ballot reading and handling requirements, system accuracy, memory stability, and the ability to withstand specified temperature, vibration, and shock tests. These characteristics also encompass system wide requirements for shelter, electrical supply, and compatibility with data networks.

## **3.2 Performance Requirements**

---

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 two distinct attributes in operational testing (exclusive of code review).

- a. , During system performance, the desired maximum system-level data error rate shall be no more than 1 in 1,000,000; that is for the recording, storage, and reporting of individual characters and markings, the error rate shall be no more than one in one million characters/marks. For example, when scanning votes for individual candidates and contests on a ballot card the maximum acceptable error rate shall be no more than one error in one million ballot positions.

- b. Quantitative system reliability shall be measured by the number of unrecoverable failures in a time-based operating test consisting of no less than 163 cumulative hours (with no failures); and
- c. All hardware performance requirements shall be met under operating conditions and after storage under non-operating conditions.

### 3.2.1 Environmental Requirements

---

The environmental requirements for voting systems include shelter, space, furnishings and fixtures, supplied energy, environmental control equipment, and external telecommunications services. The Technical Data Package (TDP) supplied by the vendor shall include a statement of all requirements and restrictions regarding environmental protection, electrical service, telecommunications service, and any other facility or resource required for the installation and operation of the system.

#### 3.2.1.1 Shelter Requirements

---

All precinct count systems shall be capable of being stored and operated in any enclosed and habitable facility ordinarily used as a warehouse or polling place, with prominent instructions as to any special storage requirements.

#### 3.2.1.2 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, or the orderly flow of voters through the polling place.

#### 3.2.1.3 Furnishings and Fixtures

---

Any furnishings or fixtures provided as a part of voting systems, and any components not a part of these systems but that are used to support its storage, transportation, or operation, shall comply with the design and safety requirements of Subsection 3.4.

#### 3.2.1.4 Electrical Supply

---

Components of voting systems that require electrical supply system shall meet the following minimum 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. Precinct count systems shall also be capable of operation for a period of at least 16 hours on battery energized power supply. This capability shall include the provision of all power required to:
  - 1) activate voting, vote recording (in electronic systems), and ballot counting (in paper based systems);
  - 2) display all system status and error messages; and
  - 3) maintain the contents of program and data memory. This capability does not require the provision of illumination of the voting area, nor does it include the production of an output report of the voting data.

#### 3.2.1.5 Environmental Control

---

Equipment used for election management activities or vote counting (including both precinct and central count systems) shall withstand storage temperatures ranging from -15 to +150 degrees Fahrenheit, and be capable of operation throughout the temperature range of 40 to 100 degrees Fahrenheit.

#### 3.2.1.6 Data Networks Guidelines

---

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 these Standards and the Security requirements described in Section 6..

#### 3.2.2 Control Requirements

---

The *Control Requirements* for voting systems consists of the physical devices, and software (supplemented by administrative procedures) that accomplish and validate specific election operations in all systems.

### 3.2.2.1 Equipment Preparation

---

Equipment preparation includes all operations necessary to install ballot displays, software, and memory devices in each electronic voting device and in each counting device for paper-based systems. The system shall be designed in such a manner as to:

- a. provide a capability for automated validation of ballot and software installation;
- b. detect errors arising from incorrect or improper installation; and
- c. notify an election official of detected errors immediately.

### 3.2.2.2 Pre-Election Testing

---

Prior to setup at the polling place, or at any location where diagnostic and maintenance support are unavailable, all voting and counting devices prepared as in the foregoing paragraph are subjected to a series of tests. The requirements for all precinct count and central count systems address hardware and software required to support these tests, and the collection of data that verifies device readiness. 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 providing 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.

### 3.2.2.3 Tests at the Polling Place

---

To activate opening of the polling place, specifically, preparing precinct count system voting devices to accept voted ballots, the system shall provide the capabilities to test each device prior to opening to verify that each is in correct operational status. The tests supported shall include, as a minimum:

- a. production of a diagnostic test record indicating that there are no hardware or software failures;
- b. identification of the device and its designated polling place location;
- c. confirmation that there are no data stored in memory locations reserved for voting data; and

- d. confirmation that the device is ready to be activated for voting.

#### 3.2.2.4 Tests at Central Counting Facilities

---

To allow opening or activation of central count facilities, specifically, preparing central count system voting devices to accept voted ballots, the system shall provide the capabilities to test each counting device prior to opening to verify that each is in correct operational status. The tests supported shall include, as a minimum:

- a. production of a diagnostic test record indicating that there are no hardware or software failures;
- b. identification of the device and its designated location;
- c. confirmation that there are no data stored in memory locations reserved for voting data; and
- d. confirmation that the device is ready to be activated for processing.

#### 3.2.2.5 Opening the Polling Place (Precinct Count Systems)

---

To activate the opening of the polling place that is, 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 the preceding section have been successfully completed; and
- b. automatic disabling from voting of any device that has not been tested until it has been tested.

#### 3.2.2.6 Activating a Ballot (Electronic Systems)

---

To activate the ballots to be used in specific elections, the system shall provide the following capabilities:

- a. activate the casting of a ballot in a general election;
- b. in a primary election, to select the party affiliation declared by the voter;
- c. activate all portions of the ballot upon which the voter is entitled to vote; and
- d. disable any portion of the ballot upon which the voter is not entitled to vote.

### 3.2.2.7 Error Recovery (Precinct Count System)

---

To accomplish recovery 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 prior to the error or failure, without loss or corruption of voting data previously stored in the device;
- b. resumption of normal operation following the correction of a failure in a memory component, or in a data processing component, including the central processing unit;
- c. recovery from any other external condition, which causes a voting device to become inoperable, provided that catastrophic electrical or mechanical damage due to external phenomena has not occurred; and
- d. for voting systems other than electronic systems equipment, checkpointing may be acceptable provided it occurs frequently enough to minimize the amount of re-processing needed to recover from an error condition.

### 3.2.2.8 Closing the Polling Place

---

To activate closing of the polling place that is, disabling the casting of additional ballots, and enabling the production of voting data reports, the system shall provide the following capabilities:

- a. an internal test or diagnostic capability which verifies that the prescribed closing procedure has been followed, and that the device status is normal; and
- b. production of a diagnostic test record that verifies the sequence of events, and indicates that the extraction of voting data has been activated.

### 3.2.2.9 Polling Place Reports

---

If a report of voting data for the polling place is required to be generated at the polling place, the system shall provide a capability to produce a report of consolidated data from all system devices in the polling place.

### 3.2.3 Election Management System Requirements

---

The *Election Management System Requirements* address electronic hardware and software required 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 Accuracy

---

Voting systems shall meet the following requirements for recording accurately all election management data entered by the user, including election officials, vendors or contractors:

- a. Detect every selection made by the user;
- b. Add permissible 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 user, such as text, line art, logos, and images.
- e. Verify the correctness of detection of data entered directly by the user and the addition of the selections correctly to memory;
- f. Preserve the integrity of election management data stored in memory against corruption by stray electromagnetic emissions, and internally generated spurious electrical signals;
- g. Achieve an error rate not to exceed one error in one million characters, as applied independently to the voting data memory and to the user's data recording devices. (Recording accuracy may be achieved or enhanced by the incorporation of multiple detection and memory elements that employ device-polling techniques); and
- h. Corrected data errors shall in these instances be logged by the system.

#### 3.2.3.2 Memory Stability

---

Electronic system memory devices, used to retain election management data, shall have demonstrated at least a 99.95 percent probability of 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.

## 3.2.4 Vote Recording Requirements

---

The *Vote Recording Requirements* address paper based equipment and electronic hardware and software required to record voter choices. There are separate and distinct requirements for paper based and electronic systems.

### 3.2.4.1 Paper Based Recording Requirements

---

The paper based recording requirements address ballot cards or sheets, punching devices, marking devices, frames or fixtures to hold the ballot while it is being punched, and pages or assemblies of pages containing ballot field identification data. They also address compartments or booths where votes may be conveniently recorded and that screen the ballot being voted from the view of others, and secure containers for the collection of voted ballots.

#### 3.2.4.1.1 Ballot Standards

---

Paper ballots utilized by voting systems shall meet the following standards:

- a. Ballot cards or sheets shall meet the specifications stated by the vendor with respect to formulation, size, thickness, color, watermarks, layout, size and style of printing, arrangement of offices, and size and location of punch or mark fields.
- b. Punchcard ballots and some Marksense ballots may be counted or recounted on various card readers; therefore, card stock, size, opacity, color, field layout, orientation, folding, and bleedthrough shall be specified by the vendor and ballots shall conform to the specifications.
- c. Printed or punched timing marks may be used for synchronizing the detection of voting punches or marks, provided that they do not appear in any of the data fields.

#### 3.2.4.1.2 Punching Devices

---

Punching devices utilized by voting systems shall:

- a. be suitable for the type of ballot card used,
- b. be designed and constructed so as to facilitate the clear and accurate recording of each vote intended by the voter,
- c. incorporate features to ensure that the chad (debris) is completely removed, without damage to other parts of the ballot card, and

- d. meet the durability and reliability requirements of this Section.

Punching devices shall be deemed suitable for use if ballots marked by them meet the system performance requirements specified previously.

#### 3.2.4.1.3 Marking Devices

---

Marking devices utilized by voting systems shall meet the following standards:

- a. Marking devices shall be constructed of any materials suitable for the intended use, provided that they meet the durability and reliability requirements of Subsections 3.4.2 and 3.4.3.
- b. Marking devices shall be deemed suitable for use if ballots marked by them meet the system performance requirements specified previously.
- c. Vendors shall provide detailed specifications for the pens to be used with marking devices, identifying:
  - 1) specific characteristics of pens that affect readability of marked ballots;
  - 2) performance capabilities with regard to each characteristic; and
  - 3) for pens manufactured by multiple external sources, a listing of sources and pen model numbers that are compatible with the system.

#### 3.2.4.1.4 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.
- 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 may be satisfied by equipment of a different design but similar in intent to the workings described above as long as they achieve the same result as the standards with regard to:
  - 1) positioning of the card;
  - 2) association of ballot label information with corresponding punch fields;
  - 3) enabling of only those voting fields which correspond to the format of the ballot; and

- 4) punching of the fields and for the positive removal of chad).

#### 3.2.4.1.5 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. be designed and constructed to 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 Subsection 3.4.

#### 3.2.4.1.6 Voting Booths

---

Voting booths, whether integral with the voting system or supplied as components of the voting system, shall comply with the following requirements:

- a. provide an enclosure, which is integral with or makes provision for the installation of the ballot punching or marking device;
- b. ensure by its structure stability against movement or overturning during entry, occupancy, and egress by the voter;
- c. provide privacy for the voter, and be designed in such a way as to prevent observation of the ballot by any person other than the voter;
- d. provide interior space and lighting sufficient to make the process of vote recording convenient and accessible to voters without physical handicap; and
- e. if the design and construction of the voting booth is such that it cannot be conveniently used by voters with disabilities relating to vision, hearing, cognitive abilities, physical mobility, or fine motor skills, then each polling place shall be equipped with at least one station, meeting the criteria listed above, that can be used by voters with these handicaps.

#### 3.2.4.1.7 Ballot Boxes and Ballot Transfer Boxes

---

Ballot boxes and ballot transfer boxes serve as secure containers for the storage and transportation of voted ballots, and shall comply with the following requirements:

- a. be provided in a size, shape, and weight commensurate with their intended use;



- b. incorporate locks and seals as required by the statutes and procedures of the jurisdictions in which they are used; and
- c. for both precinct and central count systems, may 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 cause such ballots to be marked with an identifying spot or stripe to facilitate manual segregation.

### 3.2.4.2 Electronic Systems Recording Requirements

---

The electronic 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 ones. The requirements also address the physical environment in which ballots are cast.

#### 3.2.4.2.1 Enclosure

---

Electronic systems shall provide an enclosure for the voting device whereby the enclosure complies with the following requirements:

- a. The voter is able to enter the enclosure prior to any other action related to the voting process.
- b. The structure of the enclosure ensures its stability against movement or overturning during entry, occupancy, and egress by the voter.
- c. The enclosure provides privacy for the voter, and is designed in such a way as to prevent observation of the ballot display by any person other than the voter.
- d. The enclosure provides interior space and lighting sufficient to make the process of vote recording convenient and accessible to voters without physical handicap.
- e. If the design and construction of the enclosure is such that it cannot be conveniently used by voters with sensory (including visual), physical, cognitive, or personal compatibility disabilities as described in Section 2.2.5 of these Standards, then each polling place shall be equipped with at least one station, meeting the criteria listed above, that can be used by voters with these disabilities.

#### 3.2.4.2.2 Activity Indicator

---

Electronic systems shall provide an activity indicator that meets the following requirements:

- a. Each electronic voting device shall be equipped with an audible or visible means for the poll worker indicating that the device has been activated for voting, and that a ballot has been cast.
- b. This indicator shall be capable of activation or inactivation as required by the using jurisdiction.

#### 3.2.4.2.3 Vote Recording

---

Electronic systems shall provide vote recording capabilities that meet the following requirements:

- a. Electronic systems shall contain all mechanical, electromechanical and electronic components, and software and controls required to detect and record the activation of candidate and contest selections, write-in vote selections, made by the voter in the process of casting a ballot.
- b. Electronic systems shall incorporate multiple memories, both in the voting machine and in its programmable memory device, with polling to detect any discrepancy in the content of individual memories. These systems shall also maintain an electronic or physical image of each ballot, in an independent data path.
- c. Electronic systems shall maintain a record of each ballot cast, in a manner independent and distinct from the main vote detection, interpretation, processing and reporting path, while protecting the anonymity of each voter (for example, by means of storage location scrambling). The system shall be capable of reproducing these ballot images in human readable form.
- d. The vote recording capability shall ensure that recorded ballot images protect the integrity of the data and the anonymity of the voter. 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.

#### 3.2.4.2.4 Recording Accuracy

---

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

- a. Detect every selection made by the voter;

- b. Add permissible selections correctly to the memory components of the device;
- c. Verify the correctness of detection of the voter selections and the addition of the selections correctly to memory;
- d. Preserve the integrity of voting data and ballot images (for electronic machines) stored in memory against corruption by stray electromagnetic emissions, and internally generated spurious electrical signals;
- e. Achieve an error rate not to exceed one error in one million selections, as applied independently to the voting data memory and to the ballot image recording devices. (Recording accuracy may be achieved or enhanced by the incorporation of multiple detection and memory elements that employ device-polling techniques); and
- f. Corrected data errors shall in these instances be logged by the system.

#### 3.2.4.2.5 Recording Reliability

---

Recording reliability refers to the ability to sustain accuracy during the required operating period. Electronic systems shall reliably support the collection and retention of voting data in the voting device and the transmission of voting data among devices. The retention, transmission, and collection of voting data shall be subject to the following standards during national qualification testing:

- a. Demonstrate a MTBF of at least 163 hours with the exception of Internet vote data servers; and
- b. Demonstrate a MTBF of at least 336 hours for Internet vote data servers.

#### 3.2.4.2.6 Public Counter

---

Electronic systems shall be equipped with a public counter on each voting device that meets the following requirements:

- a. Can be set to zero prior to opening of the polling place;
- b. Records the number of ballots cast during that particular election;
- c. Is incremented only by the casting of a ballot;
- d. Prevents disabling or resetting by other than authorized persons after the polls close; and
- e. Is visible to all designated polling place officials so long as the device is installed at the polling place.

#### 3.2.4.2.7 Protective Counter

---

Electronic systems shall be equipped with a protective counter on each voting device that meets the following requirements:

- a. Records all of the testing and election ballots cast since the unit was built;
- b. Maintains a reading cannot be changed by any cause other than the casting of a ballot;
- c. Is incapable of ever being disabled or reset; and
- d. Is visible at all times when the device is configured for test, maintenance, or election use.

### 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, which 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 the acceptance of a ballot card, its movement through the read station, and transfer into a collection station or receptacle. The speed of ballot handling is not important for precinct count systems into which the voter, or a polling place official, places the ballots one at a time. However, speed is important to central count systems. Speed capabilities for central count systems and their card readers shall be cited by the vendor.

##### 3.2.5.1.1 Outstacking

---

This requirement refers to the ability of the card readers designed specifically for a voting system to divert unread cards, or when some condition is detected requiring that the cards be segregated from normally processed ballots, and given special handling.

- a. Both precinct and central count systems shall provide, as a minimum, the ability to segregate or to place an identifying mark on unprocessed cards, and

to segregate or mark cards containing write-in votes, if the candidate's name is entered on the card rather than on a card stub.

- b. If the design of the card reader does not provide for outstacking, then any of the conditions referred to in the preceding paragraph shall cause the card reader to stop. A status message will be displayed permitting the operator to remove the card(s) requiring special handling from the remainder of the deck.
- c. Alternatively, such ballots may be marked with an identifying flag to facilitate their identification and removal.

#### 3.2.5.1.2 Multiple Feed Prevention

---

This paper based system requirement refers to the ability of the reader to prevent the feeding of more than one card at a time, or to detect and to provide an alarm indicating the presence of more than one ballot card passing through the read station simultaneously.

- a. If multiple feed is detected, the card reader shall halt in a condition 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 5000.

#### 3.2.5.2 Ballot Reading

---

This paper based system requirement is limited to the conversion of the physical ballot image into an analogous electronic image. The requirements for interpretation of the electronic image are described in Section 3.2.6, *Processing Requirements*. Requirements for ballot reading include accuracy and reliability.

##### 3.2.5.2.1 Reading Accuracy

---

This paper based system attribute refers to the inherent capability of the read heads to respond to vote punches or marks, and to discriminate between valid punches or marks and extraneous perforations, smudges, and folds.

It includes the conversion of the output of the read head electronic circuitry into digital signals. Conversion of the output is in response to the presence or absence of a valid voting punch or mark, and not to the presence of signals failing to meet the detection criteria of a valid punch or mark.

Paper based systems shall meet the following accuracy requirements applying to both the presence and to the absence of a punch or mark in any active ballot field.

- a. Valid punches or marks shall be detected, invalid punches or marks shall be rejected, and no detection signal shall be accepted in the absence of a valid punch or mark.
- b. Conversion testing shall be performed using all potential ballot positions as active positions.
- c. For systems without pre-designated ballot positions, ballots with active position density shall be used.
- d. The error rate measured by this criterion shall not exceed one error in one million ballot fields.

#### 3.2.5.2.2 Reading Reliability

---

This paper based system attribute refers to the ability of the system to sustain accuracy during the required operating period.

- a. In addition to the reliability requirements contained in Section 3.4.3 *Reliability*, the system shall reliably read ballots that contain vote marks meeting reasonable criteria for placement, size, and intensity.
- b. The rate of rejection of voted ballots shall not exceed 3 percent.

### 3.2.6 Processing Requirements

---

Processing requirements address 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 electronic voting systems are presented below.

#### 3.2.6.1 Paper Based System Processing Requirements

---

The paper based processing requirements address all mechanical, electromechanical, 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 as vote selection error rate, the ratio of uncorrected vote selection errors to the total number of vote selection points that could be recorded across all ballots when the system is operated at its nominal or design rate of processing, in a time interval of 4 hours.
- 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.
- d. For all paper based systems, the Maximum Acceptable Value (MAV) for the vote selection error rate shall be 1 in 1,000,000 selection points.

#### 3.2.6.1.2 Memory Stability

---

Paper based system memory devices, used to retain control programs and data, shall have demonstrated at least a 99.95 percent probability of 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 Electronic System Processing Requirements

---

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

#### 3.2.6.2.1 Processing Speed

---

Electronic 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 (less than 250 milliseconds) delay;
- b. Extract voting data from a voting device by electronic means in a time not to exceed one minute; and

- c. 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 electronic voting devices, or in removable memory modules installed in them. Processing includes all operations on the data performed after the polling places have been closed to consolidate voting data at the polling place. Electronic voting systems shall meet the following requirements for processing accuracy:

- a. All reports are completely consistent, with no discrepancy among reports of voting device data produced at any level.
- b. Consolidated reports containing absentee, provisional, or other voting data 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

---

Electronic system memory devices, used to retain control programs and data, shall have demonstrated at least a 99.95 percent probability of 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* address 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 and, where used, communications devices for transportation or transmission of data to other sites.

#### 3.2.7.1 Removable Storage Media

---

In voting systems that utilize removable 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 memory stability equal to at least a 99.95



percent probability of error-free retention for a period of 22 months under the environmental conditions for operation and non-operation contained in Section 3.2.1.

Examples of removable storage media include: programmable read-only memory (PROM), random access memory (RAM) with battery backup, and magnetic tape or disk media.

### 3.2.7.2 Communication Devices

---

Components that may be incorporated in or attached to devices of all systems for transmitting tabulation data to another data processing system, printing system or display device, shall not be used for the preparation or printing of an official canvass of the vote unless they conform to the requirements described in Section 5 of the Standards.

### 3.2.7.3 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:

- a. consolidate voting data from polling place data memory or transfer devices;
- b. report polling place summaries; and
- c. process absentee ballots, manually input data, and administrative ballot definition data.

The requirements address both hardware and software required to generate all 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 provision 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, which affect their general utility and suitability for election operations.

### 3.3.1 Size

---

There are no numerical limitations to the size of any voting system, but it should be compatible with its intended usage.

### 3.3.2 Weight

---

There are no restrictions on equipment weight, provided that it is consistent with the environment in which the equipment is to be used.

The vendor shall specify the classification of the system, based on the following use environments, so that the proper classification can be used for the hardware transit drop test.

- a. *Portable* equipment is regularly transported between its operating location and a place of storage. It is typically installed and operated on a table or stand

to which it is not permanently affixed, or it is equipped with a collapsible or removal stand or base. It is intended to be hand-carried or handled by one person.

- b. *Movable* equipment is regularly transported between its operating location and a place of storage. It is typically equipped with a rigid stand or base, with or without wheels or rollers. It is intended to be handled by one or two persons, and handling may require the use of a dolly or lifting mechanism.
- c. *Fixed* equipment is intended for long-term or permanent placement in its operating location and is not regularly transported to and from a place of storage. It is typically equipped with an integral stand or base. It is intended to be handled by more than one person, and handling may require the use of a dolly or lifting mechanism.

### 3.3.3 Transport and Storage of Portable Systems

---

All portable systems shall meet the following requirements for transport and storage:

- a. provide a handle or handles to facilitate their handling, transport, and installation; and
- b. be capable of, or be provided with a protective enclosure rendering them capable of, withstanding:
  - 1) impact, shock and vibration loads accompanying surface and air transportation; and
  - 2) stacking loads accompanying storage.

### 3.3.4 Security

---

All types of equipment shall meet the security requirements described in Section 6 of these Standards.

### 3.3.5 Transportability

---

All types of voting systems, including portable, movable and fixed equipment systems, shall be capable of transport by road, rail, or air common carriers.

### **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.

- a. The frequency of equipment malfunctions and maintenance requirements shall be reduced to the lowest level consistent with cost constraints.
- b. Manufacturers shall prepare an Approved Parts List (APL) for submission as a part of the Technical Data Package.
- c. No unit submitted for qualification testing and no production units submitted for sale shall contain parts or components not included in the APL.

##### **3.4.1.1 Ballot Cards**

---

For paper-based voting systems, the ballot cards shall meet the following requirements:

- a. For ballots processed by general purpose card readers, utilize a card stock, punch configurations, and punch field locations complying with industry standards cited by the vendor for Automatic Data Processing (ADP) supplies and equipment;
- b. For ballots intended for use only with their parent system, utilize any material and configuration consistent with the requirements of the system; and
- c. As part of stock finishing, each distinct ballot configuration utilizes a unique identification code punched or marked for machine verification.

### 3.4.1.2 Ballot Printing

---

For paper based voting systems, the content and arrangement of printing on ballot cards affects the suitability of systems for election use. Printing shall comply with the regulations and specifications of the using agency. If such do not exist, then the requirements indicated below apply.

#### 3.4.1.2.1 Punchcard Ballots

---

For punchcard ballots:

- a. Printing on pre-scored cards shall consist of ballot format identification and punch field designation in a type font not smaller than 10 point.
- b. Printing on cards that are not pre-scored shall comply with the requirements for Marksense cards.

#### 3.4.1.2.2 Marksense Ballots

---

For marksense ballots:

- a. Legends and information other than the names of candidates or the statement of issues shall be printed in a type font not smaller than 12 point.
- b. The names of candidates and the titles of issues shall be printed in a type font not smaller than 10 point, and information associated with the name of the candidate or the statement of the issue shall be printed in a type font not smaller than 8 point.

### 3.4.1.3 Punching Stylus

---

The stylus for use with automatic punchcard systems shall meet the following requirements:

- a. suitable for use with the vote recorder and ballots used by the system;
- b. designed so as to reliably remove chad; and
- c. designed to avoid excessive damage or wear to vote recorder components.

#### 3.4.1.4 Vote Recorder

---

Vote recorders, which utilize ballots to be processed by general-purpose card readers, shall comply with industry standards cited by the vendor for punch configuration and location. Otherwise, they shall produce punched or marked ballot cards in any manner compatible with their parent system.

#### 3.4.2 Durability

---

The durability of all voting systems and their components refers to their ability to withstand normal use without premature deterioration or wearing out. This property can be measured in terms of design life: the period of time throughout which, on the average, individual devices will remain serviceable without incurring excessive maintenance costs. The design life of all voting system devices shall be 10 years.

#### 3.4.3 Reliability

---

The reliability of voting system devices refers to the mean time between failure (MTBF), defined as the value of the ratio of operating time to the number of failures which have occurred in the specified time interval. For the purpose of demonstrating compliance with this requirement, a failure is defined as any event that results in the loss or unacceptable degradation of one or more of the device functions. Voting system devices shall meet the following requirements during national qualification testing:

- a. Demonstrate a MTBF of at least 163 hours with the exception of Internet vote data servers; and
- b. Demonstrate a MTBF of at least 336 hours for Internet vote data servers.

#### 3.4.4 Maintainability

---

#### 3.4.4.1 Elements of Maintainability

---

The maintainability of voting systems represents the ease with which maintenance actions can be performed based on the design characteristics of the system. Maintenance actions include all scheduled and unscheduled events, which are performed to:

- a. determine the operational status of the system and its elements;
- b. adjust, align, or service circuits and components;
- c. replace a circuit or component having a specified operating life or replacement interval;
- d. repair or replace a circuit or component, which exhibits an undesirable predetermined physical condition or performance degradation;
- e. repair or replace a circuit or component, which has failed; and
- f. verify the restoration of a circuit, a component, or the system to operational status.

Qualitative characteristics of maintainability include:

- a. ease of access to internal components;
- b. presence of labels and the identification of test points;
- c. provision of built-in test and diagnostic circuitry or physical indicators of condition;
- d. ease with which adjustment and alignment can be performed; and
- e. presence of easily disconnected electrical and mechanical interfaces, which facilitate the removal and replacement of circuits and components.

#### 3.4.4.2 Mean Time to Repair (MTTR) Guidelines

---

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.

For all voting devices and components, their MTTR attributes should be sufficient to achieve, in combination with their MTBF, the required availability defined in Section

3.4.5. In addition, vendors shall specify the 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.

### 3.4.5 Availability (A<sub>i</sub>)

---

Availability is the probability that the voting system will respond to an operational demand. It is the ratio of the time during which the system is operational (up time) to the total time period (up time plus down time). Inherent availability (A<sub>i</sub>), is based upon MTBF and active repair time (MTTR), that is:

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

The system availability ratio for all voting systems shall be at least 0.99 during normal operation.

### 3.4.6 Environmental Conditions

---

Environmental conditions applicable to the design and operation of voting systems consist of the following categories:

- a. Natural environment, which includes the effects of temperature, humidity, and atmospheric pressure;
- b. Induced environment, including both the effects of use, such as the proper and improper operation and handling of the system and its components during the election processes;
- c. Effects of transportation and storage; and
- d. Electromagnetic signal environment, including exposure to and the generation of radio frequency energy.

All voting systems shall be designed to withstand the environmental conditions contained in the appropriate test procedure of these standards. These procedures will be applied to all devices for casting, scanning and counting ballots, except those that constitute commercial off-the-shelf devices which have not been modified in any



manner to support their use as part of a voting system and which have a documented record of performance under conditions defined in these Standards.

### 3.4.7 Electromagnetic Radiation

---

All voting systems shall meet the following requirements for electromagnetic radiation:

- a. Voting systems of all types shall comply with the Rules and Regulations of the Federal Communications Commission, Part 15 "Radio Frequency Devices," Subpart J, "Computing Devices."
- b. Voting systems of any type shall be considered "Class B" computing devices, as defined therein.

### 3.4.8 Electrostatic Test (ESD)

---

All devices shall be constructed such as to prevent static electricity from disrupting or disabling their proper operation.

### 3.4.9 Magnetic Susceptibility Test

---

All devices shall be constructed such as to prevent magnetic fields generated by other polling place or vote count equipment, or devices carried by voters or election officials, from disrupting or disabling their proper operation.

### 3.4.10 Product Marking

---

All voting systems shall meet the following requirements for product marking:

- a. All voting system components shall be identified 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, and its serial number. Power requirements, if any, shall also be specified.

- b. A separate data plate containing a schedule for and list of operations required to service or to perform preventive maintenance on the component shall be similarly affixed.
- c. Advisory caution and warning instructions to assure safe operation of the equipment and to avoid exposure to hazardous electrical voltages and moving parts shall be provided at all locations where operation or exposure may occur.

### 3.4.11 Workmanship

---

All voting systems shall meet the following requirements for workmanship:

- a. Manufacturers of all voting systems and components shall adopt and adhere to practices and procedures to ensure that their products are free from damage or defect that could make them unsatisfactory for their intended purpose.
- b. Manufacturers of voting systems that utilize components provided by external suppliers shall adopt and utilize practices and procedures that assure that supplied components are free from damage or defect that could make them unsatisfactory for their intended purpose.

### 3.4.12 Interchangeability

---

Manufacturers of voting systems and components shall utilize design and construction features that maximize interchangeability, thereby facilitating maintenance and the incorporation of product revisions or improvements.

### 3.4.13 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, which can result in personal injury or equipment damage, must be detected and corrected before voting systems and components are placed into service.
- c. Equipment design for personnel safety shall be equal to or better than the appropriate requirements of the Occupational Safety and Health Act (OSHA), as identified in Title 29, part 1910, of the Code of Federal Regulations.

### 3.4.14 Human Engineering—Controls and Displays

---

All voting systems and components shall be designed and constructed so as to simplify and facilitate the functions required, and to eliminate the likelihood of erroneous stimuli and responses on the part of the voter or operator. Other specific requirements for controls and displays are described below. In addition, specific functional requirements for system use by individuals with disabilities are described in Section 2.2.5 of these Standards.

All voting systems shall meet the following requirements for controls and displays:

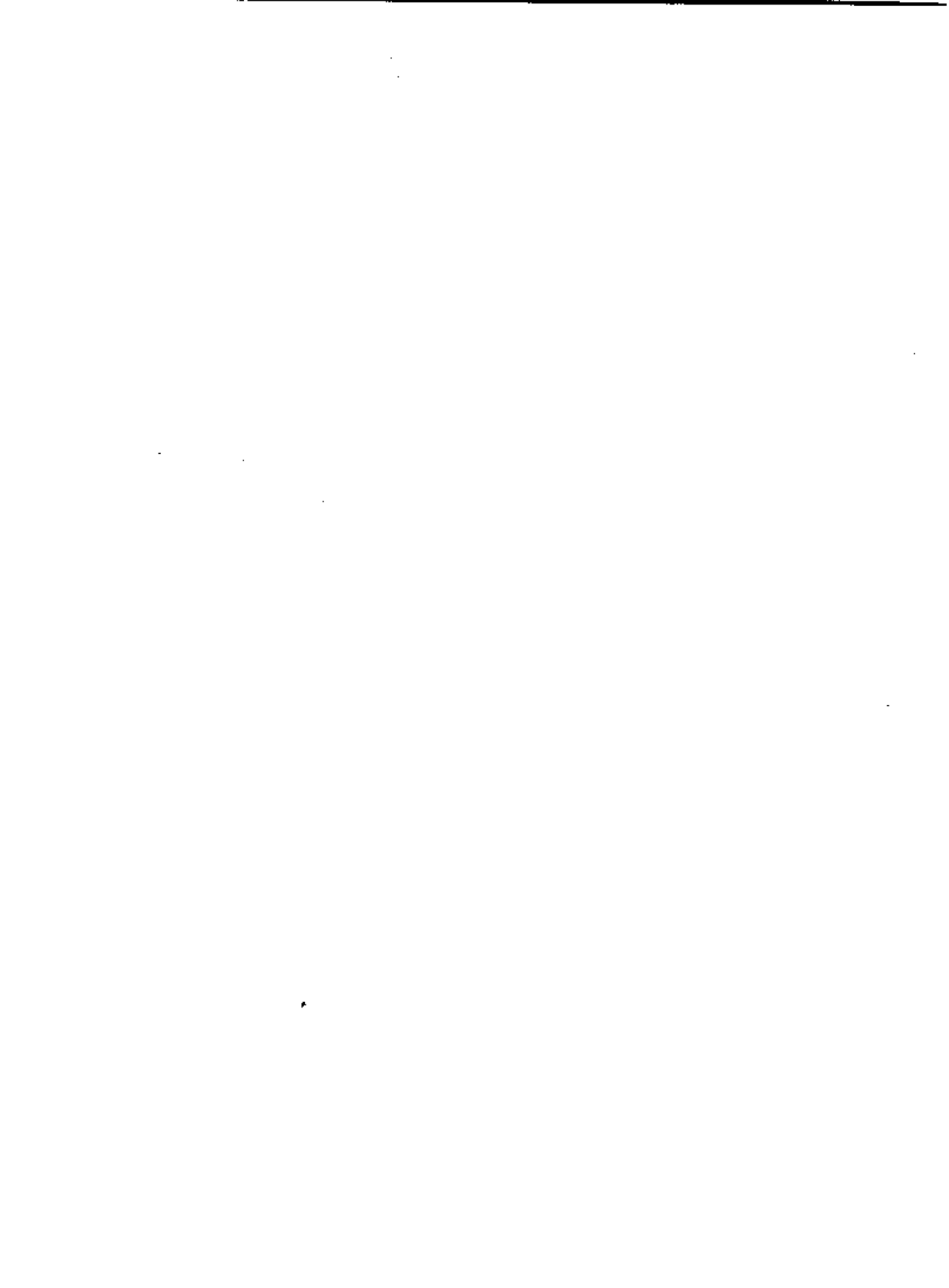
- a. In all systems, controls used by the voter or equipment operator shall be conveniently located, shall use designs that are consistent with their functions, and shall be clearly labeled. Instruction plates shall be provided, if they are necessary to avoid ambiguity or incorrect actuation.
- b. Information or data displays shall be large enough to be readable by a person with no disabilities and by individuals with disabilities consistent with the requirements defined in Section 2.2.5 of these Standards.
- c. Status displays shall meet the same requirements as data displays, and they shall also follow conventional industrial practice with respect to color:
  - 1) Green, blue, or white displays shall be used for indications of normal status;
  - 2) Amber indicators shall be used to indicate warnings or marginal status;
  - 3) Red indicators shall be used to indicate error conditions or equipment states that may result in damage, or in hazards to personnel; and
  - 4) unless the equipment is designed to halt under conditions of incipient damage or hazard, an audible alarm shall also be provided.



# Table of Contents

---

<b>4 Software/Firmware Standards</b> .....	<b>4-1</b>
4.1 Scope .....	4-1
4.1.1 Software Types .....	4-1
4.1.2 Software Sources .....	4-2
4.1.3 Location and Control of Software and Hardware on Which it Operates .....	4-2
4.1.4 Exclusions .....	4-3
4.2 Software Design and Coding Standards .....	4-3
4.3 Data Quality Assessment .....	4-3
4.4 Data and Document Retention .....	4-4
4.5 Audit Record Data .....	4-4
4.5.1 Pre-election Audit Records .....	4-5
4.5.2 System Readiness Audit Records .....	4-5
4.5.3 In-Process Audit Records .....	4-6
4.5.4 Vote Tally Data .....	4-7
4.6 Software for Internet Voting Systems .....	4-8
4.6.1 System Availability and Risk of Failure .....	4-8
4.6.2 Vote Accuracy and Integrity .....	4-8
4.6.3 Vote Privacy .....	4-9
4.6.4 Ballot Presentation .....	4-10
4.6.5 Ballot Acceptance and Storage at the Vote Server .....	4-10



# Software/Firmware Standards

---

## 4.1 Scope

---

This section describes essential design and performance characteristics of the software embodied in voting systems, addressing both system level software, such as operating systems, 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.

### 4.1.1 Software Types

---

The more general requirements of this section apply to software used to support the broad range of voting system activities, encompassing pre-voting, voting and post-voting activities. More specific requirements are defined for ballot counting, vote processing, the creation of an unalterable audit trail, and the generation of output reports and files. Requirements are also defined for Internet voting systems that address the unique characteristics and considerations of systems that support the casting of ballots over the Internet. Although this section emphasizes software, the standards described also influence hardware design considerations.

These 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 and 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.

## 4.1.2 Software Sources

---

The requirements of this section generally apply to all software developed for use in voting systems. These requirements apply to:

- a. Software provided by the voting system vendor and its component suppliers
- b. Software furnished by an external provider (for example providers of commercial off-the-shelf (COTS) operating systems and web browsers) where the software is potentially used in any way during voting system operation
- c. Software developed by the voting jurisdiction

## 4.1.3 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 and the ownership and location of the hardware on which the software is installed or operates. These requirements apply to:

- a. Software that operates on voting devices and vote counting devices installed at polling places under the control of the voting jurisdiction
- b. Software that operates on ballot printers, vote counting devices, and other hardware typically installed at central or precinct locations (including contractor facilities)
- c. Software that operates on voting devices (such as personal computers) under the control of individual voters and third persons other than the voting jurisdiction (e.g., employer, library, hotel, college) for use by the voter, such as for Internet voting systems

However, some requirements apply in only specific situations as 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 these Standards.



#### 4.1.4 Exclusions

---

This section is not intended to apply to general purpose non-voting software (e.g., operating systems, programming language compilers, database management systems, Web browsers) that is resident on a vote recording or counting device but which is not operationally supporting any voting related activities. For example, this section does not apply to an operating system that is resident on a personal computer used to record votes but which is bypassed by the installation of another operating system that controls the functioning of all software that supports voting related activities.

Compliance with the requirements of these software standards shall be assessed by means of code examination of the application software, as well as other formal tests. Commercial software will not be subject to code review. Some of the analysis and test requirements do not depend upon the design and coding of the software, but others do. The use of proven structured software design methods facilitates the necessary analysis and testing.

### 4.2 Software Design and Coding Standards

---

All voting system application software shall be designed in a modular fashion and shall not be self-modifying. Modular programs consist of code written in relatively small and easily identifiable sections, with each unit having a single entry point and a single exit point. Each module shall have a specific function that can be tested and verified more-or-less independently of the remainder of the code.

It is preferable, but not mandatory, that a high level programming language be used for that segment of the ballot tabulation software associated with the logical and numerical operations on vote data. Such languages include, but are not limited to: Visual Basic, Java, C and C++. It is similarly preferable that structured programming techniques, which embody constraints on module entry and exit conditions, and on the manner in which internal logical tests and operations are implemented, be utilized.

The preferential 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.

### 4.3 Data Quality Assessment

---

All systems shall provide data quality assessment capabilities that meet the following minimum requirements:

- a. Provide real-time monitoring of system status and data quality. The methods of assessment is determined by the vendor. Implementation options include but are not limited to: (1) hardware monitoring of redundant processing functions which are carried out in parallel or serially; and (2) statistical assessment and measures of system operation.
- b. Provide measurement of the relative frequency of entry to program units, and the frequency of exception conditions, as part of the quality assessment.

## **4.4 Data and Document Retention**

---

All systems shall contain provisions for maintaining the integrity of voting and audit data during an election, and for a period of 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. These provisions shall include protection 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. Specific data that need to be retained are described in *Section 2.2.8, Retention of Data*.

Prior to system qualification, each vendor shall submit to the Federal Election Commission a written request for information regarding the types and respective formats of election specific data that must be retained by the user jurisdictions for a 22-month period in accordance with United States Code Title 42, Sections 1974 through 1874e (as described in Section 2.4.4 of these Standards). For each system, the vendor shall present detailed operational characteristics, such that FEC can rule on specific data and document items and their preferable media (manual and/or electronic format) that are to be retained for the auditability and reconstruction of the election process.

## **4.5 Audit Record Data**

---

Election audit trails are essential to ensure the integrity of a voting system. Operational requirements for audit trails are described in Section 2.2.3 of these Standards. Audit record data are generated by these procedures. The audit record requirements listed in the following subsections are considered 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.

## 4.5.1 Pre-election Audit Records

---

The following minimum requirements apply to *Pre-election Audit Records*:

- a. During election definition and ballot preparation phases, an audit log shall be maintained of completion of the baseline ballot formats and modifications to them, a description of these modifications, and corresponding dates. These data are required to verify the election-specific database has been correctly prepared and maintained throughout subsequent modifications to the baseline format.
- b. The pre-election audit log shall include manual data maintained by election personnel, samples of all final ballot formats, and the ballot preparation edit listings associated with them.

## 4.5.2 System Readiness Audit Records

---

The following minimum requirements apply to *System Readiness Audit Records*:

- a. Prior to the initiation of ballot counting, software shall be able to verify hardware and software status through 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 capability shall test ballot formats to be processed, verifying:
  - 1) the allowable number of votes for an office or issue;
  - 2) the combinations of voting patterns permitted or required by the using jurisdiction;
  - 3) the inclusion or exclusion of offices or issues as the result of multiple districting within the polling place; and
  - 4) any other characteristics that may be peculiar to the jurisdiction, the election, or the polling place's location
- d. The software shall ensure non-contamination of voting data through checks of all data paths and memory locations to be used in actual vote recording.
- e. Upon the conclusion of the tests, the software shall provide evidence in the audit record that the test data have been expunged.

- f. For paper based systems only, the readiness audit capability shall evaluate the accuracy of the ballot reader and the arithmetic-logic unit. It shall allow the processing, or simulated processing, of sufficient test ballots to provide a statistical estimate of processing accuracy.

### 4.5.3 In-Process Audit Records

---

In-process audit records consist of data documenting precinct and central count system operation during diagnostic routines and the casting and tallying of paper-based ballots. At a minimum, the in-process audit records shall contain the following items, which apply to all systems, except as otherwise noted:

- a. Machine generated error and exception messages to ensure that successful recovery has been accomplished. Examples include, but are 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 log-in or access errors, file access errors, and physical violations of security as they occur, and a summary record of these events after processing
  - 5) For paper based systems, an event log of any ballot-related exceptions such as:
    - i. Quantity of ballots that are not processable
    - ii. Quantity of ballots requiring special handling
    - iii. In a central count environment, the quantity and identification number of aborted precincts
  - 6) 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
  - 4) For electronic machines at controlled voting locations, the event (and time, if available) of enabling/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. This information is not required in real-time and may, instead, be reported in log form. The intent is to gauge the accuracy of the ballot data and adequacy of the system in monitoring and detecting system processing errors. For example, a cumulative or summary record of data read-rite-verify, parity, or check-sum errors and retries is required.
  - 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.

#### 4.5.4 Vote Tally Data

---

In addition to the audit requirements described above, other election-related data are essential for reporting results to interested parties, the press, and the voting public, and are 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 to produce reports of them on a printer or at a terminal. At a minimum, vote tally data shall include:

- a. Number of ballots cast, by each ballot configuration/type;
- b. Candidate and measure vote totals for each contest;
- c. The number of ballots read within each precinct, by type, including totals for each party in primary elections;
- d. Separate accumulation of overvotes and undervotes for each race or issue (no overvotes would be indicated for electronic 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.

## **4.6 Software for Internet Voting Systems**

---

Voting over the Internet introduces considerations that are not addressed sufficiently by the standards for other forms of voting systems due to the inherent technical design differences of Internet voting systems. These considerations underlie additional software requirements pertaining to:

- a. system availability;
- b. vote accuracy and integrity, including precluding the changing of votes and identifying system malfunctions;
- c. vote privacy;
- d. ballot presentation; and
- e. ballot acceptance and storage at the server.

These requirements pertain in some instances to the voting machine, such as a personal computer, and in other instances to the facility used to store votes, commonly referred to as a vote server, which is operated at a Vote Server Data Center (VSDC). To provide maximum flexibility to system vendors, while assuring strong safeguarding of the integrity of the election process, the additional software requirements for Internet voting systems focus on specific objectives to be achieved and refrain to the extent possible from describing specific technical solutions.

### **4.6.1 System Availability and Risk of Failure**

---

Internet voting systems shall be designed and configured such that they are not vulnerable to a single point of failure resulting in the loss of voting capability at all of one or more controlled polling places.

### **4.6.2 Vote Accuracy and Integrity**

---

Internet voting systems shall meet the following software requirements for accuracy and integrity:

- a. Transmit an accurate copy of the voter's selections to the vote server with no reasonable possibility of undetected modifications anywhere in the transmission path in any of the intervening computers and networks, including within the voter's own machine or machine provided by a third person.
- b. Provide a capability to transmit test ballots regularly from all controlled voting machines to verify end-to-end integrity of the entire voting system. These ballots shall be undistinguishable from real ballots for all purposes except that they would not count in the final vote tally.
- c. Provide a reporting of test ballots that includes:
  - 1) Number of ballots sent
  - 2) When each ballot was sent
  - 3) Machine from which each ballot was sent
  - 4) Specific votes or selections contained in the ballot.
- d. Provide a storage media for the vote server that provides for redundant data storage
- e. Provide a storage media for the vote server that provides for backup by alternate power sources continuously during voting operations in the event of power failure.

### 4.6.3 Vote Privacy

---

Internet voting systems shall meet the following software requirements for vote privacy:

- a. Employ every reasonable technical means to prevent anyone from violating privacy anywhere along the path from the voter to the canvass. At a minimum, voting system software should check for the presence of the common kinds of remote control software, inform the voter of its presence, and not allow voting on the remotely monitored or controlled voting machine (such as a personal computer).
- b. Erase from the voting machine all record of the voter's vote immediately after the ballot is sent to the vote server or immediately after the voter chooses to cancel his/her choices. Any choices made shall be:
  - 1) Erased from the screen
  - 2) Deliberately erased from any memory.
- f. Store the voter's vote on the voting machine only in volatile memory so that it will be automatically erased in the event of a power failure or

rebooting of the machine. The encrypted and unencrypted vote shall not be:

- 1) Stored in any file, including temporary files, on the voting machine
- 2) Paged out to secondary storage as a result of virtual memory
- 3) Written to any log, cache, index, cookie, or other long-term record

#### 4.6.4 Ballot Presentation

---

Internet voting systems shall present all the information for a single contest (i.e., elected office, proposition, referendum, etc.) on a single screen page, with no scrolling required to view the information, while conforming to the minimum typeface size requirements of these Standards.

#### 4.6.5 Ballot Acceptance and Storage at the Vote Server

---

Internet voting systems shall meet the following software requirements for ballot acceptance and storage at the vote server:

- a. Wholly accept or wholly reject a ballot in its entirety at the vote server, with no acceptance of partial ballots.
  - 1) Preclude a voter from voting again if a ballot is accepted at the vote server.
  - 2) Permit a voter to vote again if a ballot is not accepted at the vote server.
- b. Check a ballot immediately at the vote server to ensure it is formatted correctly, and store it on a permanent medium (retaining its encrypted form) for later decryption and canvass, and to be considered part of the audit trail. If it is not formatted correctly, notify the user of the next action to take, and store it on a permanent medium (retaining its encrypted form).



# Table of Contents

---

<b>5 Telecommunications</b> .....	<b>5-1</b>
5.1 Scope.....	5-1
5.1.1 Types of Components .....	5-1
5.1.2 Telecommunications Operations and Providers .....	5-2
5.1.3 Data Transmissions .....	5-3
5.1.4 Organization of Standards .....	5-4
5.2 Performance Requirements .....	5-4
5.2.1 Accuracy/Integrity .....	5-5
5.2.2 Availability .....	5-5
5.2.3 Privacy .....	5-6
5.2.4 Confirmation .....	5-6
5.2.5 Reliability.....	5-6
5.2.6 Durability.....	5-7
5.2.7 Maintainability .....	5-7
5.2.7.1 Elements of Maintainability .....	5-7
5.2.7.2 Mean Time to Repair (MTTR) Guidelines .....	5-8
5.2.8 Response Time.....	5-8
5.3 Prohibitions (Pre-Voting, Voting, and Post Voting).....	5-9



# 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 these Standards, telecommunications is defined as the capability to transmit and receive data electronically over a distance using hardware and software components.

The requirements specified 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 official election results. This section, where applicable, 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.

### 5.1.1 Types of Components

---

This section addresses telecommunications hardware and software across a broad range of technologies including, but not limited to, the following:

- a. Dial-up communications technologies:
  - 1) Standard landline
  - 2) Wireless
  - 3) Microwave
  - 4) Very Small Aperture Terminal (VSAT)
  - 5) Integrated Services Digital Network (ISDN)

- 6) Digital Subscriber Line (DSL)
- b. High-speed telecommunications lines (public and private)
  - 1) FT-1, T-1, T-3
  - 2) Frame Relay
  - 3) Private line
- c. Cabling technologies:
  - 1) Universal Twisted Pair (UTP) cable (CAT 5 or higher)
  - 2) Ethernet hub/switch
  - 3) Wireless connections (Radio Frequency (RF) and Infrared)
- d. Communications routers
- e. Modems, including those internal and external to personal computers, computer servers, or other voting system components (whether installed at the polling place or central count location)
- f. Modem drivers, dial-up networking software
- g. Channel service units (CSU)/Data service units (DSU) (whether installed at the polling place or central count location)
- h. Dial-up networking applications software

### 5.1.2 Telecommunications Operations and Providers

---

This section applies to transmissions over public networks, such as those provided by regional telephone companies and long distance carriers, as well as private networks that may be employed by a jurisdiction. This section applies to private networks that transmit data between facilities (e.g., polling place and central office) regardless of whether the network is owned and operated by the election jurisdiction or by a third party, such as a telecommunications company, under contract to the jurisdiction.

- a. For systems that transmit data over public networks, including Poll Site Internet Voting systems, this Section applies to telecommunications components that are to be installed and operated at settings supervised by election officials, such as traditional polling places, and the central office. These standards apply to:
  - 1) Components acquired by the jurisdiction for the purpose of voting, including components installed at the poll site or central office (including central site facilities operated by vendors or contractors).
  - 2) Components acquired by others (such as school systems, libraries, military installations and other public organizations) which are utilized at

settings supervised by election officials, including minimum configuration components required by the vendor but which the vendor permits to be acquired from third party sources not under the vendor's control sources other than the vendor (e.g., router or modem card manufacturer or supplier)

- b. For Remote Internet Voting systems, this section applies to:
  - 1) Components acquired by the jurisdiction for the purpose of voting, including components installed at central office (including central site facilities operated by vendors or contractors).
  - 2) Telecommunications components that are required by the vendor to be installed and operated at the facility used to cast a ballot remotely, including facilities such as the voter's personal home computer or those of a third party, such as employer or university, designed to enable remote Internet voting from those facilities.

In addition to the components specified above, the telecommunications capabilities of the system as a whole are subject to the security requirements of Section 6 of these Standards.

### 5.1.3 Data Transmissions

---

These requirements apply to the use of telecommunications to transmit data during all of the three phases of voting activity described in *Section 1, Functional Requirements*: preparing the system for an election; conducting an election; and, afterwards, preserving the system data and audit trails. While this section does not assume a specific model of voting system operations and use of telecommunications to support operations, it does address, at a minimum, the following types of data transmissions:

- a. *Voter Registration Information Transmission*—Information that identifies the name and eligibility of a voter
- b. *Voter Key Transmission*—For Internet Voting Systems, coded information that uniquely identifies a voter for security purposes
- c. *Authentication of Security Information Transmission*—For Internet Voting Systems, coded information (typically used in an Internet Voting System) that confirms the identity of a voter for security purposes
- d. *Ballot Definition Transmission*—Information that describes to a voting machine the content and appearance of the ballots to be used in an election
- e. *Ballot Transmission to Voter*—For Internet Voting Systems, the transmission of the appropriate ballot image to an authenticated voter

- f. *Vote Transmission to County*—For Internet Voting Systems, the transmission of a single vote to the county (or contractor) for consolidation with other county vote data
- g. *Vote Count Transmission*—Information representing the tabulation of votes at any one of several levels: polling place, precinct, or central count
- h. *List of Voters Transmission*—A listing of the individual voters who have cast ballots in a specific election.

Additional data transmissions used to operate the 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, including all forms of Internet voting systems, this section applies to telecommunications hardware and software for transmissions between all combinations of senders and receivers indicated below:

- a. Polling places
- b. Precinct count facilities/locations
- c. Central count facilities/locations (whether operated by the jurisdiction or a contractor)
- d. Individual voter locations (for Remote Internet Voting systems)

#### 5.1.4 Organization of Standards

---

The standards presented in this section are organized as follows:

- a. *Performance Requirements*, which represent the combined operational capability of both telecommunications hardware and software across a broad range of parameters
- b. *Prohibitions*, which address specific data and combinations of data that shall not be transmitted in electronic form using telecommunications

### 5.2 Performance Requirements

---

Performance requirements for telecommunications represent the combined operational capability of both system hardware and software. These capabilities shall be considered basic to all data transmissions.

## 5.2.1 Accuracy/Integrity

---

*Accuracy/Integrity* represents the capability of the system to receive electronic signals that represent data provided by the sender and reproduce the data exactly at the point of receipt of the signals. This capability includes the ability to detect and correct automatically (i.e., without human intervention) data errors introduced during the transmission. The telecommunications components of a voting system shall meet the following requirement:

- a. Provide the capability to receive electronic signals that represent data provided by the sender and reproduce the data exactly at the point of receipt of the signals. During system performance, the maximum error rate shall be no more than the equivalent of 1 in 1,000,000 characters.

## 5.2.2 Availability

---

*Availability* represents the extent to which the system is accessible and usable to transmit data upon command under expected voting system environmental conditions. Availability is measured the probability that the telecommunications devices, including networks, will respond to an operational demand. It is the ratio of the time during which the system is operational (up time) to the total time period (up time plus down time). Inherent availability ( $A_i$ ), is based upon MTBF and active repair time (MTTR), that is:

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

The telecommunications components of a voting system shall meet the following requirements:

- a. Provide the ability to respond to operational demands upon command with availability of at least 99%, including for Internet voting systems sufficient capacity to handle the maximum rate of votes that might reasonably be expected to be cast in the last hours that Internet voting is permitted by the jurisdiction.
- b. Achieve the minimum specified availability under environmental conditions that are the same as those applicable to hardware components as described in Section 4, Hardware Standards

### 5.2.3 Privacy

---

*Privacy* generally represents the ability to protect data from access and reading by unauthorized users. For purposes of these standards, protection of data from access by unauthorized users through a system's telecommunication components is addressed in *Section 6, Security Standards*. The requirement for privacy for telecommunication components addresses the form in which data is transmitted, assuring that any data intercepted through telecommunications components is not understandable in its transmitted form to an unauthorized third person for unauthorized use.

The telecommunications components of a voting system shall encrypt data (selecting from algorithms specified in Section 6 of the Standards) into a non-readable form and allow only deciphering of specific data and specific combinations of data to only authorized individuals as defined for each type of data.

### 5.2.4 Confirmation

---

*Confirmation* represents the capability of the system to notify the user of the successful or unsuccessful completion of the data transmission, where successful completion is defined as accurate receipt of the transmitted data.

The telecommunications components of a voting system shall meet the following requirements:

- a. Provide the capability to notify the user of the successful or unsuccessful completion of the data transmission
- b. Notify the user of the action to be taken in the event of unsuccessful transmission

### 5.2.5 Reliability

---

*Reliability* represents the expected mean time between failure (MTBF), defined as the value of the ratio of operating time to the number of failures which have occurred in the specified time interval. For the purpose of demonstrating compliance with this requirement, a failure is defined as any event that results in the loss or unacceptable degradation of one or more of the system functions.

The telecommunications components of a voting system shall meet the following requirements during national qualification testing:



- a. Demonstrate a MTBF of at least 163 hours with the exception of components used at a central site for receipt of votes cast over the Internet
- b. Demonstrate a MTBF of at least 336 hours for components used at a central site for receipt of votes cast over the Internet

## 5.2.6 Durability

---

*Durability* represents the ability of the system to withstand normal use without premature deterioration or wearing out. Durability is measured as the design life of the voting system's telecommunications components.

The telecommunications components of a voting system shall withstand normal use without premature deterioration or wearing out under expected voting system environmental conditions. The telecommunications components shall have a durable life of ten years.

## 5.2.7 Maintainability

---

### 5.2.7.1 Elements of Maintainability

---

*Maintainability* represents the ease with which maintenance actions can be performed based on the design characteristics of the system. Maintainability addresses all scheduled and unscheduled events, which are performed to:

- a. Determine the operational status of the system or a component,
- b. Adjust, align, or service components,
- c. Replace a component having a specified operating life or replacement interval, or
- d. Repair or replace a component that exhibits an undesirable predetermined physical condition or performance degradation; repair or replace a component which has failed; and verify the restoration of a component, or the system to operational status.

Qualitative characteristics of maintainability include:

- a. Ease of access to internal components

Presence of labels and the identification of test points

- b. Provision of built-in test and diagnostic circuitry or physical indicators of condition
- c. Ease with which adjustment and alignment can be performed
- d. Presence of easily disconnected electrical and mechanical interfaces, which facilitate the removal and replacement of circuits and components

Qualitative measures of maintainability include mean time to repair.

### 5.2.7.2 Mean Time to Repair (MTTR) Guidelines

---

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.

For all voting devices and components, their MTTR attributes should be sufficient to achieve, in combination with their MTBF, the required availability defined in Section 5.2.2. In addition, vendors shall specify the 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 versus vendor) of qualified maintenance personnel.

### 5.2.8 Response Time

---

*Response Time* represents the elapsed time between the taking of action by the user, or by the system automatically, to transmit data and either the receipt of data at the receiving node if no confirmation is provided, or the receipt of confirmation at the sending node.

The telecommunications components of a voting system shall achieve a response time:

- a. Not to exceed 10 seconds during normal operating conditions for any operation performed by a voter
- b. Not to exceed 30 seconds during normal operating conditions for any operation performed by an election official at the poll site or central office location.

### **5.3 Prohibitions (Pre-Voting, Voting, and Post Voting)**

---

Prohibitions represent specific types of voting-related information that shall not be communicated and/or transmitted via telecommunications at any time due to the limits of existing technology to prevent unauthorized access and use of data. The design of a voting system shall provide for the secure transfer of the following types of information with no use of telecommunications as defined in this Section:

- a. Requests for Internet voting submitted by individual voters to the jurisdiction
- b. Registry of voter keys and voter PINs to any persons, including the voter (such as to authenticate himself/herself to cast a ballot over the Internet)
- c. Election Management Database
- d. Ballot definition programs and databases
- e. Ballot installation programming
- f. System programming and software installation
- g. Pre-election test programs
- h. Voting device and system audit logs



# Table of Contents

---

<b>6 Security Standards</b> .....	<b>6-1</b>
6.1 Scope.....	6-1
6.1.1 System Components and Sources.....	6-2
6.1.2 Location and Control of Software and Hardware on Which it Operates.....	6-2
6.1.3 Application to Internet Voting Systems and Public Telecommunications Networks .....	6-3
6.1.4 Exclusions.....	6-3
6.1.5 Other Elements an Effective Security Program.....	6-4
6.1.6 Organization of this Section .....	6-4
6.2 Access Control.....	6-5
6.2.1 Penetration Analysis .....	6-6
6.2.2 Access Control Policy .....	6-6
6.2.2.1 General Access Control Policy .....	6-6
6.2.2.2 Individual Access Privileges .....	6-7
6.2.3 Access Control Measures .....	6-7
6.3 Equipment and Data Security.....	6-8
6.3.1 Physical Security Measures .....	6-8
6.3.1.1 Polling Place Security.....	6-8
6.3.1.2 Central Count Location Security .....	6-8
6.4 Software and Firmware Installation.....	6-9
6.5 Telecommunications and Data Transmission.....	6-10
6.5.1 Access Control.....	6-10
6.5.2 Data Interception and Prevention.....	6-10
6.5.3 Virus Protection for Third Party Products and Services.....	6-11
6.5.3.1 Identification of Potentially Vulnerable Third Party Products.....	6-11
6.5.3.2 Virus Forms.....	6-11
6.5.3.3 Use of Antivirus Software .....	6-12
6.5.3.4 Update and Maintenance of Antivirus Software .....	6-12
6.5.4 Shared Operating Environment.....	6-12
6.5.5 Access to Incomplete Election Returns and Interactive Queries .....	6-13
6.6 Internet Voting System Security.....	6-14
6.6.1 General Security Requirements for Internet Voting Systems .....	6-14
6.6.2 Vote Server Data Center Requirements for Internet Voting Systems.....	6-15
6.6.3 Voting Process Security for Poll Site Internet Voting Systems .....	6-16

6.6.3.1 Documentation of Security Activities at Poll Site.....	6-16
6.6.3.2 Capabilities to Operate During Denial of Service Attack (Poll Site Internet System Only).....	6-16
6.6.4 Voting Process Security for Remote Site Internet Voting Systems.....	6-17
6.6.4.1 Request for Internet Balloting.....	6-17
6.6.4.2 Authorization for Internet Ballot.....	6-17
6.6.4.3 Voter Authentication.....	6-18
6.6.4.4 Casting of Votes.....	6-18
6.6.4.5 Transmitting a Ballot to the Vote Server.....	6-19
6.6.4.6 Receipt of a Ballot by the Vote Server.....	6-19
6.6.4.7 Vote Authentication and Separation from Voter Identification.....	6-20

# Security Standards

---

## 6.1 Scope

---

This section describes essential security capabilities for a voting system, encompassing the hardware, software, communications, and documentation. The standards of this section recognize that no predefined set of security capabilities is capable of defeating all conceivable or theoretical threats, while focusing on achieving an acceptable level of confidence in the integrity, reliability, and inviolability of the election process. Ultimately, the objectives of the security standards for voting systems are:

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

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, these standards identify several types of risk that must be addressed by a voting system. These include:

- ◆ Unauthorized changes to system capabilities for:
  - 1) Defining ballot formats
  - 2) Casting and recording votes
  - 3) Calculating vote totals consistent with defined ballot formats
  - 4) 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.
- ◆ 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 individual.

The standards of this security section describe specific capabilities that vendors shall provide integral to a voting system in order to address the risks listed above.

### 6.1.1 System Components and Sources

---

The requirements of this section generally apply to the broad range of hardware, software, and communications components, as well as documentation, which comprise a voting system and support the functions of a voting system as defined in Section 2 of these standards. These requirements apply to:

- a. Components provided by the voting system vendor and its component suppliers.
- b. Components furnished by an external provider (for example providers of personal computers and commercial off-the-shelf (COTS) operating systems and web browsers) where the components are potentially used in any way during voting system operation.
- c. Components developed by the 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 activities, regardless of the ownership of the software and the ownership and location of the hardware on which the software is installed or operates. These requirements apply to:



- a. Software that operates on voting devices and vote counting devices installed at polling places under the control of the voting jurisdiction.
- b. Software that operates on ballot printers, vote counting devices, and other hardware typically installed at central or precinct locations (including contractor facilities).
- c. Software that operates on voting devices (such as personal computers) under the control of individual voters and third persons other than the voting jurisdiction (e.g., employer, library, hotel, college) for use by the voter, such as for Internet voting systems.

However, some requirements apply in only specific situations as indicated in this section.

### 6.1.3 Application to Internet Voting Systems and Public Telecommunications Networks

---

The requirements of this section apply to all forms of Internet voting systems. Requirements for Internet for voting systems are identified for poll site systems that utilize voting devices under the control of election officials at controlled locations such as traditional polling places, and remote Internet Voting Systems that utilize uncontrolled devices operated by the voter at uncontrolled locations, such as at home, place of employment, or public library.

The requirements of this section also apply to telecommunications capabilities, including the use of public networks, for those systems that use such capabilities as a primary means of data transmission for system operation.

For Internet Voting Systems as well as other forms of systems that use public telecommunications networks, the requirements of this section place primary emphasis on preventing disruption of voting by individual voters, and preventing systemic manipulation of vote recording, counting, reporting and audit processing.

### 6.1.4 Exclusions

---

This section is not intended to apply to general purpose non-voting software (e.g., operating systems, programming language compilers, database management systems, Web browsers) and other software components that are resident on a vote recording or counting device but which do not operationally supporting any voting related activities, including components that are bypassed or disabled during processing for any voting related activities. For example, this section does not apply to an operating

system that is resident on a personal computer or other device used to record votes but which is bypassed completely by the installation of another operating system that controls the functioning of all voting related software.

### 6.1.5 Other Elements an Effective Security Program

---

The requirements of this section apply to the capabilities of a voting system provided by the vendor. The VSS recognize that effective security requires safeguards beyond those pertaining to the system, or "product", provided by the vendor, encompassing practices of the state or local jurisdiction which include:

- a. Administrative and management controls for the voting system and election management, including access controls
- b. Internal security procedures
- c. Adherence to, and enforcement of, operational procedures (e.g., effective password management)
- d. Physical facilities and arrangements
- e. Organizational responsibilities and personnel screening.

Specific standards for these elements are not under the direct control of the vendor and therefore are not included in this volume of the VSS. However, they will be addressed in new volumes of the VSS that address best practices for jurisdictions conducting elections and managing the operation of voting systems.

### 6.1.6 Organization of this Section

---

The standards presented in this section are organized as follows:

- ◆ *Access Control*, which addresses procedures and system capabilities that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality and accountability
- ◆ *Equipment and Data Security*, which addresses physical security measures and procedures that prevent disruption of the voting process at the poll site and corruption of voting data.
- ◆ *Software and Firmware Installation*, which addresses the installation of software or firmware in the voting system.

- ◆ *Telecommunication and Data Transmission*, which addresses security for the electronic transmission of data between system components and locations
- ◆ *Internet Voting System Security* which addresses required security capabilities for systems that communicate individual votes or vote counts over the Internet.

There are three areas of concern that must be addressed by telecommunications and data transmission security capabilities:

- ◆ Access control for telecommunications capabilities.
- ◆ Detection and prevention of data interception.
- ◆ Protection against viruses to which commercial products utilized by a voting system may be susceptible

System audit requirements are covered in Section 4, *Software Standards*. As an integral part of software capability, computer-generated audit controls provide inherent system security.

## 6.2 Access Control

---

Access controls are procedures and system capabilities that limit or detect access to critical system components 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, but are not limited to: 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 VSS are limited to those required of system vendors. Access controls required of jurisdictions will be addressed in new volumes of the VSS that address best practices for management and operation of voting systems by the jurisdictions.

## 6.2.1 Penetration Analysis

---

The vendor shall provide a penetration analysis relevant to the operating states of the system, and to its environment. This analysis shall cover:

- a. The individual use of program units
- b. The planned or inadvertent sharing of program units
- c. The resulting transitivity relationships
- d. All entry points and the methods of attack to which each is vulnerable.

Such penetration analysis will be subject to strict confidentiality and non-disclosure by the test authority. For security reasons, the penetration analysis shall not be routinely distributed to the jurisdictions that program elections. The penetration analysis, however, will be part of the escrow deposit.

## 6.2.2 Access Control Policy

---

### 6.2.2.1 General Access Control Policy

---

Voting system vendors shall specify the general features and capabilities of the access control policy recommended to provide effective voting system security. The access control policy shall be described in terms of:

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

- h. Other relevant characteristics.

The using jurisdiction in charge of voting system operations shall be responsible for determining the specific access policies applying to each election, and for defining any variations of these resulting from use of the system in more than one environment.

### 6.2.2.2 Individual Access Privileges

---

Voting system vendors shall meet the following requirements for specifying access privileges to be granted individuals:

- a. Identify all persons to whom access is granted, and the specific functions and data to which each holds authorized access.
- b. If an authorization is limited to a specific time, time interval, or phase of the voting or counting operations, this limitation shall also be specified.
- c. Not affect the ability of a voter to record votes and submit a ballot, but preclude voter access to all other physical facilities of the vote-counting processes.

### 6.2.3 Access Control Measures

---

Vendors shall provide a detailed description of all system access control measures designed to permit access to system states in accordance with the access policy, and to prevent all other types of access. Examples of such measures include:

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

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

## **6.3 Equipment and Data Security**

---

There are two areas of concern that must be addressed by equipment and data security capabilities:

- ◆ Disruption of the voting process
- ◆ Corruption of voting data.

### **6.3.1 Physical Security Measures**

---

The sensitivity of a voting system 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. Disruption of voting and vote counting results most often from a physical violation of one or more areas of the system thought to be protected. Security procedures shall, therefore, address physical threats and the corresponding means to defeat them.

#### **6.3.1.1 Polling Place Security**

---

For polling place operations, vendors shall develop and provide detailed documentation of measures to anticipate and counter acts of vandalism, civil disobedience, and similar occurrences. The measures shall:

- a. Allow the immediate detection of tampering with the vote casting devices, and with precinct ballot counters.
- b. Control physical access to a telecommunications link if such a link is used.

#### **6.3.1.2 Central Count Location Security**

---

Vendors shall develop and document in detail the measures to be enforced in a central counting environment. These measures shall include physical and procedural controls on:

- a. Handling of ballot boxes
- b. Preparing of ballots for counting
- c. Counting operations
- d. Reporting data.

## **6.4 Software and Firmware Installation**

---

The system shall meet the following requirements for installation of software or firmware:

- a. If software is resident in the system as firmware, the vendor shall require and state in the system documentation that:
  - 1) Every device is to be retested to validate each ROM prior to the start of elections operations.
  - 2) Firmware or the equipment containing it shall be maintained in a secure environment at all times.
- b. To prevent alteration of executable code, no software or firmware shall be permanently installed or resident in the system unless it is required and stated in the system documentation that the jurisdiction 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, provided that this firmware has been shown to be inaccessible to actuation or control by any means other than the authorized initiation and execution of the vote-counting program, and its associated exception handlers.
- d. After initiation of election day testing, no source code or compilers or assemblers shall be resident or accessible to prevent alteration and recompilation of the program.

## 6.5 Telecommunications and Data Transmission

---

There are three areas of concern that must be addressed by telecommunications and data transmission security capabilities:

- ◆ Access control for telecommunications capabilities.
- ◆ Detection and prevention of data interception.
- ◆ Protection against viruses to which commercial products utilized 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 Interception and Prevention

---

Voting systems that use telecommunications to communicate between system components and locations shall:

- a. Use data integrity and other relevant techniques that make the interpretation of intercepted data difficult, and that are capable of detecting corrupted data. Examples of applicable techniques include Parity checks, check-sums and error detection and correction codes.
- b. Provide a means to detect the presence of an intrusive device, such as a wiretap or electromagnetically-coupled pickup, and to prevent the leakage of data from an authorized process (such as a telecommunications transmission) to an unauthorized recipient.
- c. Use data encryption algorithms to make the interpretation of any intercepted data very difficult, expensive and time consuming. At this time, the Advanced Encryption Standard (AES) selected by the National Institute of Standards and Technology (NIST) and which will be specified in an upcoming Federal Information Processing Standard (FIPS) in second half of late 2001, or the Triple Data Encryption Standard (Triple DES) specified in FIPS 46-3 are acceptable.



### 6.5.3 Virus Protection for Third Party Products and Services

---

Voting systems that use public telecommunications networks to transmit data between system components shall deploy protection against the many forms of viruses to which they may be exposed. Vendors of such systems shall conduct certain activities that help assure that such protection is maintained in a sufficiently current status to assure protection against all known forms of viruses that could attack the vendor's system.

#### 6.5.3.1 Identification of Potentially Vulnerable Third Party Products

---

Voting systems that utilize public telecommunications networks shall provide system documentation that clearly identifies all commercial third party 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
- d. Dial-up networking software

Such documentation shall identify the name, vendor and version used for each such component.

#### 6.5.3.2 Virus Forms

---

Voting systems that utilize public telecommunications networks, including Internet systems, shall protect against all known forms and variants of viruses, including:

- a. File viruses that execute when an infected file is executed
- b. Macro viruses that infect executable code embedded in third party software programs
- c. Worms, a form of virus that alters or destroys data
- d. Trojan horses
- e. Logic bombs

### 6.5.3.3 Use of Antivirus Software

---

Voting systems that utilize telecommunications, including Internet systems, shall utilize antivirus software at the receiving end of all communications paths to:

- a. Detect the presence of a virus in a transmission.
- b. Remove the virus from infected file(s)/data.
- c. Prevent against storage of the virus anywhere on the receiving device.
- d. Provide data to the system audit log indicating the detection of a virus and processing performed.

Vendors shall use multiple forms of antivirus software as needed to provide capabilities for the full range of telecommunications products utilized by the voting system.

### 6.5.3.4 Update and Maintenance of Antivirus Software

---

Vendors of voting systems that that utilize telecommunications, including Internet systems, shall update and maintain all antivirus software on a regular basis, to assure that it is capable of responding to all virus and comparable threats known to exist for the telecommunications products utilized by the voting system. Specifically, vendors shall:

- a. Protect against all viruses and comparable threats identified by the assessments, advisories and alerts of the National Infrastructure Protection Center (NIPC), for which a current listing can be found at <http://www.nipc.gov/warnings/warnings.htm> or the quarterly summaries and advisories of the Federal Computer Incident Response Capability (FedCIRC), for which additional information can be found at <http://www.fedcirc.gov/>.
- b. Maintain such protection such that it is updated on at least a quarterly basis.
- c. Provide complete and detailed documentation of the procedure used to assure compliance with requirements a) and b) above.

## 6.5.4 Shared Operating Environment

---

In general, it is preferable to have all ballot recording and counting performed in a strictly dedicated environment. However, if ballot recording and vote-counting

operations are performed in an environment which 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 which use a shared operating environment shall meet the following requirements:

- a. Security procedures and logging records are used to control access to system functions.
- b. Voting system functions are partitioned or compartmentalized from other concurrent functions at least logically, and preferably physically as well.
- c. System access must be controlled by means of passwords, and restriction of account access to necessary functions only.
- d. Capabilities are in place to control the flow of information, precluding data leakage through shared system resources.

### 6.5.5 Access to Incomplete Election Returns and Interactive Queries

---

All systems shall meet the following requirements for access to incomplete election returns and interactive queries:

- ◆ For equipment which operates in a central counting environment, provision is made for external access to incomplete election returns before completion of the official count provided 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.
- ◆ Voting system software and its security environment is designed so 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 Internet Voting System Security**

---

Internet voting systems face security risks that are not present in other forms of voting systems. This section describes standards applicable to Internet voting systems that go beyond those established for telecommunications capabilities that do not rely on the Internet—identifying those standards applicable to all forms of such systems and standards that apply to only remote site or poll site Internet voting systems.

### **6.6.1 General Security Requirements for Internet Voting Systems**

---

All Internet voting systems shall:

- a. Preserve the secrecy of a voter's ballot choices, and use every reasonable technical means to prevent anyone from violating ballot privacy anywhere along the path from the voter to the canvass.
- b. Assure that the ballot that is transmitted to the vote server is an accurate copy of the voter's choices, with no reasonable possibility of undetected modification anywhere in the transmission path in any of the intervening computers and networks, including within the voting device.
- c. Employ encryption/decryption for all communications between the vote server and other devices that communicate with the server over the Internet.
- d. Retain decrypted ballots in a secure format to allow for subsequent auditing and recount procedures.
- e. Assure that no single election official is able to delete, change, forge, or violate the privacy of Internet ballots.
- f. Guarantee that at least 2 employees concur whenever any critical operation regarding the processing of Internet ballots takes place, i.e. the passwords or cryptographic keys of at least 2 employees are required to perform processing of votes.

## 6.6.2 Vote Server Data Center Requirements for Internet Voting Systems

---

The Vote Server Data Center (VSDC) is considered to be that part of the voting system infrastructure that receives ballots from the Internet and secures them. The VSDC may be replicated, it may be geographically distributed, and it may or may not be at the same location as the rest of the vote-handling infrastructure. The standards of this section apply to the VSDC regardless of the organization responsible for its management (i.e., voting jurisdiction, vendor or contractor).

The VSDC for all Internet voting systems shall:

- ◆ *Be physically secure*—at least as secure against physical intrusion as the county election agency where votes are stored and tallied.
- ◆ *Be engineered for highly reliable vote storage*—redundant, invulnerable to power failures, and utilizing write-once storage, such as CD-R.
- ◆ *Be architected for high availability*—capable of being up and running for voting for all but a negligible fraction of the time during the time period in which Internet voting takes place. Specific features include:
  - 1) Redundant servers
  - 2) Redundant communication
  - 3) Smooth failure response procedures so that if one resource goes down, the others remaining automatically take up its slack with no loss of votes and minimal disruption
- ◆ Be equipped with systems and procedures to withstand most attacks on its servers, including denial-of-service attacks. At a minimum, the technology and procedures used shall:
  - 4) Be capable of blocking all incoming packets on all ports except those involved in voting.
  - 5) Be configured to filter malformed packets and any other suspicious traffic.

### 6.6.3 Voting Process Security for Poll Site Internet Voting Systems

---

Systems designed for poll site Internet voting shall meet security standards oriented to address the security risks attendant with the casting of ballots from poll sites controlled by election officials using voting devices configured and installed by voting officials and/or their vendor or contractor, and using in-person authentication of individual voters.

#### 6.6.3.1 Documentation of Security Activities at Poll Site

---

Vendors of poll site Internet voting system shall provide detailed descriptions of:

- a. All activities to be performed in setting up the system for operation that are mandatory to assure effective system security, including testing of security before an election.
- b. All activities that should be prohibited during system setup and the during the timeframe for Internet voting operations, including both the hours when polls are open and when polls are closed.

#### 6.6.3.2 Capabilities to Operate During Denial of Service Attack (Poll Site Internet System Only)

---

The poll site Internet voting system shall provide the following capabilities to provide resistance to denial of service attacks and other events that prevent voting devices at the poll site from communicating with the vote server:

- a. Diagnose the occurrence of a denial of service attack 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 the vote server.
- b. Provide an alternate mode of operation that includes the functionality of an electronic voting system, and switch to this mode 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 electronic voting system mode.
- d. Upon reestablishment of communications with the vote server, transmit and process votes accumulated while operating in electronic voting system mode with all safeguards related to voter identification and authentication in effect.

## 6.6.4 Voting Process Security for Remote Site Internet Voting Systems

---

Systems designed for remote site Internet voting shall meet security standards oriented to address the security risks attendant with the casting of ballots from uncontrolled locations using uncontrolled voting devices, such as personal computers and personal data assistants (PDAs). These standards define a combination of functional processing capabilities as well as technology requirements and restrictions:

### 6.6.4.1 Request for Internet Balloting

---

Systems designed for remote site Internet Voting shall:

- a. Require that voters request Internet voting in writing with an original signature
- b. Require that voters re-request for each new election, and must not request both an absentee ballot and i-voting in any one election

### 6.6.4.2 Authorization for Internet Ballot

---

Systems designed for remote site Internet Voting shall:

- ◆ For the authorization of voting using the Internet provide a way of linking the eventual vote cast using that authorization to the registration record for that voter, such as by key distribution, so that it can be determined beyond a reasonable doubt that each Internet vote is associated with a registered voter in the proper district, and that at most one vote is counted for any voter, whether at the polls, or by absentee ballot, or by Internet voting.
- ◆ Provide the means to support key distribution prior to the opening of the polls.
- ◆ Be able to handle the voter's loss of, or failure to use, authorization for Internet balloting. If a voter loses, or claims to lose, his/her Internet ballot authorization, or if that authorization for some reason fails to work to allow voting, then the system shall be capable of enabling the voter to request a new Internet authorization, or an absentee ballot.
  - 1) The system shall cancel the old authorization before either such request is granted.

- 2) The system shall enable voter to cast a ballot at the polling place on election day and vote with a provisional ballot even if his/her authorization for Internet voting has not yet been canceled by the jurisdiction.

#### 6.6.4.3 Voter Authentication

---

Systems designed for remote site Internet Voting shall provide a level of security equivalent to that of a paper based system for absentee ballots. The system shall:

- a. Provide the voter with an authentication code from the jurisdiction that is combined with a personal identification number (P.I.N.) that will allow the voter to authenticate him/herself for the system.
- b. Prevent the use of data obtained during a single "out-of-band" transmission by an individual to cast a fraudulent ballot.

#### 6.6.4.4 Casting of Votes

---

Systems designed for remote site Internet voting shall:

- ◆ Assure that the actual contents of the voter's votes are automatically erased in the event of a power failure or rebooting.
- ◆ Not write votes to long-term storage on the client machine or for any reason, even in encrypted form.
- ◆ Not store the vote in a file on the voter's computer, including a temporary file, in secondary storage as a result of virtual memory, any log, any index, any cache, or any cookie.
- ◆ Immediately after the ballot is sent to the vote server, and without waiting for feedback from the server, or immediately after the voter clicks on the "cancel" button, erase all record of the vote from the voter's computer, including:
  - 1) Erase the voter's choices from the screen.
  - 2) Zero out the voter's choices that are recorded in the computer's RAM.



#### 6.6.4.5 Transmitting a Ballot to the Vote Server

---

Systems designed for remote site Internet Voting shall:

- a. Transmit the ballot, along with a timestamp, voter's identification, precinct, and any other appropriate information, to the vote server in encrypted form.
- b. Prevent anyone who taps the communication links between the voter's computer and the vote server to read the ballot, or any of the associated information, or to tamper with any of it in a way that might go undetected.
- c. Prevent the injection of a duplicate of the encrypted ballot and have that counted as an additional vote.

#### 6.6.4.6 Receipt of a Ballot by the Vote Server

---

The vote server of a remote site Internet voting system shall:

- a. Upon receipt of a ballot immediately check it to ensure that it is formatted correctly.
- b. Accept or not accept a ballot in its entirety, with no partial acceptance of a ballot.
- c. For a ballot formatted correctly, immediately store the ballot, still encrypted, on a permanent medium (e.g. a CD-R disk) so that any subsequent power or equipment failure will not lose the ballot.
- d. For a ballot formatted correctly, record data needed to assure that the voter for that ballot cannot vote another ballot by Internet or other means.
- e. For a ballot determined to not be formatted correctly, notify the voter and provide given advice about what to do, such as attempt to cast the ballot again or vote at the polls.
- f. For a ballot determined to not be formatted correctly, record data that enables the voter to vote again either by Internet or at a poll site by provisional ballot.
- g. For both ballots determined to be formatted correctly and those formatted incorrectly, store the vote permanently and redundantly for later decryption and canvass—enabling the encrypted to be considered part of the audit trail in case a recount is called for, or the election is challenged in court.
- h. For vote servers managed by vendors or contractors (rather than by election officials), not store on the vote server keys or other tools for decrypting

ballots, and assure that such keys and tools are not available to the vendor or contractor. All such keys must remain strictly in the hands of election officials.

#### 6.6.4.7 Vote Authentication and Separation from Voter Identification

---

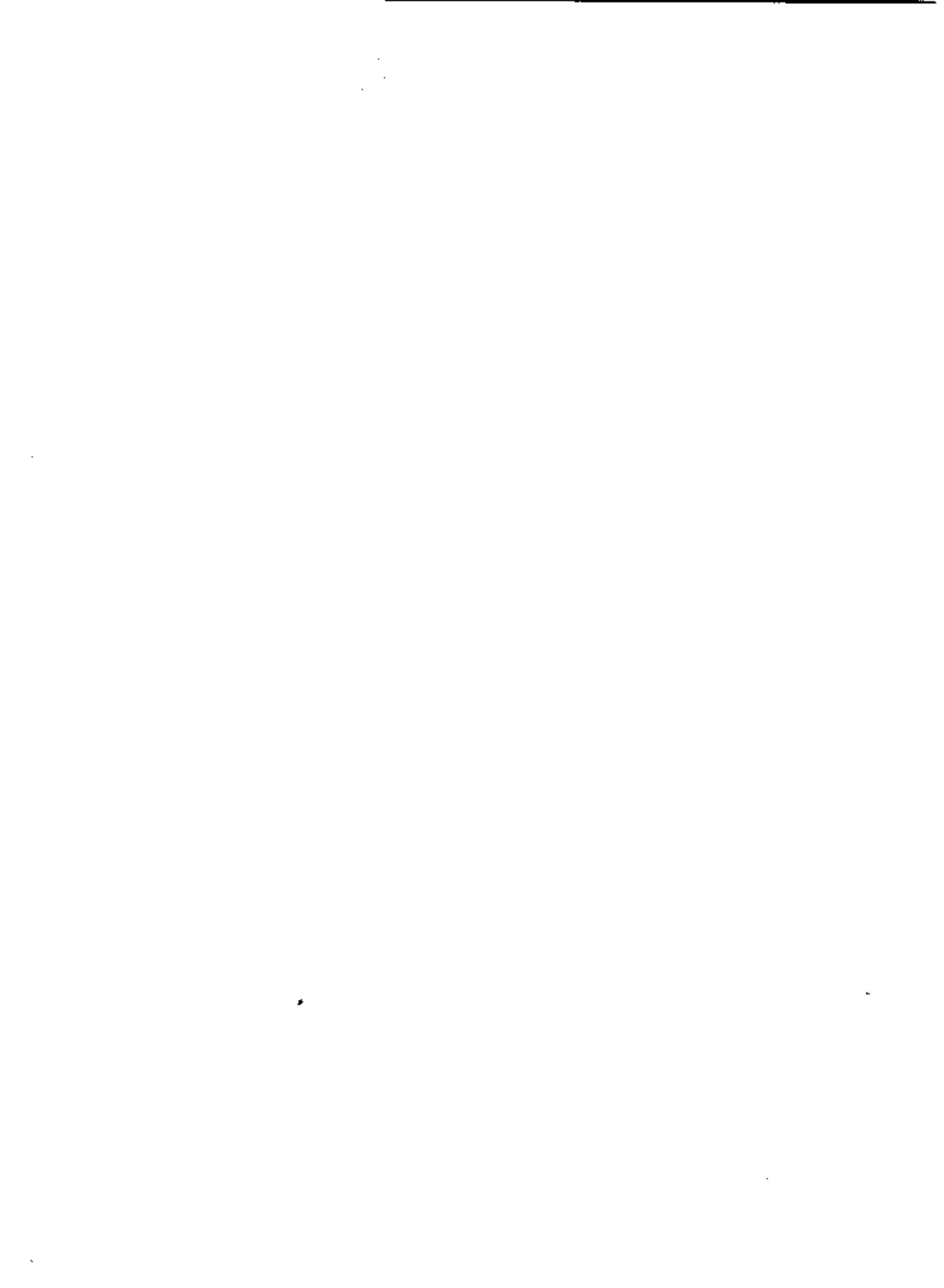
The remote site Internet voting system shall:

- a. Verify the authenticity of a ballot before the votes on the ballot are viewed or counted.
- b. Verify a for authenticity before the authenticating information is stripped from the ballot.
- c. Ensure the true source of the ballot, ensuring that the ballot really is from the person it claims to come from, and not just from another individual attempting to electronically impersonate that person.
- d. Once the ballot is separated from the authenticating information, the ballot must be incapable of being traced to the voter who cast it.
- e. Decrypted and count a ballot only after the authenticating information is reviewed and removed from the ballot.

# Table of Contents

---

<b>7 Quality Assurance .....</b>	<b>7-1</b>
7.1 General Requirements .....	7-1
7.1.1 Guidelines .....	7-2
7.2 Responsibility for Tests .....	7-2
7.3 Parts & Materials Special Tests and Examinations .....	7-3
7.4 Quality Conformance Inspections .....	7-3
7.5 Documentation .....	7-3
7.6 Error Notification Reporting Process & Issues Management .....	7-4



# Quality Assurance

---

Quality Assurance is a vendor function with associated practices that confirms throughout the system development and maintenance life cycle system that a voting system conforms with the Standards and other requirements of state and local jurisdiction. 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,
- ◆ Has been developed and maintained in a manner that reflects all changes approved during its initial development, internal testing, qualification and if applicable, additional certification processes,

## 7.1 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 and procuring parts and raw materials of the requisite quality, and for their inspection, acceptance, and control.
- b. Require the documentation of the hardware and software development process.
- c. Identify and enforce all requirements for in-process inspection and testing which the manufacturer deems necessary to ensure proper fabrication and assembly of hardware; and installation and operation of software or firmware.
- d. Include plans and procedures for post-production environmental screening and acceptance tests.

- e. Include a procedure for maintaining all data and records required to document and verify the quality inspections and tests.
- f. Include a procedure for maintaining records of errors and defects reported by state authorities and local jurisdictions.

Effective Quality Assurance conveys several benefits. For the FEC, state and local jurisdictions, and vendors these benefits include:

- a. Vendor development teams focus on meeting jurisdiction expectations.
- b. Work is accomplished efficiently because standards exist for document formats, directory structures, development and testing procedures, and management functions. This helps to decrease the time required for software qualification and certification.
- c. Issue and action item identification and tracking reduce risks.
- d. Software change recommendations are in line with jurisdiction needs because communication with jurisdiction sponsors is maintained.

### 7.1.1 Guidelines

---

Vendors who do not manufacture all components of voting systems, but who procure these components as standard commercial items for assembly and integration into voting systems, should verify that their supplier vendors follow documented quality assurance procedures that are at least as stringent as those utilized internally by the vendor.

## 7.2 Responsibility for Tests

---

The manufacturer or vendor shall be responsible for:

- a. Performing all quality assurance tests
- b. Acquiring and documenting test data
- c. Providing test reports for review by the purchaser upon request

### **7.3 Parts & Materials Special Tests and Examinations**

---

Vendors shall select voting system parts and materials according to their suitability for the intended application. Listed below are the vendor requirements regarding special tests and examinations of these parts and materials:

- a. Parts and materials to be used in voting systems and components shall be selected 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. If special tests are required, they shall be designed to evaluate the part or material under conditions accurately simulating the actual operating environment.
- c. The resulting test data shall be maintained as part of the quality control program documentation.

### **7.4 Quality Conformance Inspections**

---

The vendor performs conformance inspections to ensure the overall quality of the voting system and components delivered to the jurisdiction. The vendor conformance inspection requirements are listed below:

- a. The manufacturer or vendor shall inspect and test each voting system or component to verify that all inspection and test requirements for the system have been met.
- b. A record of tests, or a certificate of satisfactory completion, shall be delivered with each system or component.

### **7.5 Documentation**

---

Vendors are required to produce various types of documentation to support the development and formal testing of voting systems. Listed below are the vendor documentation requirements:

- a. Complete product documentation shall be provided with voting systems or components.
- b. This documentation shall be sufficient to serve the needs of the voter, the operator, and the maintenance technician.

- c. It shall be prepared and published in accordance with standard industrial practice for electronic and mechanical equipment.
- d. It shall consist, at a minimum of the following:
  - 1) System functionality specifications
  - 2) System configuration overview
  - 3) System hardware specifications
  - 4) System software specifications
  - 5) System communications specifications
  - 6) System security specifications
  - 7) System test and verification specifications
  - 8) System parts, materials and supplies specifications
  - 9) Facilities specifications
  - 10) System installation and test specifications
  - 11) Personnel deployment and training requirements
  - 12) Voter Manual
  - 13) System Operations Manual
  - 14) System Maintenance Manual
  - 15) Diagnostic Testing Manual

## **7.6 Error Notification Reporting Process & Issues Management**

---

The vendor shall have a process in place to ensure that system software is of high quality and meets jurisdiction expectations. This process focuses on the basic techniques for Quality Assurance (QA) review at major milestones during system development, and after system release, to meet the following specific objectives:

- ◆ Software releases meet quality expectations (format, content, style)
- ◆ Consistency with initial specifications and previous software releases
- ◆ Identification of subject matter errors or omissions
- ◆ Consistency with jurisdiction expectations

Vendors shall meet the following general requirements:



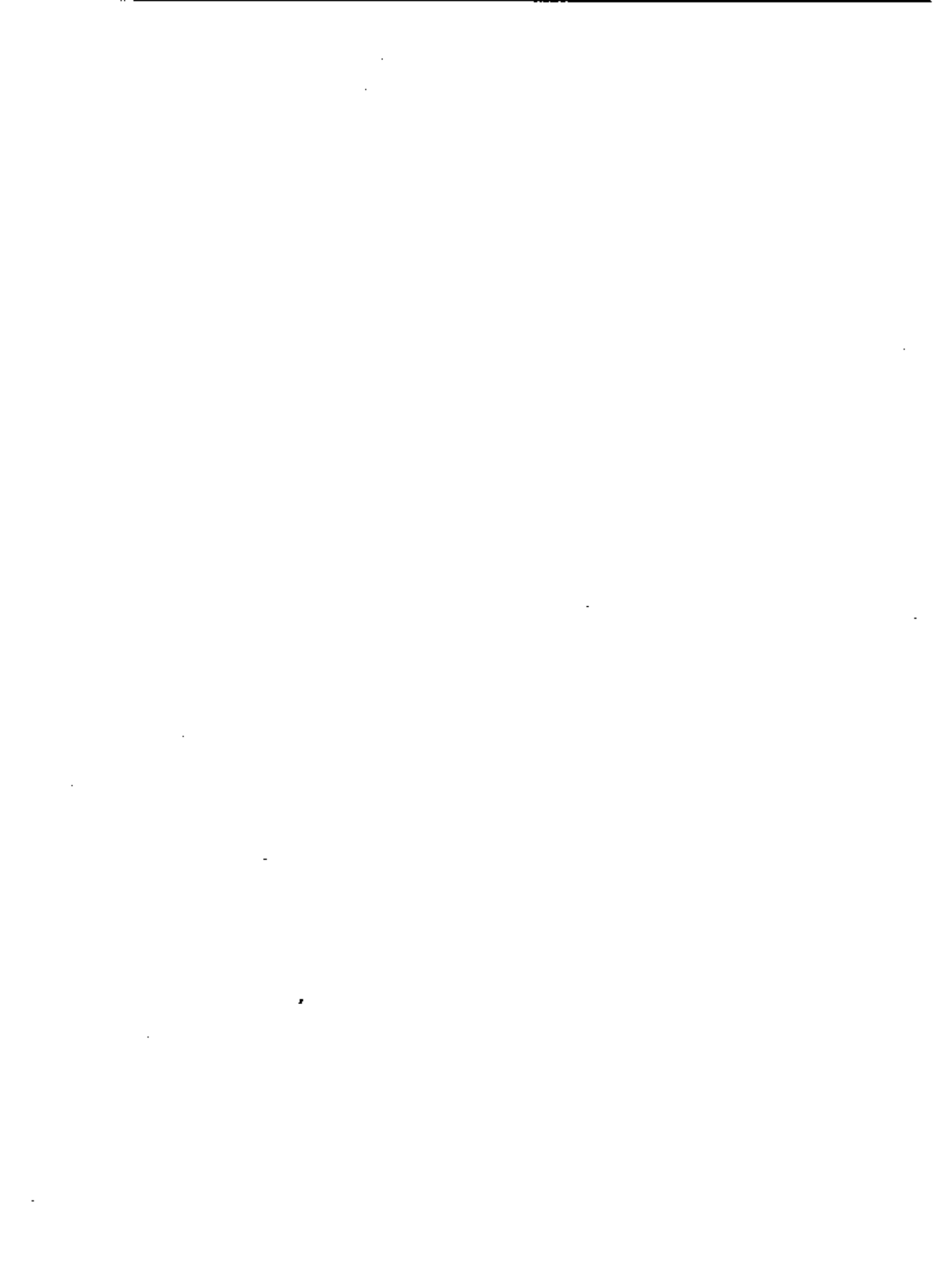
- a. Establish and adhere to some form of review process to ensure the objectives noted above are met;
- b. Implement a process to track issues and software defects reported by states, local jurisdictions, or other test authorities, and report them to affected parties;
- c. Track, analyze and formally approve change orders and requests submitted to the vendor prior to inclusion in a subsequent software release;
- d. Notify all affected jurisdictions of any defects found and their potential impact on the operation of current software releases when vendors become aware of a defect in software that has already been released to and implemented by at least one jurisdiction;
- e. Notify the state election official of each state with an affected jurisdiction when vendors become aware of a defect in software that has already been released to and implemented by at least one jurisdiction; and
- f. Send all notifications by registered mail via the U.S. Postal Service to the designated point of contact for each jurisdiction and state.



# Table of Contents

---

<b>8 Configuration Management</b> .....	<b>8-1</b>
8.1 Introduction .....	8-1
8.1.1 Configuration Management Scope .....	8-1
8.1.2 Configuration Management Benefits .....	8-2
8.1.3 Organization of Configuration Management Standards .....	8-3
8.2 Application of Configuration Management Requirements .....	8-4
8.3 Configuration Management Policy .....	8-4
8.4 Configuration Identification .....	8-4
8.4.1 Structuring and Naming Configuration Items .....	8-5
8.4.2 Versioning Conventions .....	8-5
8.5 Baseline, Promotion, and Demotion Procedures .....	8-5
8.6 Configuration Control Procedures .....	8-6
8.7 Release Process .....	8-6
8.8 Configuration Status Accounting .....	8-6
8.9 Configuration Audits .....	8-7
8.9.1 Physical Configuration Audit .....	8-7
8.9.2 Functional Configuration Audit .....	8-8
8.10 Interface Control .....	8-8
8.11 Configuration Management Resources .....	8-8



## Configuration Management

---

This section contains specific requirements for configuration management of voting systems. For the purpose of these 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, starting with its initial development and progressing through 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.

Vendors are required to submit these procedures to the Independent Test Authority (ITA) as part of the Technical Data Package for system qualifications described in *Volume II, Voting Systems Qualification Testing Standards*, for review against the requirements of this Section 8. Additionally, as articulated in state or local election legislation, 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 procedures

### 8.1 Introduction

---

#### 8.1.1 Configuration Management Scope

---

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

- a. Identifying discrete system components
- b. Creating records of a formal baseline and later versions of components
- c. Controlling changes made to the system and its components
- d. Releasing new versions of the system to ITAs

- e. Releasing new versions of the system to customers
- f. Auditing the system, including its documentation, against configuration management records
- g. Controlling interfaces to other systems
- h. Identifying tools used to build and maintain the system

## 8.1.2 Configuration Management Benefits

---

The Voting System Standards stress configuration management due to the significant benefits resulting for state and local election officials, independent test authorities, and vendors. Configuration management benefits for state and local jurisdiction election officials include:

- a. *Version Conformance to Standards*—More accurate information provided by the vendor regarding the current version of a system, its individual components, the date of last revision, and status with regard to NASED qualification and, where applicable, state certification.
- b. *Improved Documentation Quality*—Greater confidence that documentation for a system delivered to the jurisdiction has been audited and is complete and accurate.
- c. *Easier System Installations*—Improved information regarding the purpose and impact of a new system release and improved information to perform initial installation and maintenance upgrades.
- d. *Avoidance of System Disruption*—Prevention of accidental deletion or unauthorized modification of system components could adversely impact the system.

Configuration management benefits for ITAs include.

- a. *Improved System Structure, Version and Status Information*—More accurate and better organized information about the content, version and status of individual system components for national qualification or state certification.
- b. *More Efficient Test Plan Development*—Improved ability and greater efficiency to specifically identify discrete system components and compare different versions of the same component during test plan development and testing for testing of modified systems.

Configuration management benefits for vendors include those stated above for ITAs, plus the following:

- a. *Greater Consistency of Software Products*—Coding standards and naming conventions reduce variation among software products, streamlining the development, testing, and maintenance processes.
- b. *Reduced Development-to-Test Migration Cycles*—Complete and accurate system documentation and configuration management records increase programmer productivity and reduce software errors and implementation delays.
- c. *Improved Coordination among Teams*—Documented roles and responsibilities enable the various organizational entities involved with system development and implementation to accomplish interdependent tasks.
- d. *Faster and More Efficient Qualification and Certification*—Adherence to configuration management procedures enables more efficient and focused testing during initial system qualification and certification and subsequent retesting of system changes to maintain qualification and certification.

### 8.1.3 Organization of Configuration Management Standards

---

The standards presented in this section are organized as follows:

- a. Application of Configuration Management Requirements
- b. Configuration Management Policy
- c. Configuration Identification
- d. Baseline, Promotion, and Demotion Procedures
- e. Release Process
- f. Configuration Control Procedures
- g. Release Process
- h. Configuration Status Accounting
- i. Configuration Audits
- j. Interface Control
- k. Configuration Management Resources

## **8.2 Application of Configuration Management Requirements**

---

Requirements for configuration management apply to all voting systems subject to the Voting System Standards regardless of the specific technologies employed. They apply to all system components, including:

- 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
- g. File archiving and data repositories

## **8.3 Configuration Management Policy**

---

Vendors shall describe their organizational policies for configuration management. This description shall address the following elements:

- a. Scope and nature of configuration management program activities
- b. Breadth of application of vendor's policy 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)
- c. Internal organization responsibilities for carrying out the vendor's policy and practices, including the organizational position and individual ultimately accountable for implementation
- d. Procedures that will be used to determine and assure compliance with the policies, procedures and related practices submitted by the vendor.

## **8.4 Configuration Identification**

---

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



### 8.4.1 Structuring and Naming Configuration Items

---

Vendors shall describe the procedures and conventions used to:

- a. Classify configuration items into categories and subcategories
- b. Uniquely number or otherwise identify configuration items
- c. Name configuration items

### 8.4.2 Versioning Conventions

---

Vendors shall describe the conventions used to identify the specific versions of individual configuration items, and versions of sets of items that are used by the vendor to identify higher level system elements such as subsystems.

- a. Classify configuration items into categories and subcategories
- b. Uniquely number or otherwise identify configuration items
- c. Name configuration items

## 8.5 Baseline, Promotion, and Demotion Procedures

---

Vendors shall establish formal procedures and conventions for establishing and provide 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 national qualification testing
- c. Promote subsequent instances of a component to baseline status as the component is maintained throughout its life cycle until system retirement (i.e., the system is no longer sold or maintained by the vendor).

## **8.6 Configuration Control Procedures**

---

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

- a. Develop and maintain internally developed items
- b. Acquire and maintain third-party items
- c. Resolve internally identified defects for items regardless of their origin
- d. Resolve externally identified and reported defects (i.e., by customers and ITAs).

## **8.7 Release Process**

---

The release process is the means by which the vendor installs, transfers or migrates the system to external parties (i.e., ITAs and customers). Vendors 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 a system, or particular components, to an ITA
- c. Perform the initial delivery and installation of the system to a customer
- d. Perform a subsequent, or maintenance or upgrade release of a system, or particular components, to a customer

## **8.8 Configuration Status Accounting**

---

Configuration status accounting is the process of tracking the progress of and changes to configuration items through initial development and subsequent maintenance and upgrade. Vendors shall establish and provide a complete description of the procedures and related conventions used to track the following types of changes:

- a. Functional system specifications

- b. Current configuration baselines
- c. System development archives
- d. System installation archives
- e. System change proposals
- f. System trouble reports, error notifications, and comparable reports of potential system errors
- g. Notification of ITAs of confirmed system errors
- h. Notification of customers of confirmed system errors

## **8.9 Configuration Audits**

---

These standards provide for two types of configuration audits: Physical configuration audits and functional configuration audits.

### **8.9.1 Physical Configuration Audit**

---

The Physical Configuration Audit (PCA) compares the voting system components submitted for qualification to the vendor's technical documentation. Vendors shall describe and provide a complete description of the procedures and related conventions used to conduct this audit in terms of:

- a. Establishing a configuration baseline of the software and hardware to be tested
- b. Confirming whether the system documentation matches the corresponding system components
- c. Confirming whether the documentation is sufficient for the user to install, validate, operate, and maintain the system
- d. Confirming whether the vendor's documentation is sufficient for testing by the ITA or other test authorities (i.e., state certification authorities).

## 8.9.2 Functional Configuration Audit

---

The Functional Configuration Audit (FCA) encompasses an examination to verify that the system performs all the functions described in the system documentation. Vendors shall describe and provide a complete description of the procedures and related conventions used to conduct this audit for all system components.

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

## 8.10 Interface Control

---

Interface control refers to the process of managing voting system interdependencies with regard to the following types of interfaces:

- a. **Organizational**—Relationship and responsibilities between organizational entities (e.g., system vendors, third party service providers, jurisdictions, ITAs)—in terms of specific responsibilities during software development, qualification testing, certification testing, installation and maintenance.
- b. **Technical**—Relationship between the voting system and other systems with which it interfaces, such as voter registration, addressing how a change in system hardware or software can affect the surrounding technical components; connectivity and compatibility at a local jurisdiction..

Vendors shall describe and provide a complete description of the procedures and related conventions used to control the:

- a. Organizational interfaces
- b. Technical interfaces

## 8.11 Configuration Management Resources

---

Configuration management activities often are performed with the aid of automated tools. Assuring that such tools are available throughout the system life cycle, including situations where the vendor is acquired by 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 assure that they, and the data they contain, can be transferred effectively and promptly to a third party should the need arise. Within this context, vendors are 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
- c. Procedures and training materials for using the tools



# Table of Contents

---

<b>9 Overview of Qualification Tests</b> .....	<b>9-1</b>
9.1 Introduction .....	9-1
9.2 Testing Scope .....	9-2
9.2.1 Test Categories .....	9-3
9.2.1.1 Focus of Hardware Tests .....	9-3
9.2.1.2 Focus of Software Evaluation .....	9-4
9.2.1.3 Focus of Telecommunications Tests .....	9-4
9.2.1.4 Focus of Security Tests .....	9-5
9.2.1.5 Focus of Integration Tests .....	9-5
9.2.1.6 Focus of Useability/Accessibility Tests .....	9-5
9.2.1.7 Tests of Ballot Counting Accuracy .....	9-6
9.2.1.8 Sequence of Tests and Audits .....	9-6
9.2.2 Test System .....	9-6
9.3 Applicability .....	9-7
9.3.1 General Applicability .....	9-7
9.3.1.1 Exclusions .....	9-7
9.3.1.2 Software .....	9-8
9.3.2 Modifications to Qualified Systems .....	9-8
9.3.2.1 General Requirements for Modifications .....	9-8
9.3.2.2 Potential for Limited Testing of Modifications .....	9-9
9.3.2.3 Utility Software and/Device Handlers .....	9-10
9.4 Documentation Submitted by Vendor .....	9-10
9.5 Qualification Test Process .....	9-11
9.5.1 Pretest Activities .....	9-11
9.5.1.1 Initiation of Testing .....	9-11
9.5.1.2 Pretest Preparation .....	9-12
9.5.2 Qualification Testing .....	9-12
9.5.2.1 Qualification Test Plan .....	9-12
9.5.2.2 Qualification Test Practices .....	9-13
9.5.2.3 Qualification Test Conditions .....	9-14
9.5.2.4 Qualification Test Data Requirements .....	9-14
9.5.2.5 Qualification Test Fixtures .....	9-15

9.5.2.6 Witness of System Build and Installation.....	9-15
9.5.3 Qualification Report Issuance and Post Test Activities.....	9-15
9.5.4 Time Limited Qualification for Data Transmission Using Public Networks.....	9-16



# Overview of Qualification Tests

---

## 9.1 Introduction

---

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. 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.

Testing is performed by an Independent Test Authority (ITA) that is certified by NASED. The test process described in this section 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 ITAs at any point in time.

Qualification testing is distinct from all other forms of testing, including the vendor's developmental testing, certification testing by a state election organization, and system acceptance testing by a purchasing jurisdiction.

- a. Qualification testing follows the vendor's developmental testing.
- b. Qualification testing provides an assurance to state election officials and local jurisdictions of the conformance of a voting system to these Standards as input to state certification of a voting system and acceptance testing by a purchasing jurisdiction.
- c. Qualification testing may precede state certification testing, or may be conducted in parallel as established by the certification program of individual states.

The remainder of this section describes the scope of qualification testing, applicability to voting system components, documentation submitted by the vendor, and the flow of the test process.

## 9.2 Testing Scope

---

The qualification test process is intended to discover errors which, should they occur 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:

- ◆ Absolute logical 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 character error rate, for which the maximum acceptable error rate is one in one million character; (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 failure(s) or the number of unrecoverable failures under conditions simulating the intended storage, operation, transportation, and maintenance environments for voting systems, using an actual time-based period of processing test ballots.
- ◆ System performance and function under normal and abnormal conditions
- ◆ Completeness and accuracy of the system documentation and configuration management records to enable purchasing jurisdictions to effectively install, test, and operate the system.

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. The ITA may utilize automated software testing tools to assist in this process if they are available for the software under examination, and if they do not duplicate vendor testing.

The procedure for disposition of system failures or deficiencies discovered during qualification testing is described in Volume II of the VSS. 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 fully comply 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.

## 9.2.1 Test Categories

---

The qualification test procedure is presented in several parts:

- ◆ hardware qualification tests,
- ◆ software qualification tests,
- ◆ communication qualification tests,
- ◆ security tests,
- ◆ documentation tests,
- ◆ system-level tests, including audits,
- ◆ reviews of documented vendor practices for quality assurance, and
- ◆ reviews of documented vendor practices for configuration management

This division is somewhat artificial. In reality, 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 commercial 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.

### 9.2.1.1 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: transit drop, bench handling, vibration, low and high temperature, humidity, rain exposure, and sand and dust exposure. The first five tests are required. The rain, sand, and dust exposure tests are discretionary.

The operating tests involve running the system for an extended period of time under varying temperatures and voltages. This period of operation assures 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 has, in most cases, been reduced from that specified in the Military Standards to reflect commercial and industrial, rather than military and aerospace, practice

### 9.2.1.2 Focus of Software Evaluation

---

The software qualification tests encompass a number of interrelated examinations. The primary objective is to examine selectively in-depth all ballot processing source code for absolute logical correctness, for its modularity and overall construction, and for conformance with the documentation provided by the vendor. Part of this code examination will be focused on the assessment of potential (or actual) hidden code. 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.

### 9.2.1.3 Focus of Telecommunications Tests

---

Some, but not all, systems utilize telecommunications capabilities as defined in Section 5. For those systems that do utilize such capabilities, the telecommunications tests embody elements of both hardware and software testing, as well as additional tests. The physical hardware components of the telecommunications capability that are located at either the poll site or vote counting site are subject to the same tests as other components. Software components, along with hardware components, 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 will test the interface of vendor supplied components with these external components for effective interface, vote transmission, failure detection, and failure recovery.

#### 9.2.1.4 Focus of Security Tests

---

The security qualification 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, including the Internet, to transmit election management data (including blank ballot images) or official election results (i.e., individual ballots or tabulated results), tests are conducted to assure that the system is capable of detecting, logging, preventing and recovering from the broad range of viruses, variants, and other forms of attack known at the time the system is submitted for qualification. The ITA will confirm the deployment of proven commercial security software and, at its discretion, conduct or simulate attacks on the system to confirm the effectiveness of the system's security capabilities.

#### 9.2.1.5 Focus of Integration Tests

---

The hardware, software, communications and security qualification tests supplement a fuller evaluation of these components performed by the system-level tests. System-level tests focus on these aspects jointly, throughout the full range of system operations. They include tests of ballot definition, election management and ballot-counting logic, and include the Physical Configuration Audit (PCA) and the Functional Configuration Audit (FCA).

The 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 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 Voter Manual, Operations Manual, Maintenance Manual, and Diagnostic Testing Manual.

#### 9.2.1.6 Focus of Useability/Accessibility Tests

---

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 useability of voting systems by the average voter and election officials have not been defined, but are planned to be addressed in the next update of the VSS. However, standards for useability by individual voters

with disabilities have been defined in Section 2 based on Section 508 of the Rehabilitation Act Amendments of 1998. Voting systems are tested to assure that a voting device is included in the system and its design and operation conforms with these standards.

#### 9.2.1.7 Tests of Ballot Counting Accuracy

---

The various options of software counting logic shall be tested during the system-level Functional Configuration Audit. Generic test ballots or test entry data for electronic systems, representing particular sequences of ballot-counting events, will test the counting logic during this audit. For example, multiple test decks for variations in straight party and cross party endorsement will be created and processed by the ITA.

#### 9.2.1.8 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 test agency 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.

### 9.2.2 Test System

---

Vendors shall submit for testing the specific system which is to be offered to jurisdictions. Specifically,

- a. The hardware submitted for qualification testing shall be equivalent, in form and function, to the actual production versions of the hardware units.
- b. 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.
- c. The software submitted for qualification shall be identical to the escrowed version.
- 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.

## 9.3 Applicability

---

### 9.3.1 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. Hardware, system software and communications components with proven performance in commercial applications other than elections, however, need not be subject to all of the tests. Compatibility of these items with the voting environment shall be determined through functional tests integrating the standard product with the remainder of the system.

#### 9.3.1.1 Exclusions

---

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.

### 9.3.1.2 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 voting image, and including processing of the image (either from physical ballots or electronically activated images) and ending with the system's access to memory for the generation of output reports.
- b. Specialized compilers and specialized operating systems associated with ballot processing.
- c. Standard compilers and operating systems that have been modified for use in the vote counting process.

Ballot layout, vote recording, vote tabulation and audit trail shall be subjected to selectively in-depth code inspection. If an electronic voting system incorporates independent processing paths, each path or module shall be examined. 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).

## 9.3.2 Modifications to Qualified Systems

---

### 9.3.2.1 General Requirements for Modifications

---

Changes introduced after the system has completed qualification will necessitate further review. The ITA will determine tests necessary for re-qualification 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 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.

### 9.3.2.2 Potential for Limited Testing of Modifications

---

A modified system will be subject only to a limited qualification testing if it can be shown that:

- a. The change does not affect demonstrated compliance with these Standards for:
  - 1) Performance of voting system functions.
  - 2) Overall flow of system control.
  - 3) Manner in which ballots are defined and interpreted, or voting data are processed.
- b. The change also falls into one or more of the following classifications:
  - 1) It is made for the purpose of correcting a defect, and test documentation and configuration management records are provided which verify that the installation of the altered hardware or corrected code results solely in the elimination of the defect.
  - 2) It is made solely for the purpose of providing additional audit or report generating capability, using existing audit and reporting subroutines.
  - 3) It is made for the purpose of enabling interaction with other equipment (general purpose or approved), or with other computer programs and databases. Procedural and test documentation, and configuration management records, must be provided to verify that such interaction does not involve or adversely affect vote counting and data storage.
  - 4) It is made for the purpose of permitting operation on a different processor or of using additional or different peripheral devices, and does not alter the software's structure and function in any manner.

These exceptions are 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 elections software.

### 9.3.2.3 Utility Software and/Device Handlers

---

No retesting is required by the addition or alteration of utility software and device handlers that only interact with vote counting software through the Input/Output channels, as originally approved.

## 9.4 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 defines the voting system design, method of operation, and related resources. It contains:

- a. System functionality specifications
- b. System configuration overview
- c. System hardware specifications
- d. System software specifications
- e. System communications specifications
- f. System security specifications
- g. System test and verification specifications
- h. System parts, materials and supplies specifications
- i. Facilities specifications
- j. System installation and test specifications
- k. Personnel deployment and training requirements
- l. Voter Manual
- m. System Operations Manual
- n. System Maintenance Manual
- o. Diagnostic Testing Manual

The TDP is used by the ITA to assist in the construction and execution of the qualification testing plan. Volume II provides a detailed description of the TDP.

A second category of documentation is the vendor's documented practices for quality assurance and configuration management. 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 system 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 utilized for the system submitted for qualification testing.

## **9.5 Qualification Test Process**

---

The qualification test process may be performed by one or more ITAs which together perform the full scope of tests required by the VSS. 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 utilized, the testing generally consists of three phases: Pretest Activities, Qualification Testing, and Qualification Report Issuance and Post Test Activities.

### **9.5.1 Pretest Activities**

---

#### **9.5.1.1 Initiation of Testing**

---

Qualification testing shall be conducted at the request of the vendor, consistent with the provision of these Standards. The vendor shall:

- a. Request the performance of qualification testing from among the certified ITAs,
- b. Enter into formal agreement with the ITA(s) for the performance of testing, and

- c. Prepare and submit materials required for testing consistent with the requirements of these 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 9.3.2 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.

#### 9.5.1.2 Pretest Preparation

---

Pretest preparation encompasses the following activities:

- a. The vendor shall prepare and submit a complete technical data package (TDP) to the ITA. The TDP should consist of the items listed in Section 9.4 and specified in greater detail in VSS Volume II.
- b. The ITA shall perform an initial review of the TDP for completeness and clarity and requests 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 ITAs in exchange for payment by the vendor.
- e. The vendor shall deliver to the ITA all hardware and software needed to perform testing.

### 9.5.2 Qualification Testing

---

Qualification testing encompasses the activities described below:

#### 9.5.2.1 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. Verify or check equipment operational status by means of manufacturer operating procedures.
- b. Establish the test environment or the special environment required to perform the test.

- c. Initiate and complete operating modes or conditions necessary to evaluate the specific performance characteristic under test.
- d. Measure and record the value or range of values for the characteristic to be tested, demonstrating expected performance levels.
- e. Verify, as above, that the equipment is still in normal condition and status after all required measurements have been obtained.
- f. Confirm that documentation submitted by the vendor corresponds to the actual configuration and operation of the system.
- g. Confirm 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 VSS Volume II.

### 9.5.2.2 Qualification Test Practices

---

The ITA shall conduct the examinations and tests defined in the Test Plan such that all applicable tests identified in VSS Volume II are executed to determine compliance with the requirements in Sections 2-8 of these Standards. The ITA shall evaluate data resulting from examinations and tests, employing the following practices:

- a. If any malfunction or data error is detected which 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 which 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 which would invalidate the earlier test results.
- e. Any and all failures which 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:
  - 1) the vendor submits a design, manufacturing, or packaging change notice to correct a deficiency, together with test data to verify the adequacy of the change,

- 2) the examiner of the equipment agrees that the proposed change will correct the deficiency, and
  - 3) the vendor certifies that the change will be incorporated in all existing and future production units.
- f. If corrective action cannot be successfully taken as defined above, then the test shall be terminated, and the equipment shall be rejected.

### 9.5.2.3 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.
- c. Otherwise, all tests shall be performed at the required temperature and electrical supply voltage, regulated within the following tolerances:
  - 1) Temperature  $\pm 4$  degrees F
  - 2) Electrical supply voltage  $\pm 2$  vac

### 9.5.2.4 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.
- 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

### 9.5.2.5 Qualification Test Fixtures

---

ITAs may utilize 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 which utilize 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 which rely on the physical activation of a switch, a mechanical fixture with suitable motion generators is acceptable.
- b. ITAs may utilize 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 which are used in casting an actual ballot. In the event that only partial simulation is achieved, then an independent method and test procedure shall be used to validate the proper operation of those portions of the system not tested by the simulator.
- c. If the vendor provides a means of simulating the casting of ballots, the simulation device is subject to the same performance, reliability, and quality requirements that apply to the voting device itself.

### 9.5.2.6 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.

### 9.5.3 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 ITA(s). 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, for only the versions of the system elements tested by the ITA(s) and identified in the Qualification Test Report(s).
- 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.

#### 9.5.4 Time Limited Qualification for Data Transmission Using Public Networks

---

Generally a voting system remains qualified as long as no modifications are made to the system that have not been submitted to, and tested by, a certified ITA. The qualification test report remains valid for as long as the voting system remains unchanged.

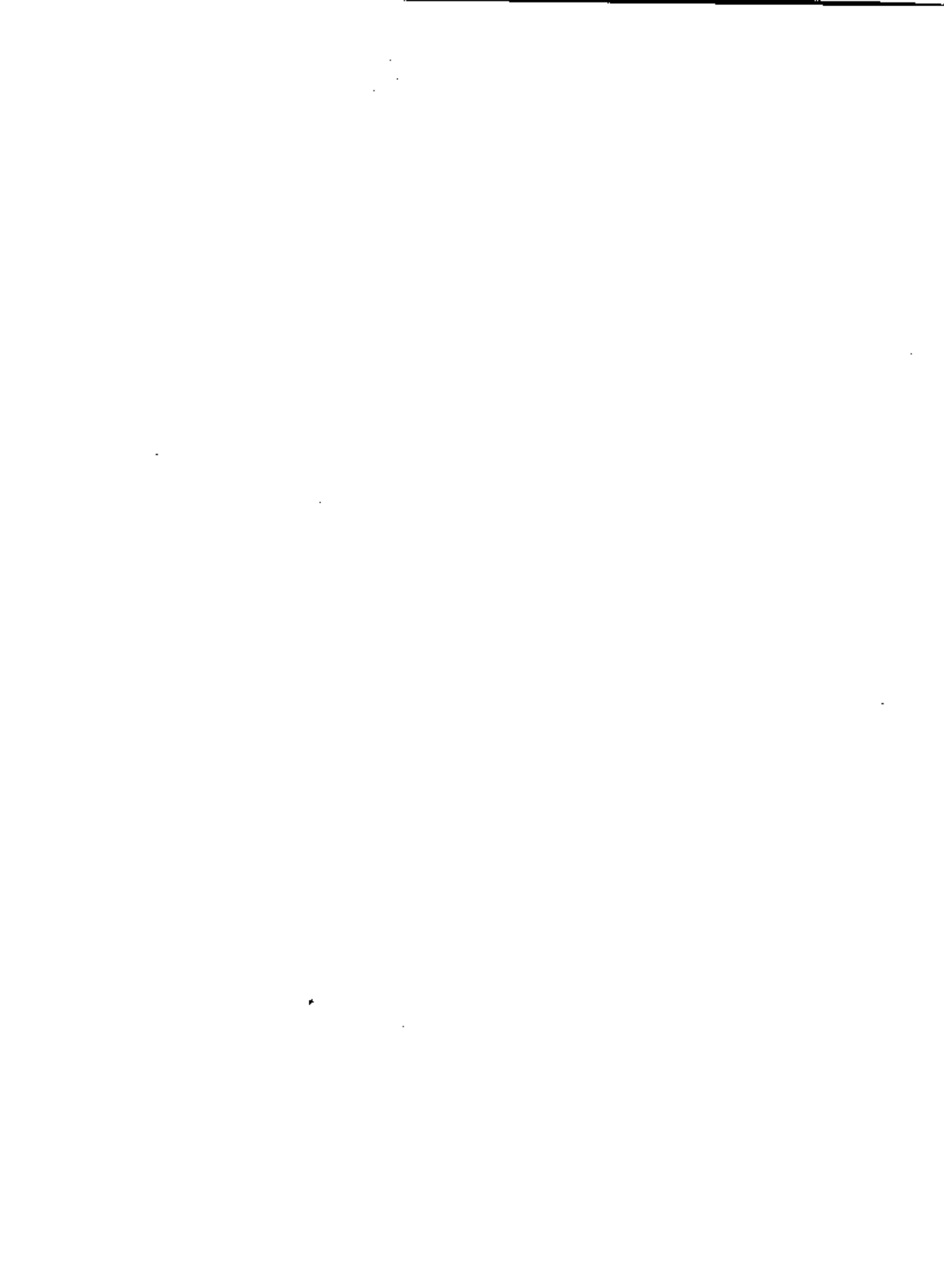
However, voting systems that transmit live system data using public networks, are subject to an additional requirement that recognizes that the risks and threats to system availability and integrity increase over time, and system capabilities that may have been adequate at one point in time may longer be sufficient. Internet voting systems, and systems that transmit data between poll sites and central offices using public networks are particularly vulnerable.

For systems that transmit live data using public networks (as defined in Section 5) the following standards for system qualification apply:



- a. The system shall therefore be given a VSS Qualification Number that is valid for only a single year, beginning with the date of issuance.
- b. The one year qualification applies to the initial system qualification, qualification of system modifications, and periodic annual re-qualification.
- c. Vendors shall submit their system for testing at least sixty calendar days in advance of the expiration of the current VSS Qualification Number.
- d. ITAs shall conduct re-qualification tests that confirm whether the system provides sufficient capabilities to fully meet the requirements of Section 5 of these Standards with respect to risks and threats that have been identified since the previous qualification testing for the system.

The above standards do not apply to systems that transmit data using public networks where the data transmitted is parallel to the transmission of official data or records and is not used to operate the system or report official election results.



# Table of Contents

---

A Glossary.....	A-1
-----------------	-----



# A

## Glossary

---

<b>Absentee ballot</b>	Ballots cast by voters unable to vote in person at their polling place on election day.
<b>Acceptance Test</b>	The examination of voting systems and their components by the purchasing election authority (usually in a simulated use environment) to validate performance of delivered units in accordance with procurement requirements, and validate that the delivered system is, in fact, a certified or qualified system. Testing to validate performance may be less broad than that involved with qualification testing and successful performance for multiple units (precinct count systems) may be inferred from a sample test.
<b>Adoption Date</b>	The date upon which the state adopts the standards.
<b>Algorithm</b>	A prescribed set of rules, processes, or sequence of steps (often iterative) to be followed to arrive at the solution to a problem.
<b>ASCII</b>	Represents the American Standard Code for Information Inter-change—A standard 7 or 8 bit code used to exchange information among equipment units. It is also the standard for digital communications over telephone lines.
<b>Application Software</b>	Software designed to fulfill specific needs of a user, for example election management, vote recording. (patterned after IEEE Std. 610.12-1990)
<b>Assembler</b>	A program that translates assembly language source code into machine-language object code. Each assembly language instruction is translated into one corresponding machine-language instruction. After all translation has taken place, the program is ready for execution by the computer.
<b>Assembly Language</b>	A lower level computer language which uses mnemonic instructions. It gives the programmer control over machine operations, and can manipulate data at the byte level, and, on some systems, at the bit level.
<b>Audit Trail</b>	An automated means to trace back to the original source of data any input record or process performed on a voting system.
<b>Authentication</b>	The process whereby a user or information source proves they are who they claim to be. In other words, the process of determining the identify of a user attempting to access a system
<b>Ballot Format</b>	One of any number of specific ballot configurations issued to the appropriate precinct. (Sometimes also referred to as 'ballot style').
<b>Ballot Image</b>	An electronically produced record of all votes cast by a single voter. (Also referred to as "ballot set")

<b>Ballot Preparation</b>	The process of using election databases to select the specific contests and questions to be contained in a ballot format and related instructions; preparing election specific software and firmware containing these selections; producing all possible ballot formats (or styles); and validating the correctness of ballot materials and software containing these selections for an upcoming election.
<b>Ballot Production</b>	The process of converting the ballot formats to a media ready for use in the physical ballot production or electronic presentation.
<b>Ballot Rotation</b>	The process of varying the location of candidate names on ballots to reduce the likelihood of positional voting bias. Candidate names may be rearranged according to a number of different formulas by voter, by precinct, or by political subdivision.
<b>Ballot Set</b>	See "Ballot Image"
<b>Baseline</b>	A product configuration that has been formally submitted for review against the Voting System Standards, and thereafter serves as the basis for further development; and that can be changed and offered to jurisdictions only through formal change control and requalification procedures (and/or recertification procedures where applicable). (Patterned after IEEE Std. 610.12-1990)
<b>Ballot Scanner</b>	A device used to read the data from a marksense ballot
<b>Bit Error Rate</b>	The number of errors divided by the total bits that are processed; the gauge of system accuracy.
<b>Block</b>	An element of structure for program coding which consists of declarations of data objects and their types, a BEGIN statement, descriptive comments, a sequence of statements that describe operations to be performed on the data objects listed in the declarations, and an END statement.
<b>Branch</b>	To depart from the sequential execution of the statements in a program by command. A branch may be conditional or unconditional. A conditional branch is one in which the flow of the program is altered from executing the next sequential instruction if certain conditions are met. An unconditional branch is one in which the flow of the program is always directed to some statement other than the next statement in the sequence of the program regardless of the condition.
<b>Canvass</b>	A compilation of election returns and validation of the outcome that forms the basis of the official results.
<b>Card Reader</b>	A device for computers, used to read the data from punch card ballots.
<b>Catastrophic System Failure</b>	A total loss of function or functions as opposed to a partial loss or degradation of function, such as, the loss or unrecoverable corruption of voting data, or the failure of an on-board battery for volatile memory.
<b>Central Processing Unit (CPU)</b>	The CPU performs all the arithmetic and logic operations, and controls the flow of information throughout the entire computer system.
<b>Certification Testing</b>	The 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 voting systems.
<b>Checkpointing</b>	A recovery method by which the system is designed to save all information necessary to define the state of the system at some point in time.

<b>Circuit</b>	A system of conducting paths and the electronic elements they connect that is constructed to perform a specific function.
<b>Client</b>	On a local area network or the Internet, a computer that accesses shared network resources provided by another computer called a server.
<b>Code</b>	As a noun, code means the system of characters, symbols, logic relationships, and rules for representing information. As a verb, to code means the same as to write, as in to code a program.
<b>Compiler</b>	A program that translates a source program written in a higher level language such as COBOL, FORTRAN, C++, Visual BASIC into a machine language program, written in object code that a computer can execute. A compiler may generate more than one machine language instruction for each source code instruction, whereas an assembler generates only one machine language instruction for each source code instruction. A compiler generates the complete object code program before it is executed by the computer.
<b>Component</b>	Individual elements or items that collectively comprise a device. Examples include circuit boards, internal modems, processors, disk drives, computer memory.
<b>Computer Program</b>	A collection of instructions coded according to specific rules, and in a specific sequence, that a computer can execute directly, or that can be translated into object code which the computer can execute. The program tells the computer what to do.
<b>Configuration Identification</b>	An element of configuration management, consisting of selecting the configuration items for a system and recording their functional and physical characteristics in technical documentation. (from IEEE Std. 610.12-1990)
<b>Configuration Index</b>	A document used in configuration management, providing an accounting of the configuration items that make up a product. (from IEEE Std. 610.12-1990)
<b>Configuration Item</b>	An aggregation of hardware, software or both that is designated for configuration management and treated as a single entity in the configuration management process. (from IEEE Std. 610.12-1990)
<b>Configuration Management</b>	A 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. (from IEEE Std. 610.12-1990)
<b>Configuration Status Accounting</b>	An element of configuration management, consisting of the recording and reporting of information needed to manage a configuration effectively. This information includes a listing of the approved configuration identification, the status of proposed changes to the configuration, and the implementation status of approved changes. (from IEEE Std. 610.12-1990)
<b>Count</b>	The process of totaling votes.
<b>Cross-party endorsement</b>	A candidate who has been nominated by more than one political party to run for a single elected office.
<b>Data Accuracy</b>	A term that refers to the system's ability to process voting data absent errors generated by the system internally. It is distinguished from data integrity which encompasses errors introduced by an outside source.

<b>Data Base</b>	The entire file or collection of data that is relevant to a particular application or the entire computer system, that is processed by the system over an extended period of time.
<b>Data Integrity</b>	A term that refers to the 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.
<b>Data Security</b>	The protection of data against unauthorized use, destruction, or disclosure, whether it is accidental or deliberate.
<b>Device</b>	A functional unit that performs its assigned tasks as an integrated whole.
<b>Diagnostic Program</b>	A test program used to test the individual units of a computer system, or the entire system itself to ensure that the software and hardware are functioning properly. Diagnostic programs can be used to test memory, the instruction set, and the various peripheral devices in an attempt to pinpoint the cause of a specific problem.
<b>Documentation</b>	Facts, notes, or instructions which are used to explain system functionality, software and hardware characteristics, and developmental testing. Many programming languages allow for documentation within the program itself.
<b>Driver</b>	A program or subprogram designed to control the operation of a specific piece of peripheral hardware, such as a card reader, printer or disk drive. The driver takes into account the specific characteristics unique to the device.
<b>Effective Date</b>	The state determined date after which systems presented for certification or acquisition should be in adherence with the standards.
<b>EEPROM (Electrically Erasable Programmable Read-Only Memory)</b>	Generally, read-only memory is memory that is nonvolatile and cannot be erased. An EEPROM is nonvolatile (will hold its data if power is shut off to it) but can be erased through a technique of pulsed signals.
<b>Election Coding</b>	See Election Programming.
<b>Election Databases</b>	A data file or set of files that contains geographic information about political subdivisions and boundaries; all contests and questions to be included in an election; and the candidates for each contest.
<b>Election Management System</b>	A 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.
<b>Election Programming</b>	The Process by which election officials or their designees use voting system software to logically define the ballot for a specific election. (Sometimes called Election Coding)
<b>Escrow</b>	The deposit of source code, object or executable code, documentation and other materials, including updates, modifications and version changes, with a neutral third party. (This third party is sometimes referred to as an Escrow Agent)
<b>FEC</b>	An acronym for the Federal Election Commission.
<b>Firmware</b>	Computer programs (software) stored in read-only memory (ROM) devices embedded in the system and not capable of being altered during system



operation.

**Functional Test**

A test performed to verify or validate the accomplishment of a function or a series of functions.

**Hardware**

The mechanical, electrical and electronic assemblies, including materials and supplies, which are a part of the system, such as microprocessor, disk drives, printer, circuit boards, integrated circuits.

**Higher Level Language**

A language which allows the programmer to write in a notation which is familiar, such as the use of English language words, as opposed to writing in mnemonics or directly in object code. Examples of higher level languages are COBOL, FORTRAN, Pascal, C++ and Visual BASIC. A higher level language is translated into object code by a compiler or interpreter.

**Initialization**

To return a computer to its original state when a program was first run by returning all counters, i.e., memory, to zero or their starting values.

**Input/Output Devices**

Those peripheral devices that allow human interface, storage of data, hard copy, or communication with another computer, such as keyboards, disk drives, printers, and modems.

**Integrated Circuit**

A microcircuit with all necessary components fabricated on a single chip. The chip is mounted inside a package, with pins along the side, that allows it to be plugged into a socket, or soldered directly onto a circuit board. The entire package is often referred to as the integrated circuit.

**ITA**

An acronym for Independent Test Authority.

**Light Pen**

A hand-held, pen-shaped, photosensitive device allowing a user to select, draw, or modify information on a CRT. The CPU can determine the coordinates of the light pen when it is touched to the screen. Light pens are very valuable in CAI or CAD applications, because the user does not have to be aware of the internal program that controls it in order to use it.

**Logical Correctness**

A condition signifying that, for a given input, a computer program will satisfy the program specification (produce the required output).

**Machine Language**

Machine language is the lowest level of programming, in which all instructions and data are represented in binary form. Programming directly in machine language consists of supplying the microprocessor in binary form with machine instructions, memory locations, and data in certain sequences. The program helps the microprocessor distinguish between instructions and data.

**Mainframe**

A high-level computer designed for the most intensive computational tasks. In early voting systems that used computer technology, this term referred to then large computers that relied primarily on punched cards for their input.

**Marksense Voting System**

A 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 use a ballot scanner to read the ballots.

**Memory**

Any device in a computer system where information can be stored for future use. The internal memory of a computer consists of ROM and RAM. ROM is Read-Only Memory. It is nonvolatile in that its contents remain stored even if power is removed. Information can be read from ROM, but cannot be placed into ROM. RAM is volatile memory. The contents of RAM will be destroyed if power is removed, and can be written over by the user. RAM is used to store the programs and information that the computer is currently processing.

<b>Microprocessor</b>	A chip that is the central processing unit of a computer containing the arithmetic-logic unit, a control unit, and data registers. Each microprocessor has its own unique instruction set.
<b>Modular Design</b>	A method of software design in which an independent body of code statements performs a single logical function. The module is self-contained, and its removal from the program will disable only its unique function.
<b>Network</b>	An interconnected system of transmission lines or wireless connections that allows computers, terminals, peripheral devices, and similar types of equipment to communicate with each other.
<b>Nonpartisan office</b>	An elected office for which candidates run independent of political party affiliation.
<b>Nonvolatile Memory</b>	Memory in which information can be stored indefinitely with no power applied. ROMs and EPROMs are examples of nonvolatile memory.
<b>Object Code</b>	The binary code produced by a compiler or assembler that can be executed directly by a computer without further simplification. A machine language program is written in object code.
<b>Operating System</b>	A supervisory program or collection of programs, used to manage the hardware and logic functions of a computer. An operating system may perform debugging, control the I/O devices, run the compiler or interpreter, and perform a variety of other housekeeping chores.
<b>Overvotes</b>	The generally prohibited practice of voting for more than the allotted number of candidates for the office being contested.
<b>Parity Check</b>	A method of determining the validity of data in which the summation of the binary digits for each word, or other specified piece of data, is checked against a previously computed parity digit.
<b>Partisan office</b>	An elected office for which candidates run as representatives of a political party.
<b>Password</b>	A series of characters that enable a user to access a file, computer, or program and help prevent unauthorized access.
<b>Political subdivision</b>	Any unit of government (often excepting school districts) having authority to hold elections for offices or on ballot issues.
<b>Polling Location</b>	The physical address of a polling place.
<b>Polling Place</b>	The area within the polling location where voters cast ballots.
<b>Precinct</b>	An administrative division representing a contiguous geographic area in which voters cast ballots at the same polling place. (A split precinct is a precinct containing more than one ballot format. Voters casting absentee ballots may also be combined into one or more absentee precincts ).
<b>Primary election</b>	An election held to determine which candidate will represent a political party in the general election. In a Closed Primary System, voters receive a ballot listing only those candidates running for office in the party with which they are registered. Unaffiliated voters may not participate. A variation of the closed primary allows unaffiliated voters to vote in one or more of the party primaries. Open Primary Systems allow all voters to vote in a party primary election. Depending on State law, voters may be required either to openly declare their choice of party ballot at the polling place, or they receive ballots for each political party and make their choice of which primary to participate in within the privacy

	of the voting booth. In a Blanket Primary System, voters receive a ballot listing all candidates running for office regardless of party affiliation.
<b>Primary presidential delegation nominations</b>	A primary election in which voters choose the delegates to the Presidential nominating conventions allotted to their State by the national party committees.
<b>Printed Circuit</b>	A circuit in which conducting strips are printed or etched into an insulating board, and used in place of wires, to form the conductive path between the various circuit components.
<b>Programming Language</b>	A systematic and structured means of communicating with a computer through the use of a defined set of characters written in predetermined sequences. There are three levels of programming languages. Machine language, which consists of binary object code, is the lowest level. Next come languages, such as assembly language, which uses mnemonics as aids for the programmer.. FORTRAN, COBOL, Pascal, C++ and Visual BASIC are examples of higher level languages. They contain familiar English words, and are translated into object code through the use of a compiler or interpreter. There are usually many machine language instructions for each source code instruction written in a higher level language.
<b>PROM (Programmable Read-Only Memory)</b>	A nonvolatile, or permanent, memory which can be programmed by the device manufacturer or supplier.
<b>Protocol</b>	The specific sequence of signals in the initial exchange between two communications devices, to make sure that the two devices can recognize each other's signals, and that the information being transmitted and received is intelligible. A protocol determines what pattern the flow of data bits will follow, and how the devices will cooperate in their communication. Protocols can be used between a computer and its peripherals. Protocols are common in networks, to verify that the user has authority to use the network.
<b>Punchcard Voting System</b>	One 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.
<b>Qualification Number</b>	A number issued by NASED to a system that has been tested by certified Independent Test Authorities for compliance with the national test standards. The issuance of a Qualification Number indicates that the system qualifies for certification process of states that have adopted the national standards.
<b>Qualification Test Report</b>	A report of results of independent testing of a voting system by an Independent Test Authority indicating the date testing was completed, the specific system version tested, and the scope of tests conducted
<b>Qualification Testing</b>	The examination and testing of a computerized voting system by an independent Test Authority using national test standards to determine if the system complies with the national performance and design standards and with its own specifications. This process occurs prior to state certification.
<b>RAM (Random Access Memory)</b>	Memory that provides immediate access to any information in storage. RAM in computers is in the form of an integrated circuit, that provides the computer with quick-access volatile memory. Information can be read from or written to RAM. However, when the power is turned off, all information in RAM is lost.
<b>Random Number</b>	A number selected from a group of numbers in such a way that each number in the group is equally likely to be chosen. Most programming languages for computers have the ability to select random numbers.
<b>Reassembly of multi-card</b>	????

<b>ballots</b>	
<b>Recall issues (with options)</b>	The 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. (There is no provision for the recall of federal office holders).
<b>Recertification</b>	The state examination, and possibly the retesting, of a voting system which 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.
<b>Remote Device</b>	A peripheral device that is not on-site, and is connected to a computer by a communications link, such as a telephone line, through the use of a modem or similar device.
<b>ROM (Read Only Memory)</b>	A nonvolatile form of memory that, once programmed, cannot be changed. ROM can be read from, but cannot be written to. If power is lost, the information in ROM remains. Also, the information in ROM cannot be changed by a computer operation.
<b>Server</b>	On a local area network, a computer running administrative software that controls access to the network and its resources, such as printers and disk drives, and provides resources to computers functioning as workstations on the network.  On the Internet or other network, a computer that responds to commands from a client.
<b>Software</b>	The application and operating system programs associated with a computer, as opposed to hardware that refers to the physical components of a computer system.
<b>Source Code</b>	A programmer codes a program in a specific language called source code. The source code of the computer language is then compiled, interpreted, or assembled into object code by the computer. The result is a machine language program in binary form which can be run by the computer.
<b>Split precinct</b>	See Precinct
<b>Straight party voting</b>	A mechanism by which voters are permitted to cast a vote indicating the selection of all candidates on the ballot for a single political party.
<b>Support Software</b>	Software that aids in the development or maintenance of other software, for example compilers, loaders and other utilities. (from IEEE Std. 610.12-1990)
<b>Systems Software</b>	The software for a particular computer, supplied by the manufacturer, and necessary for the basic operation and maintenance of the system. The software may be resident in ROM, or provided on disk or tape. Systems software generally includes the operating system, the I/O routines, diagnostic and debugging programs, and the programming language capabilities.
<b>Tabulation</b>	Same as Count
<b>Telecommunications</b>	The transmission and reception of information of any type, including data, television pictures, sound, and facsimiles using electrical or optical signals sent over wires or fibers or through the air.

<b>Undervotes</b>	The 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 3 out of a given number of candidates, and the voter chose only two candidates).
<b>Utility</b>	Computer software or firmware of a generic nature that assists the computer (and the programmer) in performing tasks as directed in specific applications programs.
<b>Validation</b>	The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements. (from IEEE Std. 610.12-1990)
<b>Verification</b>	The 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 that phase. (from IEEE Std. 610.12-1990)
<b>Vote for N of M</b>	A ballot choice in which voters are required to vote for a limited number of candidates for a single office from a larger field of candidates. (For example, in an election for city council voters may be told that they can only vote for six -the number of council seats up for election- out of twelve candidates actually listed on the ballot).
<b>Voter Registration System</b>	A 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 these Standards.
<b>Write-in-voting</b>	A 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, touchscreen or other electronic means to indicate their choice.



# Table of Contents

---

B Appendix B .....	B-1
B.1 Applicable Documents .....	B-1





# B

## Appendix B

---

### B.1 Applicable Documents

---

The following publications have been used for guidance in the preparation of this standard; they also contain information, which is useful in interpreting and complying with the requirements of this standard.

#### *Federal Regulations*

Code of Federal Regulations, Title 47, Parts 15 and 18, Rules and Regulations of the Federal Communications Commission

Code of Federal Regulations, Title 20, Part 1910, Occupational Safety and Health Act

#### *American National Standards Institute (ANSI)*

ANSI/ISO/IEC TR 9294.1990 Information Technology Guidelines for the Management of Software Documentation

#### *International Organization for Standardization (ISO)*

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 Electrotechnical Commission (IEC)*

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

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

ISO 9000-3:1997 Quality Management and Quality Assurance Standards – Part 3: Guidelines for Application of ISO9001: Development, Supply, Installation and Maintenance of Computer Software

ISO/IEC TR 13335-4:2000 Information technology—Guidelines for the management of IT Security—Part 4: Selection of safeguards

ISO/IEC TR 13335-3:1998 Information technology—Guidelines for the management of IT Security—Part 3 Techniques for the management of IT security

ISO/IEC TR 13335-2:1997	Information technology—Guidelines for the management of IT Security—Part 2: Managing and planning IT security
ISO/IEC TR 13335-1:1996	Information technology—Guidelines for the management of IT Security—Part 1: Concepts and models for IT security
ISO 10007:1995	Quality 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
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 102	Guideline for Computer Security Certification and Accreditation
FIPS 112	Password Usage
FIPS 113	Computer Data Authentication
FIPS 140-1	Security Requirements for Cryptographic Modules
FIPS 180-1	Secure Hash Standard
FIPS 188	Standard Security Label for Information Transfer
FIPS 196	Entity Authentication Using Public Key Cryptography
FIPS (number TBD)	Advanced Encryption Standard (AES) (Expected to become official August-March 2001)

**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

***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
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
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-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
MIL-STD-498	Software Development and Documentation, 27 May 1998
MIL-STD-2168	Software Quality Program, 27 March 1992

