California Voting System Standards

California Secretary of State

October 2014

Table of Contents

Voting System Standards Summary

The Voting System Standards (Standards), describe the requirements for the electronic components of voting systems. These Standards are derived from the EAC Voluntary Voting System Guidelines versions 1.1 and 2.0. The standards contain the following sections:

Section 1 describes the purpose and scope of the Voting System Standards.

Section 2 describes the functional capabilities required of voting systems. This section reflects Help America Vote Act (HAVA) Section 301 and California Elections Code requirements.

Section 3 describes standards that make voting systems more usable and accessible for as many eligible Californians as possible. This section reflects the HAVA 301 (a)(3) accessibility requirements.

Sections 4 through 6 describe specific requirements for election system hardware, software, telecommunications, and security.

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

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

Section 9 describes documentation relating to the voting system that is required as a precondition of testing. The documentation defines the voting system and its method of operation, provides technical and test data supporting the claims of the system's functional capabilities and performance levels, and documents instructions and procedures governing the system operation and field maintenance.

1 Introduction

1.1 Purpose and Scope of the Voting System Standards

The Voting System Standards provide a set of specifications and requirements against which voting systems shall be tested to determine if they provide all the basic functionality, accessibility, and security capabilities required of voting systems. The Standards specify the functional requirements, performance characteristics, documentation requirements, and test evaluation criteria for the certification of voting systems. To the extent possible, these requirements and specifications are described so they can be assessed by a series of defined, objective tests.

Except as noted, the Voting System Standards apply to all system hardware, software, telecommunications, and documentation intended for use to:

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

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

1.2 Use of the Voting System Standards

The Standards are intended to guide the development, testing, and acquisition of voting systems and will be used by:

- The state-approved testing agencies (S-ATA) who use this information to develop test plans and procedures for the analysis and testing of systems in support of the certification testing process
- Local election officials who are evaluating voting systems for potential use in their jurisdictions
- Voting system designers and manufacturers who need to ensure that their products fulfill all these requirements so they can be certified
- Voters who are interested in the rigorous testing process voting systems are subjected to California to ensure accuracy, accessibility and security in the voting process

1.3 Definitions, References, and Types of Voting Systems

1.3.1 Definitions and References

The Standards contain terms describing function, design, documentation, and testing attributes of voting system hardware, software and telecommunications. Unless otherwise specified, the intended sense of technical terms is that which is commonly used by the information technology industry. In some cases terminology is specific to elections or voting systems. Non-technical terms **shall** be interpreted according to their standard dictionary definitions.

There are a number of technical standards that are incorporated in the Standards by reference. These are referred to by title in the body of the document.

1.3.2 Types of Voting Systems

HAVA Section 301 and the California Elections Code define a voting system as the total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment), that is used to define ballots; to cast and count votes; to report or display election results; and to maintain and produce any audit trail information. In addition, a voting system includes the practices and associated documentation used to identify system components and versions of such components; to test the system during its development and maintenance; to maintain records of system errors and defects; to determine specific system changes made after initial certification; and to make available any materials to the voter (such as notices, instructions, forms, or paper ballots).

In addition to defining a common set of standards that apply to all voting systems, the Standards identify requirements specific to a particular type of voting system, where appropriate. However, the Standards recognize that as new solutions and technology continues to evolve, the distinctions between voting system types may become blurred. The Standards contain appropriate procedures to ensure new developments provide the necessary integrity and can be properly evaluated in the certification process.

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

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

- Permit the voter to verify (in a private and independent manner) the vote selected by the voter on the ballot before the ballot is cast and counted
- Provide the voter with the opportunity (in a private and independent manner) to change the ballot or correct any error before the ballot is cast and counted
- Notify the voter if he or she has selected more than one candidate for a single office, inform the voter of the effect of casting multiple votes for a single office, and provide the voter an opportunity to correct the ballot before it is cast and counted
- Be accessible for individuals with disabilities in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters
- Provide alternative language accessibility pursuant to Section 203 of the Voting Rights Act and California Elections Code section 14201

1.3.2.1 Paper-Based Voting System

A paper-based voting system records votes, counts votes, and produces a tabulation of the vote count from votes cast on paper cards or sheets. A marksense (also known as optical scan) voting system allows a voter to record votes by making marks directly on the ballot, usually in voting response locations. Additionally, a paper-based system may allow for the voter's selections to be indicated by marks made on a paper ballot by an electronic input device, as long as such an input device does not independently record, store, or tabulate the voter selections.

1.3.2.2 Direct-Recording Electronic Voting System

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

1.3.2.3 Precinct Count Voting System

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

1.3.2.4 Central Count Voting System

A central count voting system is a voting system that tabulates ballots from multiple precincts at a central location. Voted ballots are typically placed into secure storage at the polling place. Stored ballots are transported to a central counting location, via a

non-networked means. The system produces a printed report of the vote count, and may produce a report stored on electronic media.

1.4 Conformance Clause

This section provides information and requirements relating to how manufacturers and S-ATAs use this document to assess whether a voting system conforms to the Standards.

1.4.1 Structure of Requirements

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

1.4.1.1 Normative Language

The following keywords are used to convey conformance requirements:

- **Shall –** indicates a mandatory requirement in order to conform. Synonymous with "is required to."
- **Shall not**, **is prohibited** –indicates a mandatory requirement that indicates something that is not permitted (allowed) in order to conform.
- **May** - indicates an optional, permissible action. Synonymous with "is permitted."

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

1.4.1.2 Applicability

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

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

The terms used to designate requirements and procedural standards for state-approved testing agencies are indicated by referring to "S-ATA". Other terms in these Standards **shall** be construed as synonymous with "S-ATA," including "accredited test labs," and "voting system test labs."

1.4.1.3 Categorizing Requirements

The Standards set forth a common set of requirements for certification that apply to all types of electronic voting systems. They also provide requirements that are applicable for particular circumstances, such as alternative language capability or disability accessibility. The requirements implementing the HAVA Section 301(a) mandates, except for disability accessibility, must be met by all voting systems. The alternative language capability mandated by Section 301(a)(4) must be met by all systems intended for use in jurisdictions subject to Section 203 of the Voting Rights Act. The Section 301(a)(3) disability accessibility requirements must be met by all systems intended to fulfill the one per polling place disability equipped voting system provision of Section 301(a)(3)(B).

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

Among the categories defined in the Standards are two types of voting systems with respect to mechanisms to cast votes – paper-based voting systems and DRE voting systems. Additionally, paper-based voting systems are further categorized as precinct count voting systems, and central count voting systems. The Standards define specific requirements for systems that fall within these four categories as well as various combinations of these categories.

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

1.4.1.4 Extensions

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

1.4.2 Implementation Statement

The manufacturer **shall** provide an implementation statement with their application for certification testing.

An implementation statement documents the requirements that have been implemented by the voting system, the optional features and capabilities supported by the voting system, and any extensions (i.e., additional functionality beyond what is defined in the Standards) that it implements.

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

a. An implementation statement **shall** include:
    i. Full product identification of the voting system, including version number or timestamp;
    ii. Separate identification of each device that is part of the voting system;
    iii. Voting variations supported;
    iv. Device capacities and limits;
    v. List of languages supported;
    vi. List of accessibility capabilities; and
    vii. Signed attestation that the foregoing accurately characterizes the system submitted for testing.

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

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

1.5 Testing Process - Overview

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

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

- Accuracy in the recording and processing of voting data, as measured by report total error rate
- Operational failures or the number of failures under conditions simulating the intended storage, operation, transportation, and maintenance environments for voting systems
- System performance and function under normal and abnormal conditions
- Completeness and accuracy of the system documentation and configuration management records to enable purchasing jurisdictions to effectively install, test, and operate the system

1.5.1 Test Categories

The certification test is conducted in several parts against the requirements established above:

- Functionality testing - This part of the testing process is not rigidly defined. Although there are basic functionality testing requirements, additions or variations in testing are appropriate depending on the system's use of specific technologies and configurations, the system capabilities, and the outcomes of previous testing.
- Hardware testing - 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 laboratory or shop environment. The non-operating tests are intended to evaluate the ability of the system hardware to withstand exposure to the various environmental conditions incidental to voting system storage, maintenance, and transportation. The procedures are based on test methods contained in Military Standards (MIL-STD) 810D, modified where appropriate, and include such tests as: bench handling, vibration, low and high temperature, and humidity. The operating tests involve running the system for an extended period of time under varying temperatures and voltages. The procedure emphasizes equipment operability and data accuracy; it is not an exhaustive evaluation of all system functions. Moreover, the severity of the test conditions, in most cases, has been reduced from that specified in the Military Standards to reflect commercial and industrial practice.
- Software evaluation – Software evaluation looks at programming completeness, consistency, correctness, modifiability, structure, and traceability, along with its modularity and construction. The code inspection is followed by a series of functional tests to verify the proper performance of all system functions controlled by the software.
- System level integration tests, including audits – This part tests the fully integrated system components, internal and external system interfaces,

usability and accessibility, and security by exercising all election management functions, ballot-counting logic, and system capacity. The process also includes the Physical Configuration Audit (PCA) and the Functional Configuration Audit (FCA). The PCA compares the voting system components submitted for qualification to the manufacturer's technical documentation and confirms that the documentation submitted meets the requirements. As part of the PCA, the S-ATA 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 manufacturer's documentation to verify the accuracy and completeness of the system Technical Data Package (TDP). The various options of software counting logic that are claimed in the manufacturer's documentation shall be tested during the system-level FCA. Generic test ballots or test entry data for DRE systems, representing particular sequences of ballot-counting events, will test the counting logic during this audit. The security component of this part of testing focus on the ability of the system to detect, prevent, log, and recover from a broad range of security risks 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.

- Examination of documented manufacturer practices for quality assurance and for configuration management – This portion of the testing involves reviewing the documentation submitted for its completeness and accuracy in describing the system and its conformance to the requirements for manufacturer configuration and quality assurance practices.

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

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

1.5.2 Testing Sequence

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

a. Initial examination of the system and the technical documentation provided by the manufacturer to ensure that all components and documentation needed to conduct testing have been submitted, and to help determine the scope and level of effort of testing needed
b. Examination of the manufacturer's Quality and Configuration Management Manual previously submitted to the Secretary of State.
c. Development of a detailed system test plan that reflects the scope and complexity of the system, and the status of system certification (i.e., initial certification or a re-certification to incorporate modifications).
d. Code review for selected software components.
e. Witnessing of a system 'build' conducted by the manufacturer to conclusively establish the system version and components being tested.
f. Operational testing of hardware components, including environmental tests, to ensure that operational performance requirements are achieved.
g. Functional and performance testing of hardware components.
h. System installation testing and testing of related documentation for system installation and diagnostic testing.
i. Functional and performance testing of software components.
j. Functional and performance testing of the integrated system, including testing of the full scope of system functionality, performance tests for telecommunications and security; and examination and testing of the System Operations Manual.
k. Examination of the system maintenance manual.
l. Preparation of the Certification Test Report.
m. Delivery of the Certification Test Report.

1.5.3 General Applicability

Voting system hardware, software, communications and documentation are examined and tested to determine suitability for elections use. Examination and testing addresses the broad range of system functionality and components, including system functionality for pre-voting, voting, and post-voting functions. All products custom designed for election use **shall** be tested in accordance with the applicable procedures. COTS hardware, system software and communications components with proven performance in commercial applications other than elections, however, are exempted from certain

portions of the test as long as such products are not modified for use in a voting system. Compatibility of these products with other components of the voting system **shall** be determined through functional tests integrating these products with the remainder of the system.

1.5.3.1 General Requirements for Modifications

The SOS in conjunction with the S-ATA will determine tests necessary to certify the modified system based on a review of the nature and scope of changes, and other submitted information including the system documentation, manufacturer test documentation, configuration management records, and quality assurance information. Based on this review, SOS may:

a. Determine that a review of all change documentation against the baseline materials is sufficient for recommendation for certification.
b. Determine that all changes must be retested against the previously certified version. This will include review of changes to source code, review of all updates to the TDP, and performance of system level and functional tests
c. Determine that the scope of the changes is substantial and will require a complete retest of the hardware, software, and/or telecommunications

1.5.3.2 Basis for Limited Testing Determinations

The SOS may determine that a modified system will be subject only to limited certification testing if the manufacturer demonstrates that the change does not affect demonstrated compliance for:

a. Performance of voting system functions
b. Voting system security and privacy
c. Overall flow of system control
d. The manner in which ballots are defined and interpreted, or voting data are processed

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

1.5.4 Certification Test Process

The certification test process may be performed by one or more S-ATAs that together perform the full scope of tests required. Where multiple S-ATAs 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 S-ATA independently of the other testing performed by other S-ATAs. Testing may be coordinated across S-ATAs so that hardware/firmware tested by one S-ATA can be used in the overall system tests performed by another S-ATA.

When multiple S-ATAs are being used, the development of the Test Plan and the Test Report **shall** be coordinated by a lead S-ATA. The lead lab is responsible for ensuring that all testing has been performed and documented.

Whether one or more S-ATAs are used, the testing generally consists of three phases:

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

1.5.4.1 Pre-test Activities

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

a. Initiation of Testing - Certification testing **shall** be conducted at the request of any interested person and **shall**:
   i. Request the performance of certification testing from among the state-approved testing agencies
   ii. Deposit an initial sum of money, to be determined by the Secretary of State based upon the scope of testing required, into the manufacturer's escrow account held at the Office of the Secretary of State
   iii. Prepare and submit materials required for testing

   Certification testing **shall** be conducted for the initial version of a voting system as well as for all subsequent changes to the system prior to release for sale or for installation. The nature and scope of testing for system changes or new versions **shall** be determined by the SOS based on the nature and scope of the modifications to the system and on the quality of system documentation and configuration management records submitted.

b. Pre-test Preparation - Encompasses the following activities:
   i. The submittal of a complete TDP to the SOS.
   ii. The SOS **shall** perform an initial review of the TDP for completeness and clarity and request additional information as required.
   iii. Additional information, if requested by the SOS.
   iv. The delivery of all hardware and software needed to perform testing.

1.5.4.2 Certification Testing

Certification testing encompasses the preparation of a test plan, the establishment of the appropriate test conditions, the use of appropriate test fixtures, the witness of the system

build and installation, the maintenance of certification test data, and the evaluation of the data resulting from tests and examinations.

a. Test Plan - The SOS in conjunction with the S-ATA-**shall** prepare a Test Plan to define all tests and procedures required to demonstrate compliance with the Standards, including:
    i. Verifying or checking equipment operational status by means of manufacturer operating procedures.
    ii. Establishing the test environment or the special environment required to perform the test.
    iii. Initiating and completing operating modes or conditions necessary to evaluate the specific performance characteristic under test.
    iv. Measuring and recording the value or range of values for the characteristic to be tested, demonstrating expected performance levels.
    v. Verifying, as above, that the equipment is still in normal condition and status after all required measurements have been obtained.
    vi. Confirming that documentation submitted by the manufacturer corresponds to the actual configuration and operation of the system.
    vii. Confirming that documented manufacturer practices for quality assurance and configuration management comply with the Standards and the Quality and Configuration Manual.
b. Appropriate Test Conditions - The S-ATA may perform the tests in any facility capable of supporting the test environment. The following practices **shall** be employed:
    i. Preparations for testing, arrangement of equipment, verification of equipment status, and the execution of procedures **shall** be witnessed by at least one independent, qualified observer in the form of an accredited testing laboratory, which **shall** certify that all test and data acquisition requirements have been satisfied
    ii. 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
    iii. Otherwise, all tests **shall** be performed at the required temperature and electrical supply voltage, regulated within the following tolerances:
        - Temperature ±4 degrees F
        - Electrical supply voltage ±2 volts alternating current
    iv. Routine, scheduled maintenance of voting system hardware **shall** be performed in compliance with the maintenance schedule documented by the manufacturer in the voting equipment user documentation included in the Technical Data Package. If no such schedule was provided then it **shall** be assumed that no scheduled maintenance is required.
c. Appropriate Test Fixtures - The S-ATA **shall** not use simulation devices or software that bypass portions of the voting system that would be exercised in an actual election, with the following exceptions:
    i. The S-ATA may bypass the user interface of an interactive device in the

case of environmental tests that would require subjecting test "voters" to unsafe or unhealthy conditions, or that would be invalidated by the presence of a test "voter."

ii. The S-ATA may bypass the user interface of an interactive device in capacity tests to verify that the system and its constituent components are able to operate correctly at the maximum limits specified in the implementation statement; for example, maximum number of ballots that can be counted, maximum possible vote total (counter capacity), or maximum number of ballot styles.

The S-ATA may use test fixtures or ancillary devices to facilitate testing as long as they closely and validly simulate actual election use of the system. If a tabulator is specified to count paper ballots that are manually marked with a specific writing utensil, it is not valid to substitute ballots that were mechanically marked by a printer. However, ballots that were marked according to manufacturer instructions can sometimes be recycled through a tabulator without invalidating the test.

d. Witness of System Build and Installation - Although most testing is conducted at facilities operated by the S-ATA, the witness build and installation, a key element of voting system testing, **shall** be conducted at either the SOS or the S-ATA site with SOS and S-ATA personnel present. The S-ATA responsible for testing voting system software, telecommunications, and integrated system operation (i.e., system level testing) **shall** witness the final system build, encompassing hardware, software and communications, and the version of associated records and documentation. The system elements witnessed, including their specific versions, **shall** become the specific system version that is recommended for certification.

e. Certification Test Data Requirements - The following test data practices **shall** be employed:
   i. A test log of the procedure **shall** be maintained. This log **shall** identify the system and equipment by model and serial number.
   ii. Test environment conditions **shall** be noted.
   iii. 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.

f. Certification Test Practices - The S-ATA **shall** conduct the examinations and tests defined in the test plan to determine compliance with the voting system requirements. If any failure, malfunction or data error is detected, its occurrence and the duration of operating time preceding it **shall** be recorded for inclusion in the analysis of data obtained from the test.

Conformity assessment is not quality assurance. If a critical software defect (a software defect responsible for the incorrect recording, tabulation, or reporting of a vote) is found, the system cannot be considered trustworthy even after the

known fault is corrected, because the cases that the S-ATA does not have the opportunity to test can be expected to conceal similar faults. Therefore,

i. If a logic defect is found to be responsible for the incorrect recording, tabulation, or reporting of a vote, testing **shall** be halted.
ii. If the S-ATA finds such a profusion of logic defects as to indicate that the manufacturer's quality assurance was inadequate, testing **shall** be halted.
iii. If a logic defect is found that is not responsible for the incorrect recording, tabulation, or reporting of a vote, and the condition described in subrequirement ii does not apply, testing **shall** be suspended and the system returned to the manufacturer for correction and quality assurance. The failure **shall** be accounted for in the reliability assessment. Without halting or suspending the testing of the entire system, noncritical software defects may be corrected. All revisions to the software must be performed within the manufacturer's quality assurance and configuration management processes and must undergo manufacturer regression testing before the testing process is resumed for the entire system, or in the case of a noncritical defect, the affected software components. When it is resumed, the regression testing that the S-ATA performs for the change that was made **shall** be documented in the test report.

In addition to logic defects, there may be hardware failures as well as simple nonconformities in which the behavior of the system under test does not meet the requirements. In the case of hardware failures, the manufacturer may replace a component that has suffered a random failure, or the manufacturer may opt to suspend testing in order to correct a hardware design defect that caused a nonrandom failure. Either way, the failure **shall** be accounted for in the reliability assessment.

iv. If the anomaly is other than a logic defect, and if corrective action is taken to restore the equipment to a fully operational condition within eight work hours, including all troubleshooting time beyond what is needed to enable the S-ATA to categorize the anomaly, then testing may be resumed at the point of suspension.
v. Otherwise (i.e., if the previous paragraph does not apply), the S-ATA **shall** maintain a record of the procedures that have been satisfactorily completed. When testing is resumed at a later date, repetition of the successfully completed procedures may be waived provided that no design or manufacturing change has been made that would invalidate the earlier test results.
vi. Testing may resume after a nonconformity is found if:
    - The manufacturer submits a design, manufacturing, or packaging change notice to correct the nonconformity, together with test data to verify the adequacy of the change;
    - The examiner of the equipment agrees that the proposed change is responsive to the full scope of the nonconformity;
    - Any previously failed tests are passed by the revised system; and
    - The manufacturer attests that the change will be incorporated into all

existing and future production units.

Consistent with configuration management, the corrected system is formally a different system from the one that failed. The failure of the previous version is never "purged;" rather, a new revision of the system is found not to suffer the same nonconformity.

1.5.4.3 Post-test Activities

Certification report issuance and post-test activities encompass the activities described below.

a. The S-ATA **shall** prepare a Test Report that confirms the voting system has passed the required testing. This report **shall** include the date testing was completed, the specific system version addressed by the report, the version numbers of all system elements separately identified with a version number by the manufacturer, and the scope of tests conducted.
b. Where a system is tested by multiple S-ATAs, the lead S-ATA **shall** prepare a consolidated Test Report.
c. The S-ATA **shall** deliver the report to the SOS.

2 Functional Requirements

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

The following terms as used herein, are defined as follows:

- **Application logic**: Software, firmware, or hardwired logic from any source that is specific to the voting system, with the exception of border logic.
- **Ballot counting logic**: The software logic that defines the combinations of voter choices that are valid and invalid on a given ballot and that determines how the vote choices are totaled in a given election
- **Border logic**: Software, firmware, or hardwired logic that is developed to connect application logic to COTS or third-party logic. Note: Although it is typically developed by the voting system manufacturer, border logic is constrained by the requirements of the third-party or COTS interface with which it must interact. It is not always possible for border logic to achieve its function while conforming to coding standards. For this reason, border logic should be minimized relative to application logic and where possible, wrapped in a conforming interface. An example of border logic that could not be so wrapped is a customized boot manager that connects a bootable voting application to a COTS BIOS.

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

2.1 Overall System Capabilities: These functional capabilities apply throughout the election process. They include security, accuracy, integrity, system auditability, election management system, vote tabulation, ballot counters, telecommunications, and data retention.

2.2 Pre-voting Capabilities: These functional capabilities are used to prepare the voting system for voting. They include ballot preparation, the preparation of election-specific software (including firmware), the production of ballots, the installation of ballots and ballot counting software (including firmware), and system and equipment tests.

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

2.4 Post-voting Capabilities: These functional capabilities apply after all votes have been cast. They include closing the polling place; obtaining reports by voting machine, polling place, and precinct; obtaining consolidated reports; and obtaining reports of audit trails.

2.5 Maintenance, Transportation and Storage Capabilities: These capabilities are necessary to maintain, transport, and store voting system equipment.

2.6 Testing Requirements – Functionality: This section describes the test procedures that address Overall system capabilities, Pre-voting functions, Voting functions, Post-voting functions, System maintenance, and Transportation and storage. This section focuses on the testing of the component and system specific capabilities.

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

2.1 Overall System Capabilities

This section defines required functional capabilities that are system-wide in nature and not unique to pre-voting, voting, and post-voting operations. Functional capabilities outlined in this section are:

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

2.1.1 Security

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

a. Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability
b. Provide system functions that are executable only in the intended manner and order, and only under the intended conditions
c. Use the system's control logic to prevent a system function from executing if any preconditions to the function have not been met
d. Provide safeguards in response to system failure to protect against tampering during system repair or interventions in system operations

e. Provide security provisions that are compatible with the procedures and administrative tasks involved in equipment preparation, testing, and operation
f. Incorporate a means of implementing a capability if access to a system function is to be restricted or controlled
g. Provide documentation of mandatory administrative procedures for effective system security

2.1.2 Accuracy

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

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

a. Record the election contests, candidates, and issues exactly as defined by election officials
b. Record the appropriate options for casting and recording votes
c. Record each vote precisely as indicated by the voter and produce an accurate report of all votes cast
d. Include control logic and data processing methods incorporating parity and checksums (or equivalent error detection and correction methods) to demonstrate that the system has been designed for accuracy
e. Provide software that monitors the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected
f. Maintain absolute correctness (introduce no errors) in the recording, tabulating, and reporting of votes in voting system software, firmware, and hardwired logic.

In addition, DRE systems **shall:**

g. Record and retain redundant copies of the original ballot image. A ballot image is an electronic record of all votes cast by the voter, including undervotes.

The accuracy benchmark is intended to allow tolerance for unpreventable hardware-related errors that occur rarely and randomly as a result of physical phenomena affecting optical scanning sensors. It is not intended to allow tolerance of software faults that result in systematic miscounting of votes. No margin for error exists.

2.1.3 Error Recovery

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

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

2.1.4 Integrity

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

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

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

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

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

2.1.5 System Audit

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

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

The subsections that follow present operational requirements critical to acceptable performance and reconstruction of an election.

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

Documentation of items such as paper ballots delivered, paper ballots collected, administrative procedures for system security, and maintenance performed on voting equipment are also part of the election audit trail, but are not covered in these technical standards.

2.1.5.1 Operational Requirements

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

a. Voting system equipment **shall** record activities through an event logging mechanism.
b. Voting system equipment **shall** enable file integrity protection for stored log files as part of the default configuration.
c. The voting system equipment logs **shall** not contain information that, if published, would violate ballot secrecy or voter privacy or that would compromise voting system security in any way.
d. The voting system equipment **shall** log at a minimum the following data characteristics for each type of event: 1) system ID; 2) unique event ID and/or type; 3) timestamp; 4) success or failure of event, if applicable; 5) User ID trigger the event, if applicable; 6) Resources requested, if applicable.
    i. Timekeeping mechanisms **shall** generate time and date values.
    ii. The precision of the timekeeping mechanism **shall** be able to distinguish and properly order all audit records.
    iii. Timestamps **shall** include the date and time, including hours, minutes and seconds.
    iv. Timestamps **shall** comply with ISO 8601 and provide all four digits of the year and include the applicable time zone.
    v. Voting system equipment **shall** only allow administrators to set or adjust the clock.
    vi. Voting system equipment **shall** limit clock drift to a minimum of 1 minute within a 15 hour period after the clock is set.
e. Voting system equipment **shall** log all normal and abnormal events.
    i. Voting system equipment **shall** ensure that event logging cannot be disabled.

f. Voting system equipment **shall** implement default settings for secure log management activities, including log generation, transmission, storage, analysis and disposal.
g. Voting system equipment **shall** log logging failures, log clearing, and log rotation.
h. Voting systems **shall** store logs in a publicly documented log format, such as XML, or include a utility to export the logs into a publicly documented format for off-system viewing.
i. The manufacturer **shall** ensure that voting system equipment is supplied with enough free storage to include several maximum size event logs.
j. Voting systems **shall** be capable of retaining event log data from previous elections.
k. Voting system equipment **shall** only allow administrators to modify the log data retention settings including the actions to take when a log reaches its maximum retention such as overwriting logs, rotating logs, or halting logging.
l. Voting system equipment **shall** be capable of rotating the event log data to manage log file growth.
m. Voting system equipment **shall** restrict event log access to write or append-only for privileged logging processes and read-only for administrators accounts or roles.
n. Voting system equipment **shall** digitally sign and export event logs at the end of an election.
o. Voting systems **shall** include an application or program to view, analyze, and search event logs.
p. Voting system equipment **shall** halt voting activities and create an alert if the logging system malfunctions or is disabled.
q. Voting system equipment **shall** create an alert at user-defined intervals as logs begin to fill.
r. Voting system equipment **shall** protect event log information from unauthorized access, modification and deletion.
s. If the voting system provides log archival capabilities, it **shall** ensure the integrity and availability of the archived logs.

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

a. The voting system **shall** generate, store, and report to the user all error messages as they occur.
b. All error messages requiring intervention by an operator or precinct official **shall** be displayed or printed clearly in easily understood language text, or by means of other suitable visual indicators.
c. When the voting system uses numerical error codes for trained technician maintenance or repair, the text corresponding to the code **shall** be self-contained or affixed inside the voting machine. This is intended to reduce inappropriate reactions to error conditions, and to allow for ready and effective problem correction.
d. All error messages for which correction impacts vote recording or vote processing **shall** be written in a manner that is understandable to an election official who possesses training on system use and operation, but does not possess technical training on system servicing and repair.

e. The message cue for all voting systems **shall** clearly state the action to be performed in the event that voter or operator response is required.
f. Voting system design **shall** ensure that erroneous responses will not lead to irreversible error.
g. Nested error conditions **shall** be corrected in a controlled sequence such that voting system status **shall** be restored to the initial state existing before the first error occurred.

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

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

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

2.1.5.2 Use of Multitasking Operating Systems

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

Simultaneous processes of concern include: unauthorized network connections, unplanned user logins, and unintended execution or termination of operating system processes. An unauthorized network connection or unplanned user login can host unintended processes and user actions, such as the termination of operating system audit, the termination of election software processes, or the deletion of election software audit and logging data. The execution of an operating system process could be a full system scan at a time when that process would adversely affect the election software processes. Operating system processes improperly terminated could be system audit or malicious code detection.

To counter these vulnerabilities, three operating system protections are required on all multitasking operating systems. First, authentication **shall** be configured on the local terminal (*e.g.*, display screen and keyboard) and on all external connection devices *(e.g.*,

network cards and ports). This ensures that only authorized and identified users affect the system while election software is running.

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

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

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

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

For a given system, some requirements may appropriately be determined to be not applicable to a specific device (e.g., ballot marking devices), depending specifically how the design of a device is implemented and what features are included. Those determinations will be decided on a case-by-case, model by model, revision by revision basis, by the Secretary of State in conjunction with the S-ATA.

2.1.6 Election Management System

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

- Define political subdivision boundaries and multiple election districts as indicated in the system documentation
- Identify contests, candidates, and issues
- Define ballot formats and appropriate voting options

- Generate ballots and election-specific programs for voting equipment
- Install ballots and election-specific programs
- Test that ballots and programs have been properly prepared and installed
- Accumulate vote totals at multiple reporting levels as indicated in the system documentation
- Generate the post-voting reports required
- Process and produce audit reports of the data

2.1.7 Vote Tabulating Program

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

2.1.7.1 Functions

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

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

2.1.7.2 Voting Variations

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

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

2.1.8 Ballot Counter

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

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

2.1.9 Telecommunications

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

Voter Authentication: Coded information that confirms the identity of a voter for security purposes for a system that transmit votes individually over a public network
Ballot Definition: Information that describes to voting equipment the content and appearance of the ballots to be used in an election
Vote Count: Information representing the tabulation of votes at any one of several levels: polling place, precinct, or central count
List of Voters: A listing of the individual voters who have cast ballots in a specific election

2.1.10 Data Retention

All voting systems **shall** provide for maintaining the integrity of voting and audit data during an election and for a period of at least 22 months thereafter consistent with United States Code Title 42, Sections 1974 through 1974e.

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

For 22-month document retention, the general rule is that all printed copy records produced by the election database and ballot processing systems **shall** be so labeled and

archived. Regardless of system type, all audit trail information **shall** be retained in its original format, whether that is 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 vote by mail or provisional ballots, but also time logs of baseline ballot definition formats, and system readiness and testing results.

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

2.2 Pre-voting Capabilities

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

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

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

2.2.1 Ballot Preparation

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

- General capabilities
- Ballot formatting
- Ballot production

2.2.1.1 General Capabilities

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

a. Enabling the automatic formatting of ballots in accordance with the requirements for offices, candidates, and measures qualified to be placed on the ballot for each political subdivision and election district

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

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

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

2.2.1.2 Ballot Formatting

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

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

2.2.1.3 Ballot Production

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

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

a. The electronic display or printed document on which the user views the ballot is capable of rendering an image of the ballot in any of the languages required by the Voting Rights Act of 1965, as amended.
b. The electronic display or printed document on which the user views the ballot does not show any advertising or commercial logos of any kind, whether public service, commercial, or political, unless specifically provided for in state law. Electronic displays **shall** not provide connection to such material through hyperlink.
c. The ballot conforms to manufacturer specifications for type of paper stock, weight, size, shape, size and location of mark field used to record votes, folding, bleed-through, and ink for printing if paper ballot documents or paper displays are part of the system. Manufacturer specifications for type of paper stock **shall** be for a commercially available product. The manufacturer's specifications for type of paper stock may also include reference to a proprietary paper stock product.

Basic Test Methodology

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

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

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

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

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

Manufacturer documentation for marksense systems **shall** include specifications for ballot materials to ensure that vote selections are read from only a single ballot at a time, without detection of marks from multiple ballots concurrently (e.g., reading of bleed through from other ballots).

2.2.2 Election Programming

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

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

2.2.3 Ballot and Program Installation and Control

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

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

2.2.4 Readiness Testing

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

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

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

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

Paper-based systems **shall**:

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

2.2.5 Verification at the Polling Place

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

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

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

h. Confirmation that there are no hardware or software failures

i. Confirmation that the device is ready to be activated for accepting votes

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

2.2.6 Verification at the Central Location

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

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

2.3 Voting Capabilities

All voting systems **shall** support:

- Opening the polls
- Casting a ballot

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

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

2.3.1 Opening the Polls

a. All vote counters must be zeroed before polls are opened. If a device has a nonzero counter or residual votes, this is a failure to activate correctly and thus a device or system failure. Therefore the device **shall** disable itself from use in the voting system and election officials **shall** be advised of the proper corrective action, including
    i. The occurrence **shall** be recorded in the device audit log.
    ii. In addition, a clear, unambiguous warning that an attempt has been made to initiate an election with non-zero totals and that the device has been disabled from the system **shall** be documented and communicated to an election official.

Jurisdictions that allow "early voting" before the nominal election day should note that a distinction is made between the opening and closure of polls, which can occur only once

per election, and the suspension and resumption of voting between days of early voting. The open-polls operation, which requires zeroed counters, is performed only when early voting commences; the resumption of voting that was suspended overnight does not require that counters be zeroed again.

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

2.3.1.1 Precinct Count Systems

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

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

2.3.1.2 Paper-based System Requirements

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

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

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

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

2.3.1.3 DRE System Requirements

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

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

2.3.2 Activating the Ballot

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

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

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

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

2.3.3 Casting a Ballot

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

2.3.3.1 Common Requirements

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

a. Provide text that is at least 3 millimeters high and provide the capability to adjust or magnify the text to an apparent size of 6.3 millimeters
b. Protect the secrecy of the vote such that the system cannot reveal any information about how a particular voter voted, except as otherwise required by state law
c. Record the selection and non-selection of individual vote choices for each contest and ballot measure
d. Record the voter's selection of candidates whose names do not appear on the ballot, as permitted under state law, and
    i. Record as many write-in votes as the number of candidates the voter is allowed to select
e. In the event of a failure of the main power supply external to the voting system, provide the capability for any voter who is voting at the time to complete casting a ballot, allow for the successful shutdown of the voting system without loss or degradation of the voting and audit data, and allow voters to resume voting once the voting system has reverted to back-up power

2.3.3.2 Paper-based System Requirements

All paper-based systems **shall**:

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

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

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

2.3.3.3 DRE and EBM System Requirements

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

a. Prohibit the voter from accessing or viewing any information on the display screen that has not been authorized by election officials and preprogrammed into the voting system (i.e., no potential for display of external information or linking to other information sources)
b. Enable the voter to easily identify the selection button or switch, or the active area of the ballot display, that is associated with each candidate or ballot measure response
c. Allow the voter to select his or her preferences on the ballot in any legal number and combination
d. Indicate that a selection has been made or canceled
e. Indicate to the voter when no selection, or an insufficient number of selections, has been made for a contest (e.g., undervotes)
f. Notify the voter if he or she has attempted to make more than the allowable number of selections for any contest (e.g., overvotes)
g. Provide the voter opportunity to correct the ballot for an undervote before the ballot is cast or printed
h. Notify the voter when the selection of candidates and measures is completed
i. Allow the voter, before the ballot is cast or printed, to review his or her choices and, if the voter desires, to delete or change his or her choices before the ballot is cast or printed
j. Prompt the voter to confirm the voter's choices before casting or printing his or her ballot

k. Provide sufficient computational performance to provide responses back to each voter entry in no more than three seconds
l. Ensure that the votes stored or printed accurately represent the actual votes cast
m. Protect the secrecy of the vote throughout the voting process

In addition, DREs **shall:**

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

2.4 Post-Voting Capabilities

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

2.4.1 Closing the Polls

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

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

2.4.2 Consolidating Vote Data

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

2.4.3 Producing Reports

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

All systems **shall** provide capabilities to:

a. Support geographic reporting, which requires the reporting of all results for each contest at the precinct level and additional jurisdictional levels
    i. Precinct level reporting shall be capable of reporting subcategories broken down by Vote by Mail, Precinct, and All Mail. In the instance of an All Mail precinct, the results shall be accumulated into the Vote by Mail totals.
b. Produce a printed report of the number of ballots counted by each tabulator
c. Produce a printed report for each tabulator of the results of each contest that includes the votes cast for each selection, the count of undervotes, and the count of overvotes
d. Produce a consolidated printed report of the results for each contest of all votes cast (including the count of ballots from other sources supported by the system as specified by the manufacturer) that includes the votes cast for each selection, the count of undervotes, and the count of overvotes
e. Be capable of producing a consolidated printed report of the combination of overvotes for any contest that is selected by an authorized official (e.g., the number of overvotes in a given contest combining candidate A and candidate B, combining candidate A and candidate C, etc.)
f. Produce all system audit information required in the form of printed reports, or in electronic memory for printing centrally
g. Prevent data from being altered or destroyed by report generation

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

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

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

h. Prevent the printing of reports and the unauthorized extraction of data prior to the official close of the polls
i. Provide a means to extract information from a transportable programmable memory device or data storage medium for vote consolidation

j. Consolidate the data contained in each unit into a single report for the polling place when more than one voting machine or precinct tabulator is used
k. Prevent data in transportable memory from being altered or destroyed by report generation

2.4.4 Electronic Reports

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

2.4.4.1 Voting System Electronic Reports

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

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

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

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

2.4.4.2 Tabulator Electronic Reports

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

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

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

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

The tabulator **shall**:

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

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

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

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

a. Time and date at poll closing; and
b. Ballot images recorded in randomized order by the DRE for the election. NIST Special Publication 800-90: Recommendation for Random Number Generation Using Deterministic Random Bit Generators specifies techniques for the generation of random numbers that can be used to randomize the order of ballot images in a cryptographically sound way. For each voted ballot, this includes:

i. Ballot style and reporting context;
ii. For each contest:
    - The choice recorded, including undervotes and write-ins; and
    - Any information collected electronically about each write-in;
iii. Information specifying whether the ballot is provisional, type of provisional ballot, and providing a unique identifier for the ballot. Types of provisional ballots (such as "regular provisional", "extended hours provisional", and "regular extended hours") are jurisdiction-dependent.

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

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

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

2.4.4.3 EMS Electronic Reports

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

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

a. Identifiers for each tabulator contained in the summary;
b. For tabulators with public keys:
    i. The public key for each tabulator in the summary and
    ii. Signed tabulator summary count report.
c. Summary ballot counts and vote totals by tabulator, precinct, and polling place.
    i. Precinct totals include subtotals from each tabulator used in the precinct.
    ii. Precinct totals include subtotals for polling place votes and vote-by-mail votes. Should the precinct be an All-Mail precinct, the totals for the precinct **shall** be listed as vote-by-mail, but should also be reported as an All-Mail precinct.

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

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

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

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

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

2.4.5 Election Night Reporting

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

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

2.5 Maintenance, Transportation, and Storage

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

a. Function without degradation in capabilities after transit to and from the place of use, as demonstrated by meeting the requirements of these ~~Performance~~ Standards.
b. Function without degradation in capabilities after storage between elections~~, as~~ demonstrated by meeting the requirements described these ~~Performance~~ Standards.

2.6 Testing Requirements – Functionality

The S-ATA **shall** design and perform procedures that address:

a. Overall system capabilities
b. Pre-voting functions

c. Voting functions
d. Post-voting functions
e. System maintenance
f. Transportation and storage

The specific procedures to be used **shall** be identified in the Test Plan prepared by the S-ATA. These procedures may replicate testing performed by the manufacturer and documented in the manufacturer's TDP, but **shall** not rely on manufacturer testing as a substitute for independent functionality testing.

Recognizing variations in system design and the technologies employed by different manufacturers, the S-ATA **shall** design test procedures that account for such variations and reflect the system-specific functional capabilities.

The testing of the components and system readiness by the S-ATA **shall** include attempts to initiate an election with non-zero totals on counters or residual ballots, validating that the "zero" report procedure will correctly identify and warn the election officials of the presence of any previously stored results which are in a form that may be deliberately or accidentally processed.

2.6.1 Testing to Reflect Technologies

Voting systems are not designed according to a standard design template. Instead, system design reflects the manufacturer's selections from a variety of technologies and design configurations.

Functional capabilities will vary according to the relative complexity of a system and the manner in which the system integrates various technologies. Therefore, the testing procedure designed and performed for a particular system **shall** reflect the specific technologies and design configurations used by that system.

2.6.2 Testing to Reflect Additional Capabilities

Manufacturers may, and often do, provide additional capabilities in systems in order to respond to the requirements of individual states. These additional capabilities **shall** be identified by the manufacturer within the TDP. Based on this information, the Secretary of State may allow the S-ATA to design and perform system functionality testing for these additional functional capabilities.

2.6.3 Testing to Reflect Previously Tested Capabilities

The required functional capabilities of voting systems reflect a broad range of system functionality needed to support the full life cycle of an election, including post election

activities. Many systems submitted for certification are designed to address this scope, and are to be tested accordingly.

However, some new systems using a combination of new subsystems or system components interfaced with the components of a previously certified system. For example, a manufacturer can submit a voting system certification testing that has a new DRE voting device, but that integrates the election management component from a previously certified system.

In this situation, the manufacturer **shall** identify in the TDP the functional capabilities supported by new subsystems/components and those supported by subsystems/components taken from a previously certified system. The manufacturer **shall** indicate in its system design documentation and configuration management records the scope and nature of any modifications made to the re-used subsystems or components. This will assist the S-ATA to develop efficient test procedures that rely in part on the results of testing of the previously certified subsystems or components.
In this situation the S-ATA may design and perform a test procedure that draws on the results of testing performed previously on re-used subsystems or components. However, irrespective of previous testing performed, the scope of testing **shall** include certain functionality tests:

a. All functionality performed by new subsystems/modules
b. All functionality performed by modified subsystems/modules
c. Functionality that is accomplished using any interfaces to new modules, or that shares inputs or outputs from new modules
d. All functionality related to vote tabulation and election results reporting
e. All functionality related to audit trail maintenance

2.6.4 General Test Sequence

There is no required sequence for performing the system certification tests. For a system not previously certified, the S-ATA may perform tests using generic test ballots, and schedule the tests in a convenient order, provided that prerequisite conditions for each test have been satisfied before the test is initiated.

Regardless of the sequence of testing used, the full certification testing process **shall** include functionality testing for all system functions of a voting system. Generally, in depth functionality testing will follow testing of the system hardware and the source code review of the software. The S-ATA will usually conduct functionality testing as an integral element of the system integration testing.

Some functionality tests for the voting functions may be performed as an integral part of hardware testing, enabling a more efficient testing process. Ballots processed and counted during hardware operating tests for precinct count and central count systems may serve to satisfy part of the functionality testing, provided that the ballots were cast using a test procedure that is equivalent to the procedures indicated below.

2.6.5 Testing in Parallel with Precinct Count Systems

For testing voting functions in parallel with precinct count systems, the following procedures **shall** be performed during the functionality tests of voting equipment and precinct counting equipment.

a. The procedure to prepare election programs **shall**:
    i. Verify resident firmware, if any
    ii. Prepare software (including firmware) to simulate all ballot format and logic options for which the system will be used
    iii. Verify program memory device content
    iv. Obtain and design test ballots with formats and voting patterns sufficient to verify performance of the test election programs
b. The procedures to program precinct ballot counters **shall**:
    i. Install program and data memory devices, or verify presence if resident
    ii. Verify operational status of hardware
c. The procedures to simulate opening of the polls **shall**:
    i. Perform procedures required to prepare hardware for election operations
    ii. Obtain "zero" printout or other evidence that data memory has been cleared
    iii. Verify audit log of pre-election operations
    iv. Perform procedure required to open the polling place and enable ballot counting
d. The procedure to simulate counting ballots **shall** cast test ballots in a number sufficient to demonstrate proper processing, error handling, and generation of audit data
e. The procedure to simulate closing of polls **shall**:
    i. Perform hardware operations required to disable ballot counting and close the polls
    ii. Obtain data reports and verify correctness
    iii. Obtain audit log and verify correctness

These procedures need not be performed in the sequence listed, provided the necessary precondition of each procedure has been met.

2.6.6 Testing in Parallel with Central Count Systems

For testing voting functions in parallel with central count systems, the following procedures **shall** be performed during the functional tests.

a. The procedure to prepare election programs **shall**:
    i. Verify resident firmware, if any
    ii. Prepare software (including firmware) to simulate all ballot format and logic options for which the system will be used, and to enable simulation of counting ballots from at least 10 polling places or precincts
    iii. Verify program memory device content
    iv. Procure test ballots with formats, voting patterns, and format

identifications sufficient to verify performance of the test election programs

b. The procedure to simulate counting ballots **shall** count test ballots in a number sufficient to demonstrate proper processing, error handling, and generation of audit data
c. The procedure to simulate election reports **shall**:
    i. Obtain reports at polling places or precinct level
    ii. Obtain consolidated reports
    iii. Provide query access, if this is a feature of the system
    iv. Verify correctness of all reports and queries
    v. Obtain audit log and verify correctness

These procedures need not be performed in the sequence listed, provided the necessary preconditions of each procedure have been met.

2.6.7 Integration Tests

This subsection addresses the basis for integration testing, the system baseline for testing, and data volumes for testing.

a. Testing Breadth - The S-ATA **shall** design and perform procedures that test the voting system capabilities for the system as a whole. These procedures follow the testing of the systems hardware and software, and address voting system requirements. These procedures **shall** also address the requirements for testing system functionality. The selection of the baseline test cases will follow an operational profile of the common procedures, sequencing, and options among the shared state requirements and those that are specifically recognized and supported by the manufacturer.

   The S-ATA **shall** execute tests that provide coverage of every accessible instruction and branch outcome in application logic and border logic. This is not exhaustive path testing, but testing of paths sufficient to cover every accessible instruction and every accessible branch outcome. There should be no inaccessible code in application logic and border logic other than defensive code (including exception handlers) that is provided to defend against the occurrence of failures and "can't happen" conditions that cannot be reproduced and should not be reproducible by a S-ATA. Full coverage of third-party logic is not mandated because it might include a large amount of code that is never used by the voting application.

   The S-ATA **shall** execute tests that test the interfaces of all application logic and border logic modules and subsystems, and all third-party logic modules and subsystems that are in any way used by application logic or border logic.

   The specific procedures to be used **shall** be identified in the Test Plan. These procedures may replicate testing performed by the manufacturer and

documented in the manufacturer's TDP, but **shall not** rely on manufacturer testing as a substitute for testing performed by the S-ATA.

Recognizing variations in system design and the technologies employed by different manufacturers, the S-ATA **shall** design test procedures that account for these variations.

b. System Baseline for Testing - The system level certification tests are conducted using the version of the system intended to be sold by the manufacturer and delivered to jurisdictions. To ensure that the system version tested is the correct version, the S-ATA **shall** witness the build of the executable version of the system immediately prior to or as part of, the physical configuration audit. Additionally, should components of the system be modified or replaced during the testing process, the S-ATA **shall** require the manufacturer to conduct a new "build" of the system to ensure that the certified executable release of the system is built from tested components.

2.6.7.1 Testing Volume

For all systems, the total number of ballots to be processed by each precinct counting device during these tests **shall** reflect the maximum number of active voting positions and the maximum number of ballot styles that the TDP claims the system can support.

2.6.7.2 Testing Interfaces of System Components

The VSTL **shall** design and perform test procedures that test the interfaces of all system modules and subsystems with each other against the manufacturer's specifications. These tests shall be documented in the Test Plan, and **shall** include the full range of system functionality provided by the manufacturer's specifications, including functionality that exceeds the specific requirements of these Standards.

Some voting systems may use components or subsystems from previously tested and qualified systems, such as ballot preparation. For these scenarios, the S-ATA **shall**, at a minimum:

a. Confirm that the version of previously approved components and subsystems is unchanged
b. Test all interfaces between previously approved modules/subsystems and all other system modules and subsystems. Where a component is expected to interface with several different products, especially from different manufacturers, the manufacturer **shall** provide a public data specification of files or data objects used to exchange information

2.6.7.3 Physical Configuration Audit

The Physical Configuration Audit compares the voting system components submitted for qualification to the manufacturer's technical documentation, and **shall** include the following activities:

a. The audit **shall** establish a configuration baseline of the software and hardware to be tested. It **shall** also confirm whether the manufacturer's documentation is sufficient for the user to install, validate, operate, and maintain the voting system. MIL-STD-1521 can be used as a guide when conducting this audit
b. The S-ATA **shall** examine the manufacturer's source code against the submitted documentation during the Physical Configuration Audit to verify that the software conforms to the manufacturer's specifications. This review **shall** include an inspection of all records of the manufacturer's release control system. If changes have been made to the baseline version, the S-ATA **shall** verify that the manufacturer's engineering and test data are for the software version submitted for certification
c. If the software is to be run on any equipment other than a COTS mainframe data processing system, minicomputer, or microcomputer, the Physical Configuration Audit **shall** also include a review of all drawings, specifications, technical data, and test data associated with the system hardware. This examination **shall** establish the system hardware baseline associated with the software baseline
d. To assess the adequacy of user acceptance test procedures and data, manufacturer documents containing this information **shall** be reviewed against the system's functional specifications. Any discrepancy or inadequacy in the manufacturer's plan or data **shall** be resolved prior to beginning the system integration functional and performance tests
e. All subsequent changes to the baseline software configuration made during the course of testing **shall** be subject to re-examination. All changes to the system hardware that may produce a change in software operation **shall** also be subject to re-examination

The manufacturer **shall** provide a list of all documentation and data to be audited, cross-referenced to the contents of the TDP. Manufacturer technical personnel **shall** be available to assist in the performance of the Physical Configuration Audit.

2.6.7.4 Functional Configuration Audit

The Functional Configuration Audit encompasses an examination of manufacturer tests, and the conduct of additional tests, to verify that the system hardware and software perform all the functions described in the manufacturer's documentation submitted for the TDP. It includes a test of system operations in the sequence in which they would normally be performed, and **shall** include the following activities. MIL-STD-1521 may be used as a guide when conducting this audit:

a. The S-ATA **shall** review the manufacturer's test procedures and test results to determine if the manufacturer's specified functional requirements have been adequately tested. This examination **shall** include an assessment of the adequacy of the manufacturer's test cases and input data to exercise all system functions, and to detect program logic and data processing errors, if such be present
b. The S-ATA **shall** perform or supervise the performance of additional tests to verify nominal system performance in all operating modes, and to verify on a sampling basis the manufacturer's test data reports. If manufacturer developmental test data is incomplete, the S-ATA **shall** design and conduct all appropriate module and integrated functional tests. The functional configuration audit may be performed in the facility of the Secretary of State, the S-ATA or of the manufacturer, with SOS and S-ATA personnel present, and **shall** use and verify the accuracy and completeness of the System Operations, Maintenance, and Diagnostic Testing Manuals

The manufacturer **shall** provide a list of all documentation and data to be audited, cross-referenced to the contents of the TDP. Manufacturer technical personnel **shall** be available to assist in the performance of the Functional Configuration Audit.

3 Usability, Accessibility, and Privacy Requirements

3.1 Purpose

It is essential that:

All eligible voters are to have access to the voting process without discrimination. The voting process must be accessible to individuals with disabilities. The voting process includes access to the polling place, instructions on how to vote, initiating the voting session, selecting among contest choices, review of the ballot, final submission of the ballot, and getting help when needed.

Each cast ballot must accurately capture the selections made by the voter. The ballot must be presented to the voter in a manner that is clear and usable. Voters should encounter no difficulty or confusion regarding the process for recording their votes.

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

3.1.1 Special Terminology

Several uncommon terms are used in this section. For the convenience of the reader, they are defined below. Note in particular the distinctions among these terms: voting process, voting system, voting device, voting session, and voting station.

a. Audio-Tactile Interface (ATI) - a voter interface designed not to require visual reading of a ballot. Audio is used to convey information to the voter and sensitive tactile controls allow the voter to convey information to the voting system.
b. Common Industry Format (CIF) - the format to be used for summative usability test reporting, described in ISO/IEC 25062:2006 "Common Industry Format (CIF) for Usability Test Reports" [ISO06e].
c. Summative Usability Testing - evaluation of a product with representative users and tasks designed to measure the usability (defined as effectiveness, efficiency and satisfaction) of the complete product. The purpose of a summative test is to evaluate a product through defined measures, rather than diagnosis and correction of specific design problems, as in formative testing.
d. Voter-Editable Ballot Device (VEBD) - voting systems such as DREs and EBMs that present voters with an editable ballot (as opposed to manually-marked paper ballots), allowing them easily to change their votes prior to final casting of the ballot.
e. Voting Performance Protocol (VPP) - a carefully defined method for measuring how well subjects perform various voting tasks within a controlled experiment.

3.1.2 Interaction of usability and accessibility requirements

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

a. The requirements for general usability in Section 3.2 apply to ALL voting systems as indicated by their "Applies to" clause, including a VEBD. They cover the features that are applicable both to the general population and to voters with disabilities. Requirements for any alternative languages required by state or federal law are also included under Section 3.2.
b. The requirements for accessibility in Section 3.3 cover only those features that are mandatory for a VEBD in addition to the general usability requirements. For instance, an audio interface would be of interest mainly to those with vision or other reading disabilities, but not to those who can use a visual interface. Therefore, to determine what usability features are required of a VEBD, one must examine both Sections 3.2 and 3.3. The features of a VEBD may also assist those not usually described as having a disability, e.g., voters with poor reading vision or somewhat limited dexterity.

3.2 General Usability Requirements

The voting system should support a process that provides a high level of usability for all voters. The goal is for voters to be able to negotiate the process effectively, efficiently, and comfortably.

3.2.1 Performance Requirements

Usability is defined generally as a measure of the effectiveness, efficiency, and satisfaction achieved by a specified set of users with a given product in the performance of specified tasks. In the context of voting, the primary user is the voter (although the equipment is used by poll workers as well), the product is the voting system, and the primary task is the correct recording of the votes (although other tasks are associated with poll workers as users, e.g. system setup).

Additional requirements for task performance are independence and privacy: the voter should normally be able to complete the voting task without assistance from others, and the votes should be private. Lack of independence or privacy may adversely affect effectiveness (e.g., by possibly inhibiting the voter's free choice) and efficiency (e.g., by slowing down the process).

General usability is covered by both high-level performance-based requirements (in this section) and design requirements (in following sections). Whereas the latter require the presence of specific features generally thought to promote usability, the former directly address metrics for effectiveness (e.g., correct capture of voter selections), efficiency (e.g., time taken to vote), and satisfaction. The voting system is tested by having groups of people (representing voters) attempt to perform various typical voting tasks. The requirement is met only if those tasks are accomplished with a specified degree of success.

3.2.1.1 Overall Performance Metrics

The requirements of this section set benchmarks for the usability of the voting system as a whole. There are three performance requirements that deal with effectiveness and two reporting requirements, one for efficiency and one for satisfaction. The metrics are defined as follows:

a. Total Completion Score – the proportion of users who successfully cast a ballot (whether or not the ballot contains erroneous votes). Failure to cast a ballot might involve problems such as a voter simply "giving up" during the voting session because of an inability to operate the system, or a mistaken belief that one has successfully operated the casting mechanism.
b. Perfect Ballot Index – the ratio of the number of cast ballots containing no erroneous votes to the number of cast ballots containing one or more errors (either a vote for an unintended choice, or a missing vote).
c. Voter Inclusion Index – a measure of both voting accuracy and consistency. It is based on mean accuracy and the associated standard deviation. Accuracy per voter depends on how many "voting opportunities" within each ballot are performed correctly. A low value for the standard deviation of these individual accuracy scores indicates higher consistency of performance across voters.
d. Average Voting Session Time – mean time taken per voter to complete the process of activating, filling out, and casting the ballot.
e. Average Voter Confidence – mean confidence level expressed by the voters that the system successfully recorded their votes.

Because of the statistical nature of the testing, numerical results must be interpreted very carefully. The numbers have meaning only within the context of the Voting Performance Protocol (VPP), a (NIST) approved standard. Note especially that the tests associated with these requirements are designed as repeatable controlled experiments and not as "realistic" measures of voting behavior, as might be found in a wide variety of voting contexts.

a. Total completion performance - The system **shall** achieve a total completion score of at least 98% as measured by the VPP.
b. Perfect ballot performance - The system **shall** achieve a perfect ballot index of at least 2.33 as measured by the VPP.
c. Voter inclusion performance - The system **shall** achieve a voter inclusion index of at least 0.35 as measured by the VPP.

3.2.1.2 Usability Metrics from the Voting Performance Protocol

The S-ATA **shall** report the metrics for usability of the voting system, as measured by the VPP.

a. The test lab **shall** report all the effectiveness metrics for usability as defined and measured by the VPP.
b. The test lab **shall** report the average voting session time, as measured by the VPP.

Note that this requirement does not apply to the audio interface of a system, or to the use of special input devices for voters with dexterity disabilities.

c. The test lab **shall** report the average voter confidence, as measured by the VPP.

3.2.1.3 S-ATA Testing

The S-ATA **shall** conduct summative usability tests on the voting system using individuals who are representative of the general population and **shall** report the test results, using the Common Industry Format.

3.2.2 Functional Capabilities

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

3.2.2.1 Notification of Effect of Overvoting

If the voter attempts to select more than the allowable number of choices within a contest on a VEBD or PCOS, the voting system **shall** notify the voter of the effect of this action before the ballot is cast and counted. In the case of manual systems, overvotes may be mitigated through appropriately placed instructions.

3.2.2.2 Undervoting to be Permitted

The voting system **shall** allow the voter, at the voter's choice, to submit an undervoted ballot without correction.

3.2.2.3 Correction of Ballot

The voting system **shall** provide the voter the opportunity to correct the ballot for either an undervote or overvote before the ballot is cast and counted. In the case of manual systems, the permissibility of casting an undervote or overvote may be explained through appropriately placed written instructions. Some corrections may require the voter to obtain a new paper ballot from a poll worker.

3.2.2.4 Notification of Ballot Casting

If and only if the voter successfully casts the ballot, then a DRE or PCOS system ***SHALL*** so notify the voter.

3.2.2.5 Prevention of overvotes

A VEBD **shall** prevent voters from selecting more than the allowable number of

choices for each contest.

3.2.2.6 Warning of Undervotes

A VEBD **shall** provide feedback to the voter, before final casting of the ballot that identifies specific contests for which the voter has selected fewer than the allowable number of choices (i.e., undervotes). This feature **shall** not be disabled.

3.2.2.7 Independent Correction of Ballot

A VEBD **shall** provide the voter the opportunity to correct the ballot before it is cast and counted. This correction process **shall not** require external assistance. The corrections to be supported include modifying an undervote or overvote, and changing a vote from one candidate to another.

3.2.2.8 Ballot Editing per Contest

A VEBD **shall** allow the voter to change a vote within a contest before advancing to the next contest.

3.2.2.9 Contest Navigation

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

3.2.2.10 Notification of Ballot Casting Failure for a DRE

If the voter takes the appropriate action to cast a ballot, but the system does not accept and record it successfully, including failure to store the ballot image, then the DRE **shall** so notify the voter and provide clear instruction as to the steps the voter should take to cast the ballot. A device that "freezes" when the voter attempts to cast the ballot, providing no evidence one way or the other whether the ballot was cast, violates this requirement.

3.2.3 Non-Editable Interfaces

For non-editable interfaces, such as manually-marked paper ballots (MMPB) certain features are required, especially in the case of precinct-based optical scanners.

3.2.3.1 Notification of Overvoting

The voting system **shall** be capable of providing feedback to the voter that identifies specific contests for which the voter has made more than the allowable number of votes (i.e.,. overvotes).

3.2.3.2 Notification of Undervoting

A PCOS **shall** be capable of providing feedback to the voter that identifies specific contests for which the voter has made fewer than the allowable number of votes (i.e., undervotes). The system **shall** provide a means for an authorized election official to deactivate this capability entirely and by contest.

3.2.3.3 Notification of Blank Ballots

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

3.2.3.4 Ballot Correction or Submission Following Notification

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

3.2.3.5 Handling of Marginal Marks

A marginal mark is one that, according the manufacturer specifications, is neither clearly countable as a vote nor clearly countable as a non-vote.

A PCOS **shall** be able to identify a ballot containing marginal marks. When such a ballot is detected, the tabulator **shall**:

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

3.2.3.6 Notification of Ballot Casting Failure (PCOS)

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

3.2.4 Privacy

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

3.2.4.1 Privacy at the Polls

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

a. Visual privacy - The ballot, any other visible record containing ballot information, and any input controls **shall** be visible only to the voter during the voting session and ballot submission.
b. Auditory privacy - During the voting session, the audio interface of the voting system **shall** be audible only to the voter.
c. Privacy of warnings - The voting system **shall** issue all warnings in a way that preserves the privacy of the voter and the confidentiality of the ballot.
d. No receipts - The voting system **shall not** issue a receipt to the voter that would provide proof to another of how the voter voted.

3.2.4.2 No Recording of Alternative Format Usage

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

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

3.2.5 Cognitive Issues

The features specified in this section are intended to minimize cognitive difficulties for voters.

a. Completeness of instructions - The voting system **shall** provide instructions for all operations inherent to the voting system or that are generated by default. Instructions that are part of a ballot definition are not subject to this requirement.
b. Availability of assistance from the system - The voting system **shall** provide a means for the voter to get help directly from the system at any time during the voting session. However, in case of an equipment failure, the only action available to the voter might be to get assistance from a poll worker.
c. Plain language – Operational instructions and voting system help material **shall** conform to norms and best practices for plain language.
    i. Clarity of warnings - Warnings and alerts issued by the voting system **shall** clearly state:
        - The nature of the problem;
        - Whether the voter has performed or attempted an invalid operation or whether the voting equipment itself has malfunctioned in some way; and
        - The set of responses available to the voter.
    ii. Context before action - When an instruction is based on a condition, the condition **shall** be stated first, and then the action to be performed.
    iii. Start each instruction on a new line - The system **shall** start the visual presentation of each new instruction on a new line.

iv. Use of positive - The system **shall** issue instructions on the correct way to perform actions, rather than telling voters what not to do.
v. Use of imperative voice - The system's instructions **shall** address the voter directly rather than use passive voice constructions.
vi. Gender-based pronouns - The system **shall** avoid the use of gender-based pronouns.

d. No bias among choices - Consistent with the California Elections Code, the voting system **shall** support a process that does not introduce bias for or against any of the contest choices to be presented to the voter. In both visual and aural formats, the choices **shall** be presented in an equivalent manner.
e. Ballot design - The voting system **shall** provide the capability to design a ballot with a high level of clarity and comprehensibility.
   i. Contests split among pages or columns - The voting system **shall** visually present a single contest on a single page or column except where the number of choices in a contest makes it impossible.
   ii. Indicate maximum number of candidates - The voting system **shall** require that the ballot clearly indicate the maximum number of candidates for which one can vote within a single contest.
   iii. Consistent representation of candidate selection - The relationship between the name of a candidate and the mechanism used to vote for that candidate **shall** be consistent throughout the ballot.
f. Conventional use of color - The use of color by the voting system **shall** agree with common conventions: (a) green, blue or white is used for general information or as a normal status indicator; (b) amber or yellow is used to indicate warnings or a marginal status; (c) red is used to indicate error conditions or a problem requiring immediate attention.
g. Icons and language - When an icon is used to convey information, indicate an action, or prompt a response, it **shall** be accompanied by a corresponding linguistic label.

3.2.6 Perceptual Issues

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

a. Screen flicker - No VEBD display screen **shall** flicker with a frequency between 2 Hz and 55 Hz.
b. Resetting of adjustable aspects at end of session - Any aspect of the voting station that is adjustable by the voter or poll worker, including font size, color, contrast, audio volume, or rate of speech, **shall** automatically reset to a standard default value upon completion of that voter's session. For a VEBD, the aspects include synchronized audio/video mode and non-manual input mode.
c. Ability to reset to default values - If any aspect of a voting system is adjustable by the voter or poll worker, there **shall** be a mechanism to reset all such aspects to their default values.
d. Minimum font size - Voting systems **shall** provide a minimum font size of 3.0mm

(measured as the height of a capital letter) for all text intended for voters or poll workers.

e. Available font sizes - A VEBD that uses an electronic image display **shall** be capable of showing all information in at least two font sizes, (a) 3.0-4.0 mm and (b) 6.3-9.0 mm, under control of the voter. The system **shall** allow the voter to adjust font size throughout the voting session while preserving the current votes.
f. Use of font - Text intended for the voter **shall** be presented in the fonts prescribed by California Elections Code Division 13, Chapter 3.
g. Legibility of paper ballots and verification records - Voting systems using paper ballots or paper verification records **shall** provide features that assist in the reading of such ballots and records by voters with poor reading vision. The system **may** achieve legibility of paper records by supporting magnification of those records. This magnification **may** be done by optical or electronic devices. The manufacturer **may** either: 1) provide the magnifier itself as part of the system, or 2) provide the make and model number of readily available magnifiers that are compatible with the system.
h. Contrast Ratio - The minimum figure-to-ground ambient contrast ratio for all text and informational graphics (including icons) intended for voters or poll workers **shall** be 3:1.
i. High contrast for electronic displays - A VEBD **shall** be capable of showing all information in high contrast either by default or under the control of the voter. The system **shall** allow the voter to adjust contrast throughout the voting session while preserving the current votes. High contrast is a figure-to-ground ambient contrast ratio for text and informational graphics of at least 6:1.
j. Accommodation for color blindness - The default color coding **shall** support correct perception by voters with color blindness.
k. No reliance solely on color - Color coding **shall not** be used as the sole means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.

3.2.7 Interaction Issues

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

a. No page scrolling - Voting systems **shall not** require page scrolling by the voter.
b. Unambiguous feedback for voter's selection - The voting system **shall** provide unambiguous feedback regarding the voter's selection, such as displaying a checkmark beside the selected option or conspicuously changing its appearance.
c. Accidental Activation - The location and sensitivity of the input mechanisms **shall** be designed to minimize accidental activation.
    i. Size and separation of touch areas - On touch screens, the sensitive touch areas **shall** have a minimum height of 0.5 inches and minimum width of 0.7 inches. The vertical distance between the centers of adjacent areas **shall** be at least 0.6 inches, and the horizontal distance at least 0.8 inches.
    ii. No repeating keys - No key or control on a voting system **shall** have a repetitive effect as a result of being held in its active position.

3.2.8 Timing Issues

This section uses the following terms:

- Initial system response time**:** the time taken from when the voter performs some detectible action (such as pressing a button) to when the voting system *begins* responding in some obvious way (such as an audible response or any change on the screen).
- Completed system response time**:** the time taken from when the voter performs some detectible action to when the voting system completes its response and settles into a stable state (e.g., finishes "painting" the screen with a new page).
- Voter inactivity time**:** the amount of time from when the system completes its response until there is detectible voter activity. In particular, note that audio prompts from the system may take several minutes and that this time does not count as voter inactivity.
- Alert time**:** the amount of time the equipment will wait for detectible voter activity after issuing an alert before going into an inactive state requiring poll worker intervention.

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

a. Maximum initial system response time - The initial system response time of a VEBD **shall** be no greater than 0.5 seconds.
b. Maximum completed system response time for vote confirmation - When the voter performs an action to record a single vote, the completed system response time of the VEBD **shall** be no greater than one second in the case of a visual response, and no greater than five seconds in the case of an audio response.
c. Maximum completed system response time for all operations - The completed system response time of a VEBD for visual operations **shall** be no greater than 10 seconds.
d. System response indicator - If a VEBD has not completed its visual response within one second, it **shall** present to the voter, within 0.5 seconds of the voter's action, some indication that it is preparing its response.
e. Voter inactivity time - The VEBD **shall** detect and warn about lengthy voter inactivity during a voting session. Each system **shall** have a defined and documented voter inactivity time, and that time **shall** be between two and five minutes.
f. Alert time - Upon expiration of the voter inactivity time, the voting system **shall** issue an alert and provide a means by which the voter may receive additional time. The alert time **shall** be between 20 and 45 seconds. If the voter does not respond to the alert within the alert time, the system **shall** go into an inactive state requiring poll worker intervention.

3.2.9 Alternative Languages

HAVA Section 301 (a)(4) states that the voting system shall provide alternative language accessibility pursuant to the requirements of Section 203 of the Voting Rights Act of 1965 (42 U.S.C. 1973aa-1a). Elections Code section 19101(b)(5) requires a voting system to be accessible to voters who require assistance in a language other than

English if the language is one in which a ballot or ballot materials are required to be made available to voters pursuant to section 14201 and applicable federal laws, i.e., Section 203 of the federal Voting Rights Act. Thus, each election officials must ensure that the voting system deployed is capable of handling the languages meeting the state and federal legal thresholds that apply within the elections official's jurisdiction.

a. General support for alternative languages - The voting system **shall** be capable of presenting the ballot, contest choices, review screens, vote verification records, and voting instructions in any language that Elections Code section 14201 or the Section 203 of the federal Voting Rights Act requires in any California jurisdiction.
    i. Voter control of language - A VEBD **shall** allow the voter to select among the available languages throughout the voting session while preserving the current votes.
    ii. Complete information in alternative language - Information presented to the voter in the typical case of English-literate voters (including instructions, warnings, messages, contest choices, and vote verification information) **shall** also be presented when an alternative language is being used, whether the language is written or spoken.
    iii. Auditability of records for English readers - Any records, including paper ballots and paper verification records, **shall** have sufficient information to support auditing by poll workers and others who can read only English.
    iv. Usability testing by S-ATA for alternative languages - The S-ATA **shall** conduct summative usability tests for each of the system's supported languages, using subjects who are fluent in those languages but not fluent in English and **shall** report the test results, using the Common Industry Format.

3.2.10 Usability for Poll Workers

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

3.2.10.1 Operation

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

- Setup includes all the steps necessary to take the system from its state as normally delivered to the polling place, to the state in which it is ready to record votes. It does not include ballot definition.
- Polling includes such functions as:
    - voter identification and authorization;
    - preparing the system for the next voter;
    - assistance to voters who wish to change their ballots or need other help;

- system recovery in the case of voters who abandon the voting session without having cast a ballot; and
- routine hardware operations, such as installing a new roll of paper.

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

a. Ease of normal operation - The procedures for system setup, polling, and shutdown, as documented by the manufacturer, **shall** be reasonably easy for the typical poll worker to learn, understand, and perform. This requirement does not apply to inherently complex operations such as ballot definition or system repair.
b. Documentation usability - The system **shall** include clear, complete, and detailed instructions and messages for setup, polling, and shutdown. This requirement does not apply to inherently complex operations such as ballot definition.
    i. Poll Workers as target audience - The documentation required for normal system operation **shall** be presented at a level appropriate for non-expert poll workers.
    ii. Usability at the polling place - The documentation **shall** be in a format suitable for practical use in the polling place rather than a single large reference manual that simply presents
    iii. Enabling verification of correct operation - The instructions and messages **shall** enable the poll worker to verify that the system
        - Has been set up correctly (setup);
        - Is in correct working order to record votes (polling); and
        - Has been shut down correctly (shutdown).

3.2.10.2 Safety

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

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

3.3 Accessibility Requirements

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

ACCESSIBILITY FOR INDIVIDUALS WITH DISABILITIES.--The voting system shall--

(A) be accessible for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters;

(B) satisfy the requirement of subparagraph (A) through the use of at least one direct recording electronic voting system or other voting system equipped for

individuals with disabilities at each polling place;

The voting process is to be accessible to voters with disabilities through the use of a specially equipped voting station.

The requirements in this section are intended to address this HAVA mandate. Ideally, every voter would be able to vote independently and privately. As a practical matter, there may be some number of voters who, because of the nature of their disabilities, will need personal assistance with any system. Nonetheless, these requirements are meant to make the voting system independently accessible to as many voters as possible.

This section is organized according to the type of disability being addressed. For each type, certain appropriate design features are specified. Note, however, that a feature intended primarily to address one kind of disability may very well assist voters with other kinds.

3.3.1 General

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

a. Accessibility throughout the voting session - A VEBD **shall** be integrated into the manufacturer's complete voting system so as to support accessibility for disabled voters throughout the voting session.
    i. Documentation of Accessibility Procedures - The manufacturer **shall** supply documentation describing:
        - recommended procedures that fully implement accessibility for voters with disabilities; and
        - how a VEBD supports those procedures.
b. Complete information in alternative formats - When the provision of accessibility involves an alternative format for ballot presentation, then all information presented to non-disabled voters, including instructions, warnings, error and other messages, and contest choices, **shall** be presented in that alternative format.
c. No dependence on personal assistive technology - The support provided to voters with disabilities **shall** be intrinsic to the accessible voting station. It **shall not** be necessary for the accessible voting station to be connected to any personal assistive device of the voter in order for the voter to operate it correctly.
d. Secondary means of voter identification - If a voting system provides for voter identification or authentication by using biometric measures that require a voter to possess particular biological characteristics, then the system **shall** provide a secondary means that does not depend on those characteristics.
e. Accessibility of paper-based vote verification - If a VEBD generates a paper record (or some other durable, human-readable record) for the purpose of allowing voters to verify their votes, then the system **shall** provide a means to ensure that the verification record is accessible to all voters with disabilities.
    i. Audio readback for paper-based vote verification - If a VEBD generates a paper record (or some other durable, human-readable record) for the purpose

of allowing voters to verify their votes, then the system **shall** provide a mechanism that can read that record and generate an audio representation of its contents.

3.3.2 Low vision

These requirements specify the features of the accessible voting station designed to assist voters with low vision.

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

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

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

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

a. Usability testing by S-ATA for voters with low vision - The S-ATA **shall** conduct summative usability tests on the voting system using individuals with low vision and **shall** report the test results, using the Common Industry Format.
b. Adjustable saturation for color displays - An accessible voting station with a color electronic image display **shall** allow the voter to adjust the color saturation throughout the voting session while preserving the current votes. At least two options **shall** be available: a high and a low saturation presentation.
c. Distinctive buttons and controls - Buttons and controls on accessible voting stations **shall** be distinguishable by both shape and color. This applies to buttons and controls implemented either "on-screen" or in hardware. This requirement does not apply to sizeable groups of keys, such as a conventional 4x3 telephone keypad or a full alphabetic keyboard.
d. Synchronized audio and video - The voting station **shall** provide synchronized audio output to convey the same information as that which is displayed on the screen. There **shall** be a means by which the voter can disable either the audio or the video output, resulting in a video-only or audio-only presentation, respectively. The system **shall** allow the voter to switch among the three modes (synchronized audio/video, video-only, or audio-only) throughout the voting session while preserving the current votes.

3.3.3 Blindness

These requirements specify the features of the accessible voting station designed to assist voters who are blind.

a. Usability testing by S-ATA for blind voters - The S-ATA **shall** conduct summative usability tests on the voting system using individuals who are blind and **shall** report the test results, using the Common Industry Format.
b. Audio-tactile interface - The accessible voting station **shall** provide an audio-tactile interface (ATI) that supports the full functionality of the visual ballot interface. Full functionality includes at a minimum:
    - Instructions and feedback on initial activation of the ballot (such as insertion of a smart card), if applicable;
    - Instructions and feedback to the voter on how to operate the accessible voting station, including settings and options (e.g., volume control, repetition);
    - Instructions and feedback for navigation of the ballot;
    - Instructions and feedback for contest choices, including write-in candidates;
    - Instructions and feedback on confirming and changing votes; and
    - Instructions and feedback on final submission of ballot.

    i. Equivalent functionality of ATI - The ATI of the accessible voting station **shall** provide the same capabilities to vote and cast a ballot as are provided by its visual interface.
    ii. ATI supports repetition - The ATI **shall** allow the voter to have any information provided by the voting system repeated.
    iii. ATI supports pause and resume - The ATI **shall** allow the voter to pause and resume the audio presentation.
    iv. ATI supports transition to next or previous contest - The ATI **shall** allow the voter to skip to the next contest or return to previous contests.
    v. ATI can skip initiative or referendum wording - The ATI **shall** allow the voter to skip over the reading of an initiative or referendum so as to be able to vote on it immediately.
c. Audio features and characteristics - Voting stations that provide audio presentation of the ballot **shall** do so in a usable way, as detailed in the following sub-requirements.
    i. Standard connector - The ATI **shall** provide its audio signal through an industry standard connector for private listening using a 3.5mm stereo headphone jack to allow voters to use their own audio assistive devices.
    ii. T-Coil coupling - When a voting system utilizes a telephone style handset or headphone to provide audio information, it **shall** provide a wireless T-Coil coupling for assistive hearing devices so as to provide access to that information for voters with partial hearing. That coupling **shall** achieve at least a category T4 rating as defined by [ANSI01] American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19.
    iii. Sanitized headphone or handset - A sanitized headphone or handset **shall** be made available to each voter. This requirement can be achieved in

various ways, including the use of "throwaway" headphones, or of sanitary coverings.

iv. Initial volume - The voting system **shall** set the initial volume for each voting session between 40 and 50 dB SPL.

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

vi. Range of frequency - The audio system **shall** be able to reproduce frequencies over the audible speech range of 315 Hz to 10 KHz.

vii. Intelligible audio - The audio presentation of verbal information by both recorded and synthetic speech **shall** be readily comprehensible by voters who have normal hearing and are proficient in the language. This includes such characteristics as proper enunciation, normal intonation, appropriate rate of speech, and low background noise. Candidate names **shall** be pronounced as the candidate intends. This requirement applies to those aspects of the audio content that are inherent to the voting system or that are generated by default.

viii. Control of speed - The audio system **shall** allow the voter to control the rate of speech throughout the voting session while preserving the current votes. The range of speeds supported **shall** include 75% to 200% of the nominal rate.

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

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

f. Tactile discernability of controls - Mechanically operated controls or keys on an accessible voting station **shall** be tactilely discernible without activating those controls or keys.

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

3.3.4 Dexterity

These requirements specify the features of the accessible voting station designed to assist voters who lack fine motor control or use of their hands.

a. Usability testing by S-ATA for voters with dexterity disabilities - The S-ATA **shall** conduct summative usability tests on the voting system using individuals lacking fine motor control and **shall** report the test results, using the Common Industry Format.

b. Support for non-manual input - The accessible voting station **shall** provide a mechanism to enable non-manual input that is functionally equivalent to tactile input. All the functionality of the accessible voting station (e.g., straight party

voting, write-in candidates) that is available through the conventional forms of input, such as tactile, **shall** also be available through non-manual input mechanisms such as mouth sticks and "sip and puff" switches.

c. Ballot submission and vote verification - If the voting station supports ballot submission or vote verification for non-disabled voters, then it **shall** also provide features that enable voters who lack fine motor control or the use of their hands to perform these actions.
d. Manipulability of controls - Keys and controls on the accessible voting station **shall** be operable with one hand and **shall not** require tight grasping, pinching, or twisting of the wrist. The force required to activate controls and keys **shall** be no greater 5 lbs. (22.2 N).
e. No dependence on direct bodily contact - The accessible voting station controls **shall not** require direct bodily contact or for the body to be part of any electrical circuit.

3.3.5 Mobility

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

a. Clear floor space - The accessible voting station **shall** provide a clear floor space of 30 inches (760 mm) minimum by 48 inches (1220 mm) minimum for a stationary mobility aid. The clear floor space **shall** be level with no slope exceeding 1:48 and positioned for a forward approach or a parallel approach.
b. Allowance for assistant - When deployed according to the installation instructions provided by the manufacturer, the voting station **shall** allow adequate room for an assistant to the voter. This includes clearance for entry to and exit from the area of the voting station.
c. Visibility of displays and controls - Labels, displays, controls, keys, audio jacks, and any other part of the accessible voting station necessary for the voter to operate the voting system **shall** be easily legible and visible to a voter in a wheelchair with normal eyesight (no worse than 20/40, corrected) who is in an appropriate position and orientation with respect to the accessible voting station.

3.3.5.1 Controls within reach

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

a. Forward approach, no obstruction - If the accessible voting station has a forward approach with no forward reach obstruction then the high reach **shall** be 48 inches maximum and the low reach **shall** be 15 inches minimum.
b. Forward approach, with obstruction - If the accessible voting station has a

forward approach with a forward reach obstruction, the following sub-requirements **shall** apply .

i. Maximum size of obstruction - The forward obstruction **shall** be no greater than 25 inches in depth, its top no higher than 34 inches and its bottom surface no lower than 27 inches.

ii. Maximum high reach over obstruction - If the obstruction is no more than 20 inches in depth, then the maximum high reach **shall** be 48 inches, otherwise it **shall** be 44 inches.

iii. Toe clearance under obstruction - Space under the obstruction between the finish floor or ground and 9 inches (230 mm) above the finish floor or ground **shall** be considered toe clearance and **shall** comply with the following provisions:

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

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

- Knee clearance depth **shall** extend 25 inches (635 mm) maximum under the obstruction at 9 inches (230 mm) above the finish floor or ground;
- The minimum knee clearance depth at 9 inches (230 mm) above the finish floor or ground **shall** be either 11 inches (280 mm) or 6 inches less than the toe clearance, whichever is greater;
- Between 9 inches (230 mm) and 27 inches (685 mm) above the finish floor or ground, the knee clearance depth **shall** be permitted to reduce at a rate of 1 inch (25 mm) in depth for each 6 inches (150 mm) in height. (It follows that the minimum knee clearance at 27 inches above the finish floor or ground **shall** be 3 inches less than the minimum knee clearance at 9 inches above the floor.); and
- Knee clearance width **shall** be 30 inches (760 mm) minimum.

c. Parallel approach, no obstruction - If the accessible voting station has a parallel approach with no side reach obstruction then the maximum high reach **shall** be 48 inches and the minimum low reach **shall** be 15 inches.

d. Parallel approach, with obstruction - If the accessible voting station has a parallel approach with a side reach obstruction, the following sub-requirements **shall** apply.

i. Maximum size of obstruction - The side obstruction for a VEBD **shall** be no greater than 24 inches in depth and its top no higher than 34 inches.

ii. Maximum high reach over obstruction - If the obstruction is no more than 10 inches in depth, then the maximum high reach **shall** be 48 inches, otherwise it **shall** be 46 inches.

Table 3-1 Unobstructed reach measurements

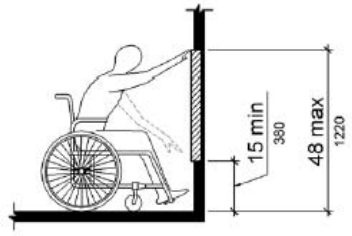

Figure 3-1
Unobstructed forward reach

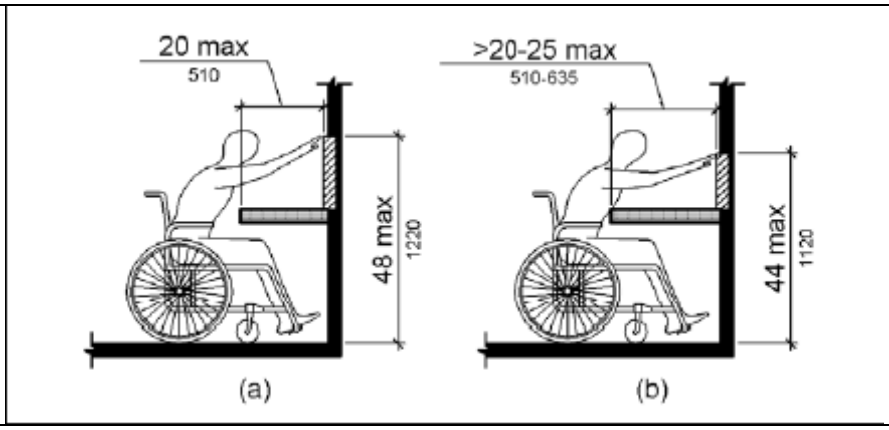

Figure 3-2
Obstructed forward reach
(a) for an obstruction depth of up to 20 inches (508 mm)
(b) for an obstruction depth of up to 25 inches (635 mm)

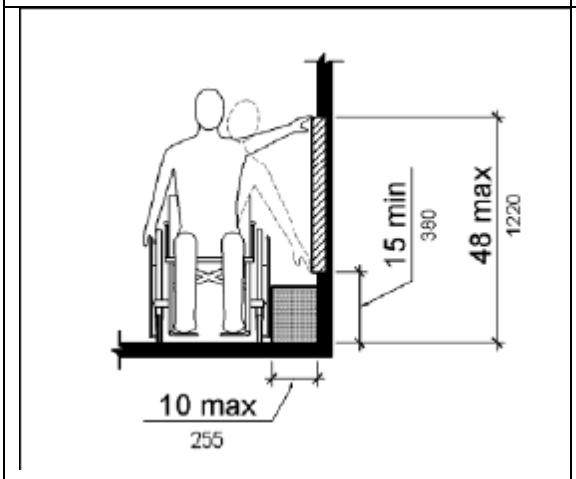

Figure 3-3
Unobstructed side reach with an allowable obstruction less than 10 inches (254 mm) deep

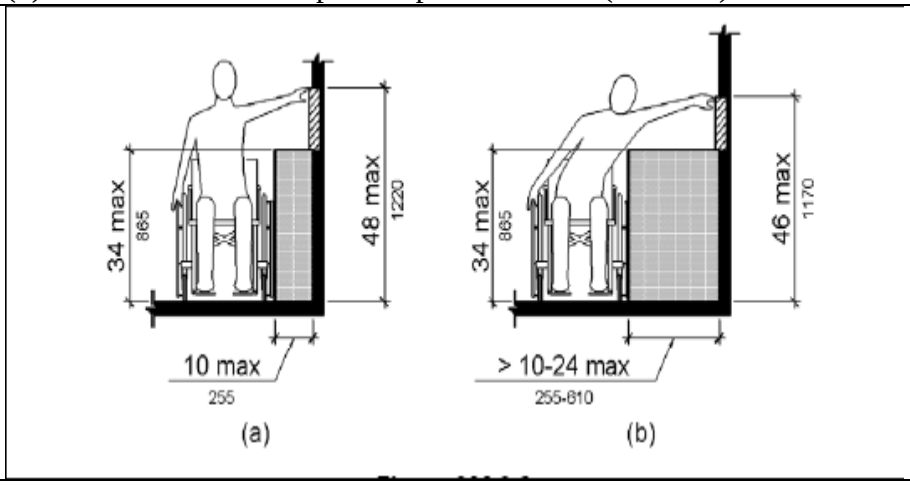

Figure 3-4
Obstructed side reach
(a) for an obstruction depth of up to 10 inches (254 mm)
(b) for an obstruction depth of up to 24 inches (610 mm)

3.3.6 Hearing

These requirements specify the features of the accessible voting station designed to assist voters with hearing disabilities.

a. Reference to audio requirements - The accessible voting station **shall** incorporate the features listed under the requirements for voting equipment that provides audio presentation of the ballot.
b. Visual redundancy for sound cues - If the voting system provides sound cues as a method to alert the voter, the tone **shall** be accompanied by a visual cue, unless the station is in audio-only mode.

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

3.3.7 English Proficiency

These requirements specify the features of the accessible voting station designed to assist voters who lack proficiency in reading English.

Use of ATI- For voters who lack proficiency in reading English, the voting equipment **shall** provide an audio interface for instructions and ballots.

3.3.8 Speech

Speech not to be required by equipment - Voting equipment **shall not** require voter speech for its operation.

4 Hardware Requirements

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

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

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

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

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

The requirements presented in this section are organized as follows:

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

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

Design, Construction, and Maintenance Requirements: These requirements address the reliability and durability of materials, product marking, quality of system workmanship, safety, and other attributes to ensure smooth system operation in the voting environment

Hardware Test Requirements: All equipment used in a voting system **shall** undergo functional, operational and non-operational testing with the exception of the following:

a. Commercially available models of general purpose information technology equipment that have been designed to an ANSI or IEEE standard, have a documented history of successful performance for relevant requirements of the standards, and have demonstrated compatibility with the voting system components with which they interface.
b. Production models of special purpose information technology equipment that have a documented history of successful performance under conditions equivalent to election use for relevant requirements of the standards and that have demonstrated compatibility with the voting system components with which they interface.
c. Any ancillary devices that do not perform ballot definition, election database maintenance, ballot reading, ballot data processing, or the production of an official output report; and that do not interact with these system functions (e.g. printers used to generate unofficial reports, or CRTs used to monitor the vote counting process).

The equipment in subsections a through c **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.

4.1 Performance Requirements

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

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

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

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

4.1.1 Accuracy Requirements

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

a. All systems **shall** achieve a report total error rate of no more than one in 125,000 (8×10^{-6}).
b. Given a set of vote data reports, the observed cumulative report total error rate **shall** be calculated as follows:
    i. Define a "report item" as any one of the numeric values (totals or counts) that must appear in any of the vote data reports. Each ballot count, each vote, overvote, and undervote total for each contest, and each vote total for each contest choice in each contest is a separate report item. The required report items are detailed in Chapters 2 and 4.
    ii. For each report item, compute the "report item error" as the absolute value of the difference between the correct value and the reported value. Special cases: If a value is reported that should not have appeared at all (spurious item), or if an item that should have appeared in the report does not (missing item), assess a report item error of one. Additional values that are reported as a manufacturer extension to the standard are not considered spurious items.
    iii. Compute the "report total error" as the sum of all of the report item errors from all of the reports.
    iv. Compute the "report total volume" as the sum of all of the correct values for all of the report items that are supposed to appear in the reports. Special cases: When the same logical contest appears multiple times, e.g. when results are reported for each ballot configuration and then combined or when reports are generated for multiple reporting contexts, each manifestation of the logical contest is considered a separate contest with its own correct vote totals in this computation.
    v. Compute the observed cumulative report total error rate as the ratio of the report total error to the report total volume. Special cases: If both values are zero, the report total error rate is zero. If the report total volume is zero but the report total error is not, the report total error rate is infinite.

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

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

4.1.2 Environmental Requirements

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

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

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

4.1.2.1 Shelter Requirements

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

4.1.2.2 Space Requirements

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

4.1.2.3 Furnishings and Fixtures

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

4.1.2.4 Electrical Supply

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

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

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

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

d. The alert to the user that the system has lost power and is shutting down (systematic) or needs to be shut down (user intervention) should be easily recognizable and documentation should be provided to illustrate the proper course of action that needs to be taken.
e. All ballots **shall** reside in either the input or output hopper with no ballots in process at the end of the shutdown process.
f. All ballots in the output hopper **shall** be fully read and saved.

g. All actions taken by the system or the user to initiate the shut down are considered "events" and **shall** be logged per Requirements 2.1.4 g & i.
h. A report, including the final state of all ballots, timestamps and of the final state of the unit, **shall** be printed or saved in a file. The report **shall** be part of the permanent election record and **shall** be available when power is restored to the system.
i. The system **shall** be capable of resuming operation from the point it stopped once power is restored.

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

4.1.2.5 Electrical Power Disturbance

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

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

4.1.2.6 Electrical Fast Transient

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

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

4.1.2.7 Lightning Surge

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

a. ±2 kV AC line to line
b. ±2 kV AC line to earth
c. + or – 0.5 kV DC line to line >10m

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

4.1.2.8 Electrostatic Disruption

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

4.1.2.9 Electromagnetic Emissions

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

4.1.2.10 Electromagnetic Susceptibility

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

4.1.2.11 Conducted RF Immunity

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

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

4.1.2.12 Magnetic Fields Immunity

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

4.1.2.13 Environmental Control - Operating Environment

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

required range, the system **shall** be tested to the level of humidity asserted in the documentation.

4.1.2.14 Environmental Control - Transit and Storage

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

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

4.1.2.15 Data Network Requirements

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

4.1.3 Election Management System Requirements

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

4.1.3.1 Recording Requirements

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

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

a. Record every entry made by the user
b. Add permissible voter selections correctly to the memory components of the device
c. Verify the correctness of detection of the user selections and the addition of the selections correctly to memory
d. Add various forms of data entered directly by the election official or designee, such as text, line art, logos, and images
e. Verify the correctness of detection of data entered directly by the user and the addition of the selections correctly to memory

f. Preserve the integrity of election management data stored in memory against corruption by stray electromagnetic emissions, and internally generated spurious electrical signals
g. Log corrected data errors by the voting system

4.1.3.2 Memory Stability

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

4.1.4 Vote Recording Requirements

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

4.1.4.1 Common Requirements

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

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

4.1.4.2 Paper-based Recording Requirements

The paper-based recording requirements govern:

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

a. Paper ballots used by paper-based voting systems **shall** meet the following standards:
    i. Marks that identify the unique ballot format **shall** be outside the area in which votes are recorded, so as to minimize the likelihood that these marks will be mistaken for vote responses and the likelihood that recorded votes will obliterate these marks
    ii. If printed alignment marks are used to locate the vote response fields on the ballot, these marks **shall** be outside the area in which votes are recorded, so as to minimize the likelihood that these marks will be mistaken for vote responses and the likelihood that recorded votes will obliterate these marks

iii. The Technical Data Package **shall** specify the required paper stock, size, shape, opacity, color, watermarks, field layout, orientation, size and style of printing, size and location of mark fields used for vote response fields and to identify unique ballot formats, placement of alignment marks, ink for printing, and folding and bleed-through limitations for preparation of ballots that are compatible with the system

b. The Technical Data Package **shall** specify marking devices, which, if used to make the prescribed form of mark, produce readable marked ballots such that the system meets the performance requirements for accuracy. Marking devices can be either manual (such as pens or pencils) or electronic. These specifications **shall** identify:
   i. Specific characteristics of marking devices that affect readability of marked ballots
   ii. Performance capabilities with regard to each characteristic
   iii. For marking devices manufactured by multiple external sources, a listing of sources and model numbers that are compatible with the system
c. A frame or fixture for printed ballots is optional. However, if such a device is provided, it **shall**:
   i. Be of any size and shape consistent with its intended use
   ii. Position the card properly
   iii. Hold the ballot securely in its proper location and orientation for voting
   iv. Comply with the requirements for design and construction
d. Ballot boxes and ballot transfer boxes, which serve as secure containers for the storage and transportation of voted ballots, shall:
   i. Be of any size, shape, and weight commensurate with their intended use
   ii. Incorporate locks or seals, the specifications of which are described in the system documentation
   iii. Provide specific points where ballots are inserted, with all other points on the box constructed in a manner that prevents ballot insertion
   iv. For precinct count systems, contain separate compartments for the segregation of unread ballots, ballots containing write-in votes or any irregularities that may require special handling or processing.

4.1.4.3 DRE System Recording Requirements

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

a. DRE systems shall include an audible or visible activity indicator providing the status of each voting device. This indicator **shall**:
   i. Indicate whether the device has been activated for voting
   ii. Indicate whether the device is in use
b. To ensure vote recording accuracy and integrity while protecting the anonymity of the voter, all DRE systems **shall**:
   i. Contain all mechanical, electromechanical, and electronic components; software; and controls required to detect and record the activation of selections made by the voter in the process of voting and casting a ballot

ii. Incorporate redundant memories to detect and allow correction of errors caused by the failure of any of the individual memories
iii. Provide at least two processes that record the voter's selections that:
    - To the extent possible, are isolated from each other
    - Designate one process and associated storage location as the main vote detection, interpretation, processing and reporting path
iv. Use a different process to store ballot images, for which the method of recording may include any appropriate encoding or data compression procedure consistent with the regeneration of an unequivocal record of the ballot as cast by the voter
v. Provide a capability to retrieve ballot images in a form readable by humans
vi. Ensure that all processing and storage protects the anonymity of the voter

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

4.1.5 Paper-based Conversion Requirements

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

4.1.5.1 Ballot Handling

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

a. The capacity to convert the marks on individual ballots into signals is uniquely important to central count systems. The capacity for a central count system **shall** be documented by the manufacturer. This documentation **shall** include the capacity for individual components that impact the overall capacity

b. When ballots are unreadable or some condition is detected requiring that the ballots be segregated from normally processed ballots for human review (e.g. write-ins), all central count paper-based systems **shall** do one of the following:
    i. Outstack the ballot
    ii. Stop the ballot reader and display a message prompting the election official or designee to remove the ballot
    iii. Mark the ballot with an identifying mark to facilitate its later identification
c. Additionally, the system **shall** provide a capability that can be activated by an authorized election official to identify ballots containing overvotes, blank ballots, and ballots containing undervotes in a designated contest. If enabled, these capabilities **shall** perform one of the above actions in response to the indicated condition.
d. When ballots are unreadable or when some condition is detected requiring that the ballots be segregated from normally processed ballots for human review (e.g. write-in votes) all precinct count systems **shall**:
    i. In response to an unreadable or blank ballot, return the ballot and provide a message prompting the voter to examine the ballot
    ii. In response to a ballot with a write-in vote, segregate the ballot or mark the ballot with an identifying mark to facilitate its later identification
    iii. In response to a ballot with an overvote the system **shall**:
        - Provide a capability to identify an overvoted ballot
        - Return the ballot
        - Provide an indication prompting the voter to examine the ballot
        - Allow the voter to correct the ballot
        - Provide a means for an authorized election official to deactivate this capability entirely and by contest
    iv. In response to a ballot with an undervote, the system **shall**:
        - Provide a capability to identify an undervoted ballot
        - Return the ballot
        - Provide an indication prompting the voter to examine the ballot
        - Allow the voter to correct the ballot
        - Allow the voter to submit the ballot with the undervote
        - Provide a means for an authorized election official to deactivate this capability
e. Ballot readers **shall** prevent multiple feed or detect and provide an alarm indicating multiple feed. Multiple feed occurs when a ballot reader attempts to read more than one ballot at a time.
    i. If multiple feed is detected, the ballot reader **shall** halt in a manner that permits the operator to remove the unread ballots causing the error, and reinsert them in the input hopper

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

f. All paper-based tabulators and EBMs **shall** achieve a misfeed rate of no more than 0.002 (1⁄500).

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

4.1.5.2 Ballot Reading Accuracy

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

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

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

a. Detect marks that conform to manufacturer specifications with an error rate that enables satisfaction of the system-level accuracy requirement
b. Ignore, and not record, extraneous perforations, smudges, and folds

4.1.6 Tabulation Processing Requirements

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

4.1.6.1 Paper-based System Processing Requirements

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

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

4.1.6.2 DRE System Processing Requirements

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

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

4.1.7 Reporting Requirements

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

4.1.7.1 Removable Storage Media

In voting systems that use storage media that can be removed from the system and transported to another location for readout and report generation, these media **shall** use devices with demonstrated error-free retention for a period of 22 months under the environmental conditions for operation and non-operation.

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

4.1.7.2 Printers

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

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

4.1.8 Vote Data Management Requirements

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

These capabilities allow the system to:

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

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

4.1.8.1 Data File Management

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

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

4.1.8.2 Data Report Generation

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

4.2 Physical Characteristics

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

4.2.1 Size

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

4.2.2 Weight

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

4.2.3 Transport and Storage of Precinct Systems

All precinct voting systems **shall**:

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

4.3 Design, Construction, and Maintenance Characteristics

This subsection covers voting system materials, construction workmanship, and specific design characteristics important to the successful operation and efficient maintenance of the voting system. Three terms introduced in this section and their definitions are provided below.

- **Critical failure**: Functional failure the occurrence of which jeopardizes the validity of the election or casts doubt on the credibility of the election result.
- **Non-user-serviceable failure**: Functional failure that requires the manufacturer or highly trained personnel to repair.
- **User-serviceable failure**: Functional failure that can be remedied by a troubleshooter and/or election official using only knowledge found in voting equipment user documentation.

4.3.1 Materials, Processes, and Parts

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

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

All voting systems **shall**:

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

4.3.2 Durability

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

4.3.3 Reliability

This section covers the requirements for failure rates for voting system components. Before the requirements there are two informative sections that cover use cases and the basis for the requirements.

4.3.3.2 Use Case (Informative)

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

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

4.3.3.3 Basis of Requirements (Informative)

Manufacturers are required to apply best practices to assure reliability. In the manufacturer's reliability analysis, each specific, individual, identified failure mode would be assigned a probability, and the system probability of failure would then be derived mathematically. As a trivial example, if a device has only two failure modes, each has probability 0.01 of occurring, and they are independent of one another, the probability of failure is $1 - 0.99^2 = 0.0199$. Since the underlying probabilities are likely to depend on the volume that a device is expected to handle in the course of the election, minimum values for the assumed volume per device per election~~, from Table 6-1~~ are specified in a requirement.

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

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

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

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

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

4.3.3.4 Requirements

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

Device class	Probability of critical failure (F_C)	Probability of critical or non-user-serviceable failure ($F_C \cup F_N$)	Probability of Failure ($F_C \cup F_N \cup F_S$)
EMS	$\leq 10^{-6}$	$\leq 10^{-6}$	≤ 0.1
Central Tabulator	$\leq 10^{-6}$	≤ 0.01735	≤ 0.01735
Precinct Tabulator	$\leq 10^{-6}$	≤ 0.002452	≤ 0.01374
Voter-Editable Ballot Device (VEBD)	$\leq 10^{-6}$	≤ 0.002452	≤ 0.01374
Other electronic vote capture device	$\leq 10^{-6}$	≤ 0.003856	≤ 0.01718
Activation device	$\leq 10^{-6}$	≤ 0.002452	≤ 0.002452
Activation media/token (e.g. smart card)	$\leq 10^{-6}$	≤ 0.01978	≤ 0.01978

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

4.3.4 Product Marking

All voting systems **shall**:

a. Display on each device a separate data plate containing a schedule for and list of operations required to service or to perform preventive maintenance
b. Display advisory caution and warning instructions to ensure safe operation of the equipment and to avoid exposure to hazardous electrical voltages and moving parts at all locations where operation or exposure may occur

4.3.5 Workmanship

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

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

4.3.6 Safety

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

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

In order to meet these safety requirements, voting system manufacturers **shall** submit their systems for review to a Nationally Recognized Testing Laboratory (NRTL.) This standard does not require that a voting system carry a Product Safety Listing (Label), but voting system manufacturers may voluntarily choose to implement such labeling.

4.4 Testing - Hardware

The S-ATA **shall** design and perform procedures that test the voting system hardware requirements. Test procedures **shall** be designed and performed for both operating and non-operating environmental tests:

a. Operating environmental tests apply to the entire system, including hardware components that are used as part of the voting system telecommunications capability
b. Non-operating tests apply to those elements of the system that are intended for use at poll site voting locations, such as voting machines and precinct counters. These tests address environmental conditions that may be encountered by the voting system hardware at the voting location itself, or while in storage or transit to or from the poll site

Additionally, compatibility of this equipment with the voting system environment **shall** be determined through functional tests integrating the standard product with the remainder of the system.

All hardware components that are custom-designed for election use **shall** be tested in accordance with the applicable procedures contained in this section. Unmodified COTS hardware will not be subject to all tests. Generally such equipment has been designed to rigorous industrial standards and has been in wide use, permitting an evaluation of its performance history. To enable reduced testing of such equipment, manufacturers **shall** provide the manufacturer specifications and evidence that the equipment has been tested to the equivalent of these Standards.

The specific testing procedures to be used **shall** be identified in the Test Plan prepared by the S-ATA. These procedures may replicate testing performed by the manufacturer and documented in the manufacturer's TDP, but **shall not** rely on manufacturer testing as a substitute for hardware testing performed by the S-ATA.

4.4.1 Hardware Provided by Manufacturer

The hardware submitted for certification testing **shall** be equivalent, in form and function, to the actual production versions of the hardware units. Engineering or developmental prototypes are not acceptable unless the manufacturer can show that the equipment to be tested is equivalent to standard production units in both performance and construction.

4.4.2 Test Conditions

Certification tests may be performed in any facility capable of supporting the test environment. Preparation for testing, arrangement of equipment, verification of equipment status, and the execution of procedures **shall** be witnessed by at least one independent, qualified observer who **shall** certify that all test and data acquisition requirements have been satisfied.

When a test is to be performed at "standard" or "ambient" conditions, this requirement **shall** refer to a nominal laboratory environment at prevailing atmospheric pressure and relative humidity. Otherwise, all tests **shall** be performed at the required temperature and electrical supply voltage, regulated within the following tolerances:

a. Temperature of ±4 degrees F
b. Electrical supply voltage ±2 volts alternating current

4.4.3 Test Log Data Requirements

The S-ATA **shall** maintain a test log of the procedure employed. This log **shall** identify the system and equipment by model and serial number. Test environment conditions **shall** be noted.

In the event that the S-ATA deems it necessary to deviate from requirements pertaining to the test environment, the equipment arrangement and method of operation, the specified test procedure, or the provision of test instrumentation and facilities, the deviation **shall** be recorded in the test log. A discussion of the reasons for the deviation and the effect of the deviation on the validity of the test procedure **shall** also be provided.

4.4.4 Test Fixtures

The S-ATA **shall** not use simulation devices or software that bypass portions of the voting system that would be exercised in an actual election, with the following exceptions.

a. The S-ATA may bypass the user interface of an interactive device in the case of environmental tests that would require subjecting test "voters" to unsafe or unhealthy conditions, or that would be invalidated by the presence of a test "voter."
b. The S-ATA may bypass the user interface of an interactive device in capacity tests to verify that the system and its constituent components are able to operate correctly at the maximum limits specified in the implementation statement; for example, maximum number of ballots that can be counted, maximum possible vote total (counter capacity), or maximum number of ballot styles.

The S-ATA may use test fixtures or ancillary devices to facilitate testing as long as they closely and validly simulate actual election use of the system. If a tabulator is specified to count paper ballots that are manually marked with a specific writing utensil, it is not valid to substitute ballots that were mechanically marked by a printer. However, ballots that were marked according to manufacturer instructions can sometimes be recycled through a tabulator without invalidating the test.

4.4.5 Non-operating Environmental Tests

This section addresses a range of tests for voting machines and precinct counters, as such devices are stored between elections and are transported between the storage facility and polling place.

Environmental tests of non-operating equipment are intended to simulate exposure to physical shock and vibration associated with handling and transportation of voting equipment and precinct counters between a jurisdiction's storage facility and precinct polling places. These tests additionally simulate the temperature and humidity conditions that may be encountered during storage in an uncontrolled warehouse environment or precinct environment. The procedures and conditions of these tests correspond generally to those of MIL-STD-810D, "Environmental Test Methods and Engineering Guidelines," 19 July 1983. In most cases, the severity of the test conditions has been reduced to reflect commercial, rather than military, practice.

Systems exclusively designed with system-level COTS hardware whose configuration has not been modified in any manner are not subject to this segment of hardware testing. Systems made up of individual COTS components such as hard drives, motherboards, and monitors that have been packaged to build a voting machine or other device will be required to undergo the hardware testing.

Prior to each test, the equipment **shall** be shown to be operational. The equipment may then be prepared as if for actual transportation or storage, and subjected to appropriate test procedures outlined. After each procedure has been completed, the equipment's operational status will again be verified.

The following requirements for equipment preparation, functional tests, and inspections **shall** apply to each of the non-operating test procedures.

a. Pretest Data -The test technician **shall** verify that the equipment is capable of normal operation. Equipment identification, environmental conditions, equipment configuration, test instrumentation, operator tasks, time-of-day or test time, and test results **shall** be recorded.
b. Preparation for Test - The equipment **shall** be prepared as for the expected non-operating use, as noted below. When preparation for transport between the storage site and the polling place is required, the equipment **shall** be prepared with any protective enclosures or internal restraints that the manufacturer specifies for such transport. When preparation for storage is required, the equipment **shall** be prepared using any protective enclosures or internal restraints that the manufacturer specifies for storage.
c. Mechanical Inspection and Repair - After the test has been completed, the devices **shall** be removed from their containers, and any internal restraints **shall** be removed. The exterior and interior of the devices **shall** be inspected for evidence of mechanical damage, failure, or dislocation of internal components. Devices **shall** be adjusted or repaired, if necessary.
d. Electrical Inspection and Adjustment - After completion of the mechanical inspection and repair, routine electrical maintenance and adjustment may be performed, according to the manufacturer's standard procedure.
e. Operational Status Check - When all tests, inspections, repairs, and adjustments have been completed, normal operation **shall** be verified by conducting an operational status check. During this process, all equipment **shall** be operated in a manner and under environmental conditions that simulate election use to verify the functional status of the system. Prior to the conduct of each of the environmental hardware non-operating tests, a supplemental test **shall** be made to determine that the operational state of the equipment is within acceptable performance limits.

The following procedures **shall** be followed to verify the equipment status:

Step 1: Arrange the system for normal operation.
Step 2: Turn on power, and allow the system to reach recommended operating temperature.
Step 3: Perform any servicing, and make any adjustments necessary, to achieve operational status.
Step 4: Operate the equipment in all modes, demonstrating all functions and features that would be used during election operations.
Step 5: Verify that all system functions have been correctly executed.

f. Failure Criteria - Upon completion of each non-operating test, the system hardware **shall** be subject to functional testing to verify continued operability. If any portion of the voting machine or precinct counter hardware fails to remain fully functional, the testing will be suspended until the failure is identified and corrected by the manufacturer. The system will then be subject to a retest.

4.4.5.1 Bench Handling Test

The bench handling test simulates stresses faced during maintenance and repair of voting machines and ballot counters.
All systems and components, regardless of type, **shall** meet the requirements of this test.
This test is equivalent to the procedure of MIL-STD-810D, Method 516.3, Procedure VI.

Step 1: Place each piece of equipment on a level floor or table, as for normal operation or servicing.
Step 2: Make provision, if necessary, to restrain lateral movement of the equipment or its supports at one edge of the device. Vertical rotation about that edge shall not be restrained.
Step 3: Using that edge as a pivot, raise the opposite edge to an angle of 45 degrees, to a height of four inches above the surface, or until the point of balance has been reached, whichever occurs first.
Step 4: Release the elevated edge so that it may drop to the test surface without restraint.
Step 5: Repeat steps 3 and 4 for a total of six events.
Step 6: Repeat steps 2, 3, and 4 for the other base edges, for a total of 24 drops for each device.

4.4.5.2 Vibration Test

The vibration test simulates stresses faced during transport of voting machines and ballot counters between storage locations and polling places.
All systems and components, regardless of type, **shall** meet the requirements of this test.
This test is equivalent to the procedure of MIL-STD-810D, Method 514.3, Category 1-Basic Transportation, Common Carrier.

Step 1: Install the test item in its transit or combination case as prepared for transport.
Step 2: Attach instrumentation as required to measure the applied excitation.
Step 3: Mount the equipment on a vibration table with the axis of excitation along the vertical axis of the equipment.
Step 4: Apply excitation as shown in MIL-STD-810D, Method 514.3-1, “Basic transportation, common carrier, vertical axis”, with low frequency excitation cutoff at 10 Hz, for a period of 30 minutes.
Step 5: Repeat steps 2 and 3 for the transverse and longitudinal axes of the equipment with the excitation profiles shown in Figures 514.3-2 and

514.3-3, respectively. (Note: The total excitation period equals 90 minutes, with 30 minutes excitation along each axis.)

Step 6: Remove the test item from its transit or combination case and verify its continued operability.

4.4.5.3 Low Temperature Test

The low temperature test simulates stresses faced during storage of voting machines and ballot counters.

All systems and components, regardless of type, **shall** meet the requirements of this test. This test is equivalent to the procedure of MIL-STD-810D, Method 502.2, Procedure I-Storage. The minimum temperature **shall** be -4 degrees F.

Step 1: Arrange the equipment as for storage. Install it in the test chamber.

Step 2: Lower the internal temperature of the chamber at any convenient rate, but not so rapidly as to cause condensation in the chamber, and in any case no more rapidly than 10 degrees F per minute, until an internal temperature of -4 degrees F has been reached.

Step 3: Allow the chamber temperature to stabilize. Maintain this temperature for a period of 4 hours after stabilization.

Step 4: Allow the internal temperature of the chamber to return to standard laboratory conditions, at a rate not exceeding 10 degrees F per minute.

Step 5: Allow the internal temperature of the equipment to stabilize at laboratory conditions before removing it from the chamber.

Step 6: Remove the equipment from the chamber and from its containers, and inspect the equipment for evidence of damage.

Step 7: Verify continued operability of the equipment.

4.4.5.4 High Temperature Test

The high temperature test simulates stresses faced during storage of voting machines and ballot counters.

All systems and components, regardless of type, **shall** meet the requirements of this test. This test is equivalent to the procedure of MIL-STD-810D, Method 501.2, Procedure I-Storage. The maximum temperature **shall** be 140 degrees F.

Step 1: Arrange the equipment as for storage. Install it in the test chamber.

Step 2: Raise the internal temperature of the chamber at any convenient rate, but in any case no more rapidly than 10 degrees F per minute, until an internal temperature of 140 degrees F has been reached.

Step 3: Allow the chamber temperature to stabilize. Maintain this temperature for a period of 4 hours after stabilization.

Step 4: Allow the internal temperature of the chamber to return to standard laboratory conditions, at a rate not exceeding 10 degrees F per minute.

Step 5: Allow the internal temperature of the equipment to stabilize at laboratory conditions before removing it from the chamber.
Step 6: Remove the equipment from the chamber and from its containers, and inspect the equipment for evidence of damage.
Step 7: Verify continued operability of the equipment.

4.4.5.5 Humidity Test

The humidity test simulates stresses faced during storage of voting machines and ballot counters.

All systems and components regardless of type **shall** meet the requirements of this test. This test is similar to the procedure of MIL-STD-810D, Method 507.2, Procedure I-Natural Hot-Humid. It is intended to evaluate the ability of the equipment to survive exposure to an uncontrolled temperature and humidity environment during storage. This test lasts for ten days.

Step 1: Arrange the equipment as for storage. Install it in the test chamber.
Step 2: Adjust the chamber conditions to those given in MIL-STD-810D Table 507.2-I, for the time 0000 of the HotHumid cycle (Cycle 1).
Step 3: Perform a 24-hour cycle with the time and temperature-humidity values specified in Figure 507.2-1, Cycle 1.
Step 4: Repeat Step 2 until 5, 24-hour cycles have been completed.
Step 5: Continue with the test commencing with the conditions specified for time = 0000 hours.
Step 6: At any convenient time in the interval between time = 120 hours and time = 124 hours, place the equipment in an operational configuration, and perform a complete operational status check.
Step 7: If the equipment satisfactorily completes the status check, continue with the sixth 24-hour cycle.
Step 8: Perform 4 additional 24-hour cycles, terminating the test at time = 240 hours.
Step 9: Remove the equipment from the test chamber and inspect it for any evidence of damage.
Step 10: Verify continued operability of the equipment.

4.4.6 Operating Environmental Tests

This section addresses a range of tests for all voting system equipment, including equipment for both precinct count and central count systems.

a. All voting systems **shall** be tested in accordance with the appropriate procedures of MIL-STD-810D, "Environmental Test Methods and Engineering Guidelines".
    i. All voting systems **shall** be tested according to the low temperature and high temperature testing specified by MIL-STD-810-D: Method 502.2, Procedure II – Operation and Method 501.2, Procedure II – Operation, with test conditions that simulate system operation.

ii. All voting systems **shall** be tested according to the humidity testing specified by MIL-STD-810-D: Method 507.2, Procedure II – Natural (Hot–Humid), with test conditions that simulate system operation.

b. The reliability engineering **shall** be validated by the S-ATA in two ways:
   i. The S-ATA's reliability engineer **shall** review the reliability analysis and design documentation that the manufacturer provides in the TDP, and report a finding on its completeness, correctness, consistency with the requirements, and conformity to best practices.
   ii. Each failure observed during the test campaign (i.e., during *any* operational test) **shall** be traced back through the manufacturer's reliability analysis to determine whether it was correctly accounted for. The S-ATA **shall** report a finding on whether the observed performance validates or refutes the manufacturer's reliability analysis, or falls short of statistical significance.

4.4.6.1 Other Environmental Tests

For all voting system equipment, including equipment for both precinct count and central count systems:

a. The test for power disturbance disruption **shall** be conducted in compliance with the test specified in IEC 61000-4-11 (1994-06).
b. The test for electromagnetic radiation **shall** be conducted in compliance with the FCC Part 15 Class B requirements by testing per ANSI C63.4.
c. The test for electrostatic disruption **shall** be conducted in compliance with the test specified in IEC 61000-4-2 (2008-12) Ed. 2.0. Contact discharge at the 8 kV level is the preferred test method. Where contact discharge cannot be applied, air discharge **shall** be used at all four identified test levels (2 kV, 4 kV, 8 kV, 15 kV). During exploratory pre-testing, investigation of the possibility of windowing effects should be explored. If there are indications that a unit has sensitivity at a lower voltage but not at a higher voltage, test levels **shall** be added to evaluate the immunity at lower voltage levels.
d. The test for electromagnetic susceptibility **shall** be conducted in compliance with the test specified in IEC 61000-4-3 (1996).
e. The test for electrical fast transient protection **shall** be conducted in compliance with the test specified in IEC 61000-4-4 (2004-07) Ed. 2.0.
f. The test for lightning surge protection **shall** be conducted in compliance with the test specified in IEC 61000-4-5 (1995-02).
g. The test for conducted RF immunity **shall** be conducted in compliance with the test specified in IEC 61000-4-6 (1996-04).
h. The test for AC magnetic fields RF immunity **shall** be conducted in compliance with the test specified in IEC 61000-4-8 (1993-06).

5 Software Requirements

5.1 Software configuration

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

5.2 Software Design and Coding Standards

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

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

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

5.2.1 Scope

The requirements of this section that constrain programming practices—design requirements—apply to all application logic, regardless of the ownership of the logic or the ownership and location of the hardware on which the logic is installed or operates. Although it would be desirable for COTS software to conform to the design requirements on software workmanship, its conformity to those requirements could not be assessed without access to the source code; hence, the design requirements are scoped to exclude COTS software. In contrast, requirements that can be tested without access to source code, such as the requirement to detect and respond to invalid input without crashing, apply to COTS software in exactly the same way as they apply to non-COTS software.

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

Third-party logic, border logic, and configuration data are not required to conform to the design requirements on software workmanship, but manufacturers **shall** supply

that source code and data to the S-ATA to enable a complete review of the application logic.

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

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

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

5.2.2 Selection of Programming Languages

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

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

Block-structured exception handling (e.g., try/throw/catch). By excluding border logic, this requirement allows the use of assembly language for hardware-related segments, such as device controllers and handler programs. It also allows the use of an externally-imposed language for interacting with an Application Program Interface (API) or database query engine. However, the special code should be insulated from the bulk of the code, e.g. by wrapping it in callable units expressed in the prevailing language, to minimize the number of places that special code appears. C.f. MISRA-C:2004[1] Rule 2.1: "Assembly language **shall** be encapsulated and isolated." The term callable units is defined as function, method, operation, subroutine, procedure, or analogous structural unit that appears within a module.

Acceptable programming languages are also constrained by Requirements 5.2.7.a.iii and iv, which effectively prohibit manufacturers from inventing new languages.

The above requirement may be satisfied by using COTS extension packages to add missing control constructs to languages that could not otherwise conform. For example,

[1] MISRA-C:2004: Guidelines for the use of the C language in critical systems, MIRA Limited, U.K., 2004-10.

C11[2] does not support block-structured exception handling, but the construct can be retrofitted using (e.g.) cexcept[3] or another COTS package.

The use of non-COTS extension packages or manufacturer-specific code for this purpose is not acceptable, as it would place an unreasonable burden on the S-ATA to verify the soundness of an unproven extension (effectively a new programming language). The package must have a proven track record of performance supporting the assertion that it would be stable and suitable for use in voting systems, just as the compiler or interpreter for the base programming language must.

5.2.3 Selection of General Coding Standard

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

Coding standards **shall** be considered published if and only if they appear in a publicly available book, magazine, journal, or new media with analogous circulation and availability, or if they are publicly available on the Internet. Following are examples of published coding standards (links valid as of 2012-04-05). These are only examples and are not necessarily the best available for the purpose.

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

Coding standards **shall** be considered credible if and only if at least two different organizations with no ties to the creator of the rules or to the manufacturer seeking conformity assessment, and which are not themselves voting equipment manufacturers, independently decided to adopt them and made active use of them at some time within the three years before conformity assessment was first sought.

Coding standards evolve, and it is desirable for voting systems to be aligned with modern practices. If the "three year rule" was satisfied at the time that a system was first submitted for testing, it is considered satisfied for the purpose of subsequent

---

[2] ISO/IEC 9899:2011, Programming languages—C. Available from ISO, http://www.iso.org/.
[3] CEXCEPT (exception handling in C), software package, 2000. Available at http://cexcept.sourceforge.net/.

reassessments of that system. However, new systems must meet the three year rule as of the time that they are first submitted for testing, even if they reuse parts of older systems.

5.2.4 Software Modularity and Programming

a. Application logic **shall** be designed in a modular fashion. Each module **shall** have a specific function that can be tested and verified independently of the remainder of the code. In practice, some additional modules (such as library modules) may be needed to compile the module under test, but the modular construction allows the supporting modules to be replaced by special test versions that support test objectives.
b. Callable units **shall** have cyclomatic complexity[4] less than 20.

5.2.5 Structured Programming

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

Concept	Ada[5,6]	C[7,8]	C++[9,10]	C#[11,12]	Java[13,14]	Visual Basic 2005 (VB 8.0)[15]
Sequence	Yes	Yes	Yes	Yes	Yes	Yes
Loop with exit conditional	Yes	Yes	Yes	Yes	Yes	Yes
If/Then/Else conditional	Yes	Yes	Yes	Yes	Yes	Yes
Case conditional	Yes	Yes	Yes	Yes	Yes	Yes
Named block exit	Yes	No	No	No	Yes	No[16]
Block-structured exception handling	Yes	No	Yes	Yes	Yes	Yes

[4] T. McCabe, "A Complexity Measure," IEEE Transactions on Software Engineering Vol. SE-2, No. 4, pp. 308-320 (December 1976).
[5] ISO/IEC 8652:1987, Programming languages—Ada.
[6] ISO/IEC 8652:1995, Information technology—Programming languages—Ada. Available from ISO, http://www.iso.org/.
[7] ISO/IEC 9899:1990, Programming languages—C.
[8] ISO/IEC 9899:1999, Programming languages—C. Available from ISO, http://www.iso.org/.
[9] ISO/IEC 14882:1998, Programming languages—C++.
[10] ISO/IEC 14882:2003, Programming languages—C++. Available from ISO, http://www.iso.org/.
[11] ISO/IEC 23270:2003, Information technology—C# language specification.
[12] ISO/IEC 23270:2006, Information technology—Programming languages—C#. Available from ISO, http://www.iso.org/.
[13] The Java Language Specification, Third Edition, 2005. Available at http://docs.oracle.com/javase/specs.
[14] The Java Language Specification, Java SE 7 Edition, 2011. Available at http://docs.oracle.com/javase/specs.
[15] Paul Vick, The Microsoft® Visual Basic® Language Specification, Version 8.0, 2005. Available from Microsoft Download Center, http://go.microsoft.com/fwlink/?linkid=62990.
[16] Visual Basic 8 does not support named block exit, but it does support specifying the kind of block (do loop, for loop, while loop, select, subroutine, function, etc.) from which to exit, which need not be the innermost block.

The requirement to follow a coding standard serves two purposes. First, by requiring specific risk factors to be mitigated, coding standards support integrity and maintainability of voting system logic. Second, by making the logic more transparent to a reviewer, coding standards facilitate S-ATA evaluation of the logic's correctness to a level of assurance beyond that provided by operational testing.
Prominent among the requirements addressing logical transparency is the requirement to use high-level control constructs and to refrain from using the low-level arbitrary branch (a.k.a. goto). As is reflected in the above table, most high-level concepts for control flow are supported by all of the programming languages that were examined as probable candidates for voting system use as of this iteration. However, two additional concepts have been slower to gain universal support.

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

The second additional concept, called here "block-structured exception handling," is the ability to associate exception handlers with blocks of logic, and implicitly, the presence of the exception concept in the programming language. (This simply means try/throw/catch or equivalent statements, and should not be confused with the specific implementation known as Structured Exception Handling (SEH).[17]) Unlike deeply nested blocks, exceptions cannot be eliminated by restructuring logic. "When exceptions are not used, the errors cannot be handled but their existence is not avoided."[36]

These Standards require programming language exceptions because without them, the programmer must check for every possible error condition in every possible location, which both obfuscates the application logic and creates a high likelihood that some or many possible errors will not be checked for. Additionally, these Standards require block-structured exception handling because, like all unstructured programming, unstructured exception handling obfuscates logic and makes its verification by the S-ATA more difficult. "One of the major difficulties of conventional defensive programming is that the fault tolerance actions are inseparably bound in with the normal processing which the design is to provide. This can significantly increase design complexity and, consequently, can compromise the reliability and maintainability of the software."[37]

Existing voting system logic implemented in programming languages that do not support block-structured exception handling can be brought into compliance either through migration to a newer programming language (most likely, a descendant of the same

---

[17] Matt Pietrek, "A Crash Course on the Depths of Win32™ Structured Exception Handling," Microsoft Systems Journal, 1997-01. Available at http://www.microsoft.com/msj/0197/exception/exception.aspx. 36 ISO/IEC TR 15942:2000, Information technology—Programming languages—Guide for the use of the Ada programming language in high integrity systems. Available from ISO, http://www.iso.org/. 37 M. R. Moulding, "Designing for high integrity: the software fault tolerance approach," Section 3.4. In C. T. Sennett, ed., High-Integrity Software, Plenum Press, New York and London, 1989.

language that would require minimal changes) or through the use of a COTS package that retrofits block-structured exception handling onto the previous language with minimal changes. While the latter path may at first appear to be less work, it should be noted that many library functions may need to be adapted to throw exceptions when exceptional conditions arise, whereas in a programming environment that had exceptions to begin with the analogous library functions would already do this (see Requirement a below).

a. Application logic **shall** handle exceptions using block-structured exception handling constructs. If application logic makes use of any COTS or third-party logic callable units that do not throw exceptions when exceptional conditions occur, those callable units **shall** be wrapped in callable units that check for the relevant error conditions and translate them into exceptions, and the remainder of application logic **shall** use only the wrapped version. For example, if an application written in C99 + cexcept used the malloc function of libc, which returns a null pointer in case of failure instead of throwing an exception, the malloc function would need to be wrapped. Here is one possible implementation:

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

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

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

b. Application logic **shall** contain no unstructured control constructs.
   i. Arbitrary branches (a.k.a. gotos) are prohibited.
   ii. Exceptions **shall** only be used for abnormal conditions. Exceptions **shall** not be used to redirect the flow of control in normal ("non-exceptional") conditions. "Intentional exceptions" cannot be used as a substitute for arbitrary branch. Normal, expected events, such as reaching the end of a file that is being read from beginning to end or receiving invalid input from a user interface, are not exceptional conditions and should not be implemented using exception handlers.
   iii. Unstructured exception handling (e.g., On Error GoTo, setjmp/longjmp, or explicit tests for error conditions after every executable statement) is prohibited. The internal use of such constructs by a COTS extension package that adds block-structured exception handling to a programming language that otherwise would not have it, as described in Requirement a, is allowed. Analogously, it is not a problem that source code written in a high-level programming language is compiled into low-level machine code

that contains arbitrary branches. It is only the direct use of low-level constructs in application logic that presents a problem.

c. Application logic **shall** not compile or interpret configuration data or other input data as a programming language. Distinguishing what is a programming language from what is not requires some professional judgment. However, in general, sequential execution of imperative instructions is a characteristic of conventional programming languages that should not be exhibited by configuration data. Configuration data must be declarative or informative in nature, not imperative.

   For example: it is permissible for configuration data to contain a template that informs a report generating application as to the form and content of a report that it should generate, but it is not permissible for configuration data to contain instructions that are executed or interpreted to generate a report, essentially embedding the logic of the report generator inside the configuration data. The reasons for this requirement are (1) mingling code and data is bad design, and (2) embedding logic within configuration data is an evasion of the conformity assessment process for application logic.

5.2.6 Header Comments

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

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

5.2.7 Executable Code and Data Integrity[18]

a. Subrequirements i through iv apply to application logic (and only to application logic):
   i. Self-modifying code is prohibited.
   ii. Application logic **shall** be free of race conditions, deadlocks, livelocks, and resource starvation.
   iii. If compiled code is used, it **shall** only be compiled using a COTS compiler. This prohibits manufacturers from using arbitrary, nonstandard compilers and consequently prohibits the manufacturers from inventing new programming languages.
   iv. If interpreted code is used, it **shall** only be run under a specific, identified version of a COTS runtime interpreter. This ensures (1) that manufacturers do not use arbitrary, nonstandard interpreted languages, and (2) that the software tested and approved during the conformity assessment process does not change behavior because of a change to the interpreter.
b. All programmed devices **shall** prevent replacement or modification of executable or interpreted code (e.g., by other programs on the system, by people physically replacing the memory or medium containing the code, or by faulty code) except where this access is necessary to prepare authorized software and equipment for use. This requirement may be partially satisfied through a combination of read-only memory (ROM), the memory protection implemented by most popular COTS operating systems, error checking, and access and integrity controls.
c. All voting devices **shall** prevent access to or manipulation of configuration data, vote data or audit records (e.g., by physical tampering with the medium or mechanism containing the data, by other programs on the system, or by faulty code) except where this access is necessary to conduct the voting process. This requirement may be partially satisfied through a combination of the memory protection implemented by most popular COTS operating systems, error checking, and access and integrity controls. Systems using mechanical counters to store vote data must protect the counters from tampering. If vote data are stored on paper, the paper must be protected from tampering. Modification of audit records after they are created is never necessary.
d. All programmed devices **shall** provide the capability to monitor the transfer quality of I/O operations, reporting the number and types of errors that occur and how they were corrected.
e. Application logic and border logic **shall** contain no inaccessible code (dead code) other than defensive code (including exception handlers) that is provided to defend against the occurrence of failures and "can't happen" conditions.

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

5.2.8 Error Checking[19]

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

a. All programmed devices **shall** check information inputs, whether from manual entry or other external source, for completeness and validity and ensure that incomplete or invalid inputs do not lead to irreversible error.
    i. At any point where it is possible for a user (voter, poll worker, etc.) to enter a scalar or enumerated type value that is outside the range of values that is valid in the context of the device's logic, that input **shall** be range-checked. This applies to inputs of values of numeric types, character types, temporal types, and any other types for which the concept of range is well-defined.
    ii. ii. At any point where it is possible for a user to enter a character string or list of values that is longer than the maximum or shorter than the minimum length that is valid in the context of the device's logic, that input **shall** be length-checked.
    iii. The device **shall** respond to an invalid input by notifying the user of the error and enabling the user to correct the erroneous input before consequential errors and/or loss of program integrity occur.
b. All application logic that is vulnerable to the following types of errors **shall** check for these errors at run time and respond defensively (as specified by Requirement f) when they occur: (1) out-of-bounds accesses of arrays or strings (includes buffers used to move data); (2) stack overflow errors; (3) CPU-level exceptions such as address and bus errors, dividing by zero, and the like; (4) variables that are not appropriately handled when out of expected boundaries; (5) numeric overflows; (6) known programming language specific vulnerabilities.
    i. If the application logic uses arrays, vectors, or any analogous data structures and the programming language does not provide automatic run-time range checking of the indices, the indices **shall** be ranged-checked on every access. Range checking code should not be duplicated before each access. Clean implementation approaches include: (1) consistently using dedicated accessors (functions, methods, operations, subroutines, procedures, etc.) that range-check the indices; (2) defining and consistently using a new data type or class that encapsulates the range-checking logic; (3) declaring the array using a template that causes all accessors to be range-checked; or (4) declaring the array index to be a data type whose enforced range is matched to the size of the array. Range-enforced data types or classes may be

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

provided by the programming environment or they may be defined in application logic. If acceptable values of the index do not form a contiguous range, a map structure may be more appropriate than a vector.

ii. If stack overflow does not automatically result in an exception, the application logic **shall** explicitly check for and prevent stack overflow. Embedded system developers use a variety of techniques for avoiding stack overflow. Commonly, the stack is monitored and warnings and exceptions are thrown when thresholds are crossed. In non-embedded contexts, stack overflow often manifests as a CPU-level exception related to memory segmentation, in which case it can be handled pursuant to Requirement b.iii.

iii. The application logic **shall** implement such handlers as are needed to detect and respond to CPU-level exceptions. For example, under Unix a CPUlevel exception would manifest as a signal, so a signal handler is needed. If the platform supports it, it is preferable to translate CPU-level exceptions into software-level exceptions so that all exceptions can be handled in a consistent fashion within the voting application; however, not all platforms support it.

iv. All scalar or enumerated type parameters whose valid ranges as used in a callable unit (function, method, operation, subroutine, procedure, etc.) do not cover the entire ranges of their declared data types **shall** be range checked on entry to the unit. This applies to parameters of numeric types, character types, temporal types, and any other types for which the concept of range is well-defined. In cases where the restricted range is frequently used and/or associated with a meaningful concept within the scope of the application, the best approach is to define a new class or data type that encapsulates the range restriction, eliminating the need for range checks on each use. This requirement differs from Requirement a. Requirement a deals with user input, which is expected to contain errors, while this requirement deals with program internal parameters, which are expected to conform to the expectations of the designer. User input errors are a normal occurrence; the errors discussed here are grounds for throwing exceptions.

v. If the programming language does not provide automatic run-time detection of numeric overflow, all arithmetic operations that could potentially overflow the relevant data type **shall** be checked for overflow. This requirement should be approached in a manner similar to Requirement b.i of this section. Overflow checking should be encapsulated as much as possible.

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

i. If application logic uses pointers or a similar mechanism for specifying absolute memory locations, the application logic should validate pointers or addresses before they are used. Improper overwriting should be prevented in general as required by Requirements 5.2.7.b and c. Nevertheless, even if read-only memory would prevent the overwrite from succeeding, an attempted overwrite indicates a logic fault that must be corrected. Pointer use that is fully encapsulated within a standard platform library is treated as COTS software.

d. Application logic should be instrumented and/or analyzed with a COTS tool for detecting the kinds of errors enumerated in requirements b and c above.
e. If pointers are used, any pointer variables that remain within scope after the memory they point to is deallocated **shall** be set to null or marked as invalid (pursuant to the idiom of the programming language used) after the memory they point to is deallocated. If this is not done automatically by the programming environment, a callable unit should be dedicated to the task of deallocating memory and nullifying pointers. Equivalently, "smart pointers" like the C++ std::unique_ptr can be used to avoid the problem. One should not add assignments after every deallocation in the source code. In languages using garbage collection, memory is not deallocated until all pointers to it have gone out of scope, so this requirement is moot.
f. The detection of any of the errors enumerated in Requirements b and c **shall** be treated as a complete failure of the callable unit in which the error was detected. An appropriate exception **shall** be thrown and control **shall** pass out of the unit forthwith.
g. Error checks detailed in Requirements b and c **shall** remain active in production code. These errors are incompatible with voting integrity, so masking them is unacceptable. Manufacturers should not implement error checks using the C/C++ assert() macro. It is often disabled, sometimes automatically, when software is compiled in production mode. Furthermore, it does not appropriately throw an exception, but instead aborts the program.
h. Exceptions resulting from failed error checks or CPU-level exceptions **shall** require intervention by an election official or administrator before voting can continue. These errors are incompatible with voting integrity, so masking them is unacceptable.
i. Electronic devices **shall** include a means of identifying device failure and any corrective action needed.
j. Electronic devices should proactively detect equipment failures and alert an election official or administrator when they occur.
k. Electronic devices **shall** proactively detect or prevent basic violations of election integrity (e.g., stuffing of the ballot box or the accumulation of negative votes) and alert an election official or administrator if they occur. Equipment can verify only those conditions that are within the scope of what the equipment does. This provides defense-in-depth to supplement procedural controls and auditing practices.

5.3 Data and Document Retention

All systems **shall**:

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

5.4 Audit Record Data

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

5.4.1 Pre-election Audit Records

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

The log **shall** include:

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

5.4.2 System Readiness Audit Records

The following minimum requirements apply to system readiness audit records:

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

i. Number of ballots sent
ii. When each ballot was sent
iii. Machine from which each ballot was sent
iv. Specific votes or selections contained in the ballot

5.4.3 In-process Audit Records

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

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

5.4.4 Vote Tally Data

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

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

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

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

5.5 Vote Secrecy on DRE and EBM Systems

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

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

5.6 Testing – Software

The S-ATA **shall** design and perform procedures that test the voting system software requirements.

Unmodified, general purpose COTS non-voting software (e.g., operating systems, programming language compilers, data base management systems, and Web browsers) is not subject to source code review. However, the S-ATA **shall** examine such software to confirm that the specific version of software being used agrees with the design specification. Portions of COTS software that have been modified by the manufacturer in any manner are subject to source code review.

Source code that is generated by a COTS package and embedded in software modules for compilation or interpretation **shall** be provided in human readable form to the S-ATA. The S-ATA may inspect the generated source code in preparation of test plans and to check for embedded application logic or unauthorized changes. However, source code that is generated by a COTS package is third-party logic and is therefore not in scope of the requirements that apply only to application logic, such as the requirement to adhere to a coding standard.

Compatibility of the voting system software components or subsystems with one another, and with other components of the voting system environment, **shall** be determined through functional tests integrating the voting system software with the remainder of the system.
The specific procedures to be used **shall** be identified in the Test Plan prepared by the S-ATA in conjunction with the SOS. These procedures may replicate testing performed by the manufacturer and documented in the manufacturer's TDP, but **shall** not rely on manufacturer testing as a substitute for software testing performed by the S-ATA. Recognizing the variations in system design and the technologies employed by different manufacturers, the S-ATA **shall** design test procedures that account for these variations.

5.6.1 Initial Review of Documentation

Prior to initiating the software review, the S-ATA **shall** verify that the documentation submitted by the manufacturer in the TDP is sufficient to enable:

a. Review of the source code
b. Design and conduct tests at every level of the software structure to verify that the software meets the manufacturer's design specifications and the requirements of the performance guidelines

5.6.2 Source Code Review

Although the following requirements are scoped to application logic, in some cases the test lab may need to inspect border logic and third-party logic to assess conformity. The source code for all of these must be provided as part of the Technical Data Package.

a. The test lab **shall** assess the extent to which the application logic adheres to the specifications made in its design documentation.
b. The test lab **shall** assess the extent to which the application logic adheres to the requirements. This **shall** include an assessment of the extent to which the application logic adheres to the published, credible coding standard chosen by the manufacturer. Since the nature of the requirements specified by the manufacturer and the chosen coding standard cannot be known until they are made available to the test lab, conformity may be subject to interpretation. Nevertheless, egregious disagreements between the application logic and its design documentation or the coding standard should lead to a defensible adverse finding.
c. The test lab **shall** verify the efficacy of built-in measurement, self-test, and diagnostic capabilities of the voting system, including those that support logic and accuracy testing and any others.

6 Telecommunications Requirements

6.1 Scope

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

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

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

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

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

Local area network (LAN) components consist of the hardware and software infrastructure used to transport information between users in a local environment, typically a building or group of buildings. Typically a LAN connects workstations with a local server.

An application may be a single program or a group of programs that work together to provide a function to an end user, who may be a voter or an election administrator. Voter programs may include voter registration, balloting, and status checking. Administrator programs may include ballot preparation, registration for preparation, registration approval, ballot vetting, ballot processing, and election processing.

This section is intended to complement the network security requirements, which include requirements for voter and administrator access, availability of network service, data confidentiality, and data integrity. Most importantly, security services must prevent access to local election system components from public resources.

6.1.1 Types of Components

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

- Cabling technologies including Universal Twisted Pair cable (CAT 5 or higher) or Ethernet hub/switch

6.1.2 Data Transmission

These requirements apply to the use of telecommunications to transmit data for the preparation of the system for an election, the execution of an election, and the preservation of the system data and audit trails during and following an election. While this section does not assume a specific model of voting system operations and does not assume a specific model for the use of telecommunications to support such operations, it does address the following types of data, where applicable:

Voter Authentication: Coded information that confirms the identity of a voter for security purposes for a system that transmits votes individually

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

Vote Count: Information representing the tabulation of votes at any level within the control of the jurisdiction, such as the polling place, precinct or central count

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

Additional data transmissions used to operate a voting system in the conduct of an election, but not explicitly listed above, are also subject to the requirements of this section.

6.2 Design, Construction, and Maintenance Requirements

Design, construction, and maintenance requirements for telecommunications represent the operational capability of both system hardware and software. These capabilities **shall** be considered basic to all data transmissions.

6.2.1 Confirmation

Confirmation occurs when the system notifies the user of the successful or unsuccessful completion of the data transmission, where successful completion is defined as accurate receipt of the transmitted data. To provide confirmation, the telecommunications components of a voting system shall notify the user of the successful or unsuccessful completion of the data transmission. In the event of unsuccessful transmission the user shall be notified of the action to be taken.

7. Security Requirements

7.1 Scope

This section describes essential security capabilities for a voting system, encompassing the system's hardware, software, communications and documentation. No predefined set of security standards will address and defeat all conceivable or theoretical threats. The *Standards* articulate requirements to achieve acceptable levels of integrity and reliability. The objectives of the security standards for voting systems are:

- To protect critical elements of the voting system
- To establish and maintain controls to minimize errors
- To protect the system from intentional manipulation, fraud and malicious mischief
- To identify fraudulent or erroneous changes to the voting system
- To protect secrecy in the voting process

The *Voting System Standards* are intended to address a broad range of risks to the integrity of a voting system. While it is not possible to identify all potential risks, the Standards identify several types of risks that must be addressed. These include:

- Unauthorized changes to system capabilities for:
  - Defining ballot formats
  - Casting and recording votes
  - Calculating vote totals consistent with defined ballot formats
  - Reporting vote totals
- Alteration of voting system audit trails
- Changing, or preventing the recording of, a vote
- Introducing data for a vote not cast by a registered voter
- Changing calculated vote totals
- Preventing access to vote data--including individual votes and vote totals--by unauthorized individuals
- Preventing access to voter identification data and data for votes cast by the voter such that an individual can determine the content of specific votes

The requirements apply to the broad range of hardware, software, communications components, and documentation that comprises a voting system. These requirements apply to those components that are:

- Provided by the voting system manufacturer and the manufacturer's suppliers
- Furnished by an external provider (i.e., providers of personal computers and COTS operating systems) where the components are capable of being used during voting system operation
- Developed by a voting jurisdiction

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

- Voting devices and vote counting devices installed at polling places under the control or authority of the voting jurisdiction
- Ballot printers, vote counting devices, and other hardware typically installed at central or precinct locations (including contractor facilities)

7.1.1 Elements of Security Outside Manufacturer Control

The requirements of this section apply to the capabilities of a voting system that must be provided by the manufacturer. However, an effective security program requires well defined security practices by the purchasing jurisdiction and the personnel managing and operating the system. These practices include:

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

Implementation of these elements is not under the control of the manufacturer. However, manufacturers must provide appropriate system capabilities to enable the implementation of management controls.

7.1.2 Organization of This Section

The standards presented in this section are organized as follows:

Access Control: These standards address procedures and system capabilities that limit or detect access to critical system components in order to guard against loss of system integrity, availability, confidentiality, and accountability.

Physical Security: These standards address physical security measures and procedures that prevent disruption of the voting process at the polling place and corruption of voting data.

Software Security: These standards address the installation of software, including firmware, in the voting system and the protection against malicious software. It should be noted that computer-generated audit controls facilitate system security and are an integral part of software capability.

Telecommunications and Data Transmission: These standards address security for the electronic transmission of data between systems.

Use of Public Communications Networks: These standards prohibit voting systems from having the capability to communicate individual votes or vote totals over public communications networks.

Wireless Communications: These standards prohibit wireless communications capabilities in voting systems.

Independent Verification Systems: This section provides an introduction to the concept of independent verification as a method to demonstrate voting system integrity. This discussion provides the context for the requirements for voter verifiable paper audit trails in DREs.

Direct-Recording Electronic Systems with Voter Verifiable Paper Audit Trails: This capability is required for certification.

7.2 Access Control

Access controls are procedures and system capabilities that detect or limit access to system components in order to guard against loss of system integrity, availability, confidentiality, and accountability. Access controls provide reasonable assurance that system resources such as data files, application programs, and computer-related facilities and equipment are protected against unauthorized operation, modification, disclosure, loss or impairment. Unauthorized operations include modification of compiled or interpreted code, run-time alteration of flow control logic or of data, and abstraction of raw or processed voting data in any form other than a standard output report by an authorized operator.

Access controls may include physical controls, such as keeping computers in locked rooms to limit physical access, and technical controls, such as security software programs designed to prevent or detect unauthorized access to sensitive files. The access controls described in this section are limited to those controls required to be provided by system manufacturers.

7.2.1 General Access Control

General requirements address the high-level functionality of a voting system. These are the fundamental access control requirements upon which other requirements in this section are based.

a. Voting system equipment **shall** provide access control mechanisms designed to permit authorized access to the voting system and to prevent unauthorized access to the voting system.
    i. Access control mechanisms on the EMS **shall** be capable of identifying and authenticating individuals permitted to perform operations on the EMS.
b. Voting system equipment **shall** provide controls that permit or deny access to the device's software and files.
c. The default access control permissions **shall** implement the minimum permissions needed for each role or group identified by a device.
d. The voting device **shall** prevent a lower-privileged process from modifying a higher-privileged process.
e. An administrator of voting system equipment **shall** authorize privileged operations.

f. Voting system equipment **shall** prevent modification to or tampering with software or firmware through any means other than the documented procedure for software upgrades.

7.2.2 Access Control Identification

Identification requirements provide controls for accountability when operating and administering a voting system.

a. The voting system **shall** identify users and processes to which access is granted and the specific functions and data to which each entity holds authorized access.
b. Voting system equipment that implements role-based access control **shall** support the recommendations for Core RBAC in the ANSI INCITS 359-2004 American National Standard for Information Technology- Role Based Access Control document.
c. Voting system equipment **shall** allow the administrator group or role to configure the permissions and functionality for each identity, group, or role to include account and group/role creation, modification, and deletion.

7.2.3 Access Control Authentication

Authentication establishes the validity of the identity of the user, application, or process interacting with the voting system. Authentication is based on the identification provided by the user, application, or process interacting with the voting system. User authentication is generally classified in one of the following three categories:

- Something the user knows – this is usually a password, pass phrase, or PIN
- Something the user has – this is usually a token that may be either hardware or software based, such as a smart card
- Something the user is – this is usually a fingerprint, retina patter, voice pattern or other biometric data

Traditional password authentication is a single factor authentication method. A more secure method of authentication combines the various methods of authentication into two-factor authentication, or multi-factor authentication. For example, a user may use an authentication token and a passphrase for authentication. Using multi-factor provides stronger authentication than single factor. There are also cryptographic-based authentication methods such as digital signatures and challenge-response authentication, which are either software or hardware-based based tokens.

The following authentication requirements apply to all voting system equipment.

a. Voting system equipment **shall** authenticate users prior to granting them access to system functions or data.
b. When private or secret authentication data is stored in voting system equipment, the data **shall** be protected to ensure that the confidentiality and integrity of the data is not violated.
c. Voting system equipment **shall** allow the administrator group or role to set and change passwords, pass phrases, and keys.

d. Voting system equipment **shall** allow privileged groups or roles to be disabled and allow new individual privileged groups or roles to be created.
e. Voting system equipment **shall** lock out groups, roles, or individuals after a specified number of consecutive failed authentication attempts within a predefined time period.
f. Voting systems **shall** allow the administrator group or role to configure the account lock out policy, including the time period within which failed attempts must occur, the number of consecutive failed access attempts allowed before lock out, and the length of time the account is locked out.
g. If the voting system uses a user name and password authentication method, the voting system **shall** allow the administrator to enforce password strength, histories, and expiration.
h. The voting system **shall** allow the administrator group or role to specify password strength for all accounts, including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters.
i. The voting system **shall** enforce password histories, and allow the administrator to configure the history length.
j. Voting system equipment **shall** ensure that the username is not used in the password.
k. Voting systems **shall** provide a means to automatically expire passwords in accordance with the voting jurisdiction's policies.

7.2.4 Access Control Authorization

Authorization is the process of determining access rights based on authentication of a user, application, or process within a voting system. Authorization permits or denies access to an object by a subject. Subjects may be users, applications, or processes that interact with the voting system. Objects may be files or programs within the voting system.

a. Voting systems **shall** ensure that only authorized roles, groups, or individuals have access to election data.
b. Voting systems **shall** explicitly authorize subject's access based on access control lists or policies.
c. Voting systems **shall** explicitly deny subject's access based on access control lists or policies.

7.3 Physical Security Measures

A voting system's sensitivity to disruption or corruption of data depends, in part, on the physical location of equipment and data media. Most often, the disruption of voting and vote counting results from a physical violation of one or more areas of the system thought to be protected. Therefore, security procedures **shall** address physical threats and the corresponding means to defeat them.

a. Any unauthorized physical access **shall** leave physical evidence that an unauthorized event has taken place.
b. Voting systems **shall** only have physical ports and access points that are essential to voting operations and to voting system testing and auditing.

c. An event log entry that identifies the name of the affected device **shall** be generated if a component connected to a piece of voting system equipment is disconnected while polls are open.
d. Ports disabled while polls are open **shall** only be re-enabled by authorized administrators.
e. Access points, such as covers and panels, **shall** be secured by locks or tamper evident seals or tamper resistant countermeasures **shall** be implemented so that system owners can monitor access to voting system components through these points.
f. Ballot boxes **shall** be designed such that any unauthorized physical access results in physical evidence that an unauthorized event has taken place.

7.3.1 Polling Place Security

For polling place operations, manufacturers **shall** develop and provide detailed documentation of measures to enable poll workers to physically protect and perform orderly shutdown of voting equipment to counteract vandalism, civil disobedience, and similar occurrences.

The measures **shall** allow the immediate detection of tampering with vote casting devices and precinct ballot counters.

7.3.2 Central Count Location Security

Manufacturers **shall** develop and document in detail the measures to be taken in a central counting environment. These measures **shall** include physical and procedural controls related to the handling of ballot boxes, preparing of ballots for counting, counting operations and reporting data.

7.4 Software Security

Voting systems **shall** meet specific security requirements for the installation of software and for protection against malicious software.

7.4.1 Software and Firmware Installation

The system **shall** meet the following requirements for installation of software, including hardware with embedded firmware.

a. Air Gap Architecture

    i. Every voting system **shall** be capable of being deployed in a segregated dual-installation architecture to protect against propagation of viruses. The architecture **shall** allow elections officials to use one or more, permanent server(s) and set of central-office voting devices, known to be running unaltered, certified software and firmware to create memory cards before each election and to use another, physically separate "sacrificial" server and set of voting devices after the election to tabulate results and generate reports. The architecture **shall** allow transfer of the election definition and tally database from the permanent server(s) to the

sacrificial server using a write-once medium, such as a CD-R. The voting system architecture **shall** allow each installation to use its own Ethernet network, port server, and central-office vote-recording units, including any DRE and optical scan units, permitting the two installations to be segregated and air-gapped to ensure that there are no cross connections. An air gap is established by keeping two installations/networks physically separate and seeing that no device attached to the sacrificial installation/network is connected (directly or indirectly) to the first network, ensuring that data cannot flow from one installation/network to the other.

ii. The TDP for the voting system **shall** provide full procedures and instructions, to be incorporated into the Official Use Procedures for the voting system, to implement the segregated dual-installation architecture.

b. Voting and Tabulating Units

i. If software is resident in the system as firmware, the manufacturer **shall** require and state in the system documentation that every device is to be retested to validate each ROM prior to the start of elections operations.

ii. To prevent alteration of executable code, no software **shall** be permanently installed or resident in the voting system unless the system documentation states that the jurisdiction must provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of the system hardware.

iii. The voting system bootstrap, monitor, and device-controller software may be resident permanently as firmware, provided that this firmware has been shown to be inaccessible to activation or control by any means other than by the authorized initiation and execution of the vote counting program, and its associated exception handlers.

iv. The election-specific programming may be installed and resident as firmware, provided that such firmware is installed on a component (such as a computer chip) other than the component on which the operating system resides.

v. After initiation of Election Day testing, no source code or compilers or assemblers **shall** be resident or accessible.

7.4.2 Protection against Malicious Software

Voting systems **shall** deploy commercial-off-the-shelf (COTS) protection against the many forms of threats to which they may be exposed such as file and macro viruses, worms, Trojan horses, and logic bombs.

Manufacturers **shall** develop and document the procedures to be followed to ensure that such protection is maintained in a current status. Virus and malware protection software and updates **shall** be installed using transportable portable media only and **shall not** be installed by download from the Internet.

7.4.3 Software Distribution and Setup Validation

Subsections 7.4.4, 7.4.5 and 7.4.6 specify requirements for the distribution of voting system software and the setup validation performed on voting system equipment. These requirements are applicable to voting systems that have completed certification testing. The goal of the software distribution requirements is to ensure that the correct voting

system software has been distributed without modification. The goal of setup validation requirements, including requirements for verifying the presence of certified software and the absence of other software, is to ensure that voting system equipment is in a proper initial state before being used.

In general, a voting system can be considered to be composed of multiple associated systems including polling place systems, central counting/aggregation systems, and election management systems. These other systems may reside on different computer platforms at different locations and run different software. Voting system software is considered to be all executable code and associated configuration files critical for the proper operation of the voting system regardless of the location of installation and functionality provided. This includes third party software such as operating systems, drivers, and database management systems.

7.4.4 Software Distribution

The manufacturer **shall** document all software including voting system software, third party software (such as operating systems and drivers) to be installed on the certified voting system, and installation programs.

a. The documentation **shall** have a unique identifier (such as a serial number or part number) for the following set of information: documentation, software manufacturer name, product name, version, the certification application number of the voting system, file names and paths or other location information (such as storage addresses) of the software.
b. The documentation **shall** designate all software files as static, semi-static or dynamic.

7.4.5 Software Reference Information

a. The manufacturer **shall** provide the NSRL, any California certified escrow facility, pursuant to Title 2, Division 7, Chapter 6 of the California Code of Regulation, and the Office of the Secretary of State with a copy of the software installation disk, including the executable binary images of all third party software. Further, the manufacturer **shall** deposit the source code, tools, and documentation, to allow the complete and successful compilation of a system in its production/operation environment.
    i. The manufacturer **shall** document that the process used to verify the software distributed on unalterable storage media is the certified software by using the reference information provided by the NSRL or other designated repository before installing the software.
b. The voting system equipment **shall** be designed to allow the voting system administrator to verify that the software is the certified software by comparing it to reference information produced by the NSRL or other designated repository.
c. The manufacturers **shall** document to whom they provide voting system software.

7.4.6 Software Setup Validation

The following requirements support the security of voting systems by providing methods to verify that only authorized software is present on voting systems. It includes

requirements for two software verification techniques. One method verifies digital signatures on software prior to installation on pieces of voting system equipment. This is a useful mechanism that helps prevent accidental or malicious software from being installed and could be employed by any voting system to protect against unauthorized software. The second method provides an external interface to voting system software. A separate piece of equipment could use this interface to verify the software on the voting system. However, this method merely provides a mechanism for detecting unauthorized software and, by itself, does not help prevent the installation of accidental or malicious software.

a. Setup validation methods **shall** verify that only authorized software is present on the voting equipment. Authorized software is COTS software components needed to run the voting system and voting software components identified by the manufacturer as authorized.
b. The manufacturer **shall** provide a method to comprehensively list all software files that are installed on voting systems.
    i. This method **shall** list version names and numbers for all application software on the voting system.
    ii. This method should list of the date of installation for all application software on the voting system.
c. Setup validation methods **shall** include a software verification method that ensures that the voting system software has not been modified illegitimately.
    i. The voting systems **shall** include any supporting software and hardware necessary to conduct the software verification method.
    ii. The manufacturer **shall** document the process used to conduct the software verification method.
    iii. The software verification method **shall** not modify the voting system software on the voting system.
d. Voting systems **shall** include a software verification method that either verifies software prior to installation or a method that verifies software using an external interface. Voting systems may include both software verification methods. Voting systems may provide ancillary setup validation methods, including methods for verifying or identifying installed software, other than those described in this section. There are no specific requirements for ancillary setup validation methods. However, any method intended to serve as the voting system software verification method must meet the requirements outlined in this section.
e. Voting systems which implement a software verification method that verifies software prior to installation **shall** meet the following requirements.
    i. The voting system **shall** contain no more than one method for installing, updating, or removing software on a system.
        - Voting system equipment **shall** prevent processes from installing software except for the one specific software installation process identified by the manufacturer.
        - The voting system manufacturer **shall** document the procedures for installing, updating, and removing voting system software, configuration files, and data files.
        - Voting system equipment **shall** prevent processes from installing, updating or removing software while the polls are open.

- Voting system equipment **shall** prevent the execution of software not installed using the specified software installation process.

ii. The voting system **shall** only allow authenticated administrators to install software on voting equipment. The voting system **shall** present the administrator with a description of the software change being performed, including:
   - A list of all applications and/or file names being updated.
   - The type of action performed on each application and/or file (e.g., new application/file, deletion or overwriting of existing file)

iii. Voting system equipment **shall** store the current version identification of all software installed on the voting system equipment.
   - The current version identification **shall** be included as part of reports created by the voting system equipment.
   - The current version identification **shall** be displayed as part of the voting system equipment start up process.

iv. The process for installing, updating and removing software **shall** make software changes based on information contained in software update packages. Software update packages **shall** minimally contain the following information:
   - A unique identifier for the software update package.
   - Names of the applications or files modified during the update process.
   - Version numbers of the applications or files modified during the update process.
   - Any software prerequisites or dependencies for the software involved in the update.
   - A description of the type of action performed on each application and/or file (e.g., new application/file, deletion or overwriting of existing file).
   - The binary data of any new or updated files involved in the update process.

v. The software update package **shall** be formatted in a non-restrictive, publicly-available format. Manufacturers **shall** provide a specification describing how they have implemented the format with respect to the manufacturer's specific voting devices and data, including such items as descriptions of elements, attributes, constraints, extensions, syntax and semantics of the format, and definitions for data fields and schemas. vi. Software update packages **shall** be digitally signed by using a NIST approved algorithm with a security strength of at least 112 bits. vii. The software installation process **shall** verify digital signatures, software version identification, software prerequisites and dependencies, and manufacturer specific authorization information associated with the software before the software is installed. The software installation process **shall** not install software with invalid digital signatures, version numbers, or manufacturer specific authorization information, and **shall** not install software on systems that do not meet the update requisites.

vi. The voting system **shall** have the capability to prevent the installation of previous versions of applications or files.

vii. The software installation process **shall** result in information being stored in the voting system equipment's log such that altering or deleting log entries or the log will be detected.
viii. The minimum information to be included in the voting system equipment log **shall** be:
- Success or failure of the software installation process;
- Cause of a failed software installation (such as invalid version identification, digital signature, etc.);
- Application or file name(s), and version number(s);
- A description of the type of action performed on each application and/or file (e.g., new application/file, deletion or overwriting of existing file);
- A cryptographic hash of the software update package using FIPS 1402 level 1 or higher validated cryptographic module.

f. If software is verified after being installed on the voting system equipment, the voting system equipment **shall** provide an external interface to the location of the voting system software for software verification purposes.
i. The external interface:
- **Shall** be protected using tamper evident techniques,
- **Shall** have a physical indicator showing when the interface is enabled and disabled
- **Shall** be disabled during voting
- Should provide a direct read-only access to the location of the voting system software without the use of installed software ii. The verification process should be able to be performed using COTS software and hardware available from sources other than the voting system manufacturer.
- If the process uses hashes or digital signatures, then the verification software **shall** use a FIPS 140-2 level 1 or higher validated cryptographic module.
- The verification process **shall** either (a) use reference information on unalterable storage media received from the repository or (b) verify the digital signature of the reference information on any other media.

g. Setup validation methods **shall** verify the contents of all system storage locations (e.g., system registers, variables, files, etc.) containing election specific information (e.g., ballot style, candidate registers, measure registers, etc.).
i. The manufacturer should provide a method to query the voting system to determine the value contained in all system storage locations containing election specific information.
ii. The manufacturer **shall** document the default values of all system storage locations that hold election specific information.

7.5 Open-Ended Vulnerability Testing

Vulnerability testing is an attempt to bypass or break the security of a system or a device. Like functional testing, vulnerability testing can falsify a general assertion (namely, demonstrate that the system or device is secure) but it cannot verify the security (show that the system or device is secure in all cases). Open-ended vulnerability testing (OEVT) is conducted without the confines of a pre-determined test suite. It instead relies

heavily on the experience and expertise of the OEVT Team Members, their knowledge of the system, its component devices and associated vulnerabilities, and their ability to exploit those vulnerabilities.

The goal of OEVT is to discover architecture, design and implementation flaws in the system that may not be detected using systematic functional, reliability, and security testing and which may be exploited to change the outcome of an election, interfere with voters' ability to cast ballots or have their votes counted during an election or compromise the secrecy of the vote. The goal of OEVT also includes attempts to discover logic bombs, time bombs or other Trojan Horses that may have been introduced into the system hardware, firmware, or software for said purposes.

7.5.1 OEVT Scope and Priorities

a. Scope of open-ended vulnerability testing - The scope of open ended vulnerability testing **shall** include the voting system security during all phases of the voting process and **shall** include all manufacturer supplied voting system use procedures. The scope of OEVT includes but is not limited to the following:
    i. Voting system security;
    ii. Voting system physical security while voting devices are:
        - In storage;
        - Being configured;
        - Being transported; and
        - Being used.
    iii. Voting system use procedures.
b. Focus of open-ended vulnerability testing - OEVT Team members **shall** seek out vulnerabilities in the voting system that might be used to change the outcome of an election, to interfere with voters' ability to cast ballots or have their votes counted during an election or to compromise the secrecy of vote.
c. OEVT General Priorities - The OEVT team **shall** prioritize testing efforts based on:
    i. threat scenarios for the voting system under investigation;
    ii. the availability of time and resources;
    iii. the OEVT team's determination of easily exploitable vulnerabilities; and
    iv. the OEVT team's determination of which exploitation scenarios are more likely to impact the outcome of an election, interfere with voters' ability to cast ballots or have their votes counted during an election or compromise the secrecy of the vote.
    v. All threat scenarios must be plausible in that they should not be in conflict with the anticipated implementation, associated use procedures, the workmanship requirements (assuming those requirements were all met) or the development environment specification as supplied by the manufacturer in the TDP;
    vi. Open-ended vulnerability testing should not exclude those threat scenarios involving collusion between multiple parties including manufacturer insiders. It is acknowledged that threat scenarios become less plausible as the number of conspirators increases;

vii. It is assumed that attackers may be well resourced and may have access to the system while under development;
viii. Threats that can be exploited to change the outcome of an election and flaws that can provide erroneous results for an election should have the highest priority;
ix. Threats that can cause a denial of service during the election should be considered of very high priority;
x. Threats that can compromise the secrecy of the vote should be considered of high priority;
xi. A threat to disclosure or modification of metadata (e.g., security audit log) that does not change the outcome of the election, does not cause denial of service during the election, or does not compromise the secrecy of ballot should be considered of lower priority;
xii. If the voting device uses COTS products, then the OEVT team should also investigate publicly known vulnerabilities; and
xiii. The OEVT team should not consider the voting device vulnerabilities that require Internet connectivity for exploitation if the voting device is not connected to the Internet during the election and otherwise. However, if the voting device is connected to another device which in turn may have been connected to the Internet (as may be the case of epollbooks), Internet based attacks may be plausible and should be investigated.

7.5.2 OEVT Resources and Level of Effort

a. OEVT team resources - The OEVT team **shall** use the manufacturer supplied Technical Data Package (TDP) and User documentation, have access to voting devices configured similar to how they are to be used in an election, and have access to all other material and tools necessary to conduct a thorough investigation. Materials supplied to the OEVT team **shall** include but not be limited to the following:
    i. Threat analysis describing threats mitigated by the voting system;
    ii. Security architecture describing how threats to the voting system are mitigated;
    iii. High level design of the system;
    iv. Any other documentation provided to an EAC voting system testing laboratory or S-ATA, if applicable;
    v. Source code;
    vi. Operational voting system configured for election, but with the ability for the OEVT team to reconfigure it;
    vii. Testing reports from the developer and from the testing laboratory including previous OEVT results;
    viii. Tools sufficient to conduct a test lab build; and
    ix. Procedures specified by the manufacturer as necessary for implementation and secure use.
b. Open-ended vulnerability team establishment - The test lab **shall** establish an OEVT team of at least 3 security experts and at least one election management expert to conduct the open-ended vulnerability testing.

c. OEVT Team Composition: Security Experts - The OEVT team **shall** have at least one member with 6 or more years of experience in the area of software engineering, at least one member with 6 or more years of experience in the area of information security, at least one member with 6 or more years of experience in the area of penetration testing and at least one member with 6 or more years of experience in the area of voting system security.
d. OEVT Team Composition: Election Management Expert - The OEVT team **shall** have at least one member with at least 8 years of experience in the area of election management. The OEVT team **shall** consult with an elections expert, designated by the Secretary of State, who is familiar with election procedures, how the voting systems are installed and used, and how votes are counted.
e. OEVT team knowledge - The OEVT team knowledge **shall** include but not be limited to the following:
    i. Complete knowledge of work done to date on voting system design, research and analysis conducted on voting system security, and known and suspected flaws in voting systems;
    ii. Complete knowledge of threats to voting systems;
    iii. Knowledge equivalent to a Bachelor's degree in computer science or related field;
    iv. Experience in design, implementation, security analysis, or testing of technologies or products involved in voting system; and
    v. Experience in the conduct and management of elections.
f. OEVT level of effort: test plan - In determining the level of effort to apply to open-ended vulnerability testing, the test lab **shall** take into consideration the size and complexity of the voting system; any available results from the "close ended" functional, security, and usability testing activities and laboratory analysis and testing activities; the number of vulnerabilities found in previous security analyses; and testing of the voting system and its prior versions.
g. OEVT level of effort: commitment of resources - The OEVT team **shall** examine the system for a minimum of 12 staff weeks.

7.5.3 Context of OEVT Testing

a. Context of testing - Open ended vulnerability testing shall be conducted within the context of a process model describing a specific implementation of the voting system and a corresponding model of plausible threats.
b. Adequate system model - The OEVT team shall verify that the manufacturer provided system model sufficiently describes the intended implementation of the voting system.
c. Adequate threat model - The OEVT team shall verify that the threat model sufficiently addresses significant threats to the voting system. Significant threats are those that could:
    i. Change the outcome of an election;
    ii. Interfere with voters' ability to cast ballots or have their votes counted during an election; or
    iii. Compromise the secrecy of vote.

OEVT team may modify the manufacturer's threat model to include additional, plausible threats.

7.5.4 Fail Criteria

a. OEVT fail criteria: violation of requirements - The voting device shall fail open ended vulnerability testing if the OEVT team finds vulnerabilities or errors in the voting device that violate requirements in the Standards. While the OEVT is directed at issues of device and system security, a violation of any requirement can lead to failure. The S-ATA **shall** report an OEVT failure if any of the following are found:
    i. Evidence that any single person can cause a violation of a voting system security goal (e.g., integrity of election results, privacy of the voter, availability of the voting system), assuming that all other parties follow procedures appropriate for their roles as specified in the manufacturer's documentation;
    ii. Manufacturer's documentation fails to adequately document all aspects of system design, development, and proper usage that are relevant to system security. This includes but is not limited to the following:
        - System security objectives;
        - Initialization, usage, and maintenance procedures necessary to secure operation;
        - All attacks the system is designed to resist or detect; and
        - Any security vulnerabilities known to the manufacturer.
    iii. Use of a cryptographic module that has not been validated against FIPS 140-2;
    iv. Ability to modify electronic event logs without detection;
    v. A VVPR that has an inaccurate or incomplete summary of the cast electronic vote;
    vi. Unidentified software on the voting system;
    vii. Identified software which lacks documentation of the functionality it provides to the voting device;
    viii. Access to configuration file without authentication;
    ix. Ability to cast more than one ballot within a voting session;
    x. Ability to perform restore operations in Activated State;
    xi. Enabled remote access in Activated State; and/or
    xii. Ballot boxes without appropriate tamper evidence countermeasures.
b. Threat model: failure - Voting systems shall fail open ended vulnerability testing if the manufacturer's model of the system along with associated use procedures and security controls does not adequately mitigate all significant threats as described in the threat model. The OEVT team may use a threat model that has been amended based on their findings in accordance with 7.5.~~4.~~3.~~c~~
c. OEVT fail criteria: critical flaws - The voting device shall fail open ended vulnerability testing if the OEVT team provides a plausible description of how vulnerabilities or errors found in a voting device or the implementation of its security features could be used to:
    i. Change the outcome of an election;

ii. Interfere with voters' ability to cast ballots or have their votes counted during an election; or
iii. Compromise the secrecy of vote without having to demonstrate a successful exploitation of said vulnerabilities or errors.

7.5.5 OEVT Reporting Requirements

a. OEVT reporting requirements - The OEVT team **shall** record all information discovered during the open-ended vulnerability test, including but not limited to:
    i. Names, organizational affiliations, summary qualifications, and resumes of the members of the OEVT;
    ii. Time spent by each individual on the OEVT activities;
    iii. List of hypotheses considered;
    iv. List of hypotheses rejected and rationale;
    v. List of hypotheses tested, testing approach, and testing outcomes; and
    vi. List and description of remaining vulnerabilities in the voting system:
        - A description of each vulnerability including how the vulnerability can be exploited and the nature of the impact;
        - For each vulnerability, the OEVT team should identify any Standards requirements violated; and
        - The OEVT team should flag those vulnerabilities as serious if the vulnerability can result in the violation of one or more Standards requirements; a change of the outcome of an election; or a denial of service (lack of availability) during the election.

7.6 Telecommunications and Data Transmission

There are four areas that must be addressed by telecommunications and data transmission security capabilities: access control, data integrity, detection and prevention of data interception, and protection against external threats.

7.6.1 Maintaining Data Integrity

Voting systems that use telecommunications to communicate between system components and locations are subject to the same security requirements governing access to any other system hardware, software, and data function.

a. Voting systems that use electrical or optical transmission of data **shall** ensure the receipt of valid vote records is verified at the receiving station. This should include standard transmission error detection and correction methods such as checksums or message digest hashes. Verification of correct transmission **shall** occur at the voting system application level and ensure that the correct data is recorded on all relevant components consolidated within the polling place prior to the voter completing casting of his or her ballot.
    i. Cryptography used to verify the receipt of vote records **shall** use NIST approved algorithms with security strength of at least 112 bits. Message Authentication Code (MAC) keys **shall** have a security strength of at least 112 bits.

7.6.2 Election Returns

If the voting system provides access to election returns or interactive inquiries, the system **shall**:

a. Allow authorized administrators the ability to disable or restrict access to election returns (for equipment that operates in a central counting environment). This requirement applies as well to polling place equipment that contains a removable memory module or that may be removed in its entirety to a central place for the consolidation of polling place returns
b. Design voting system software and its security environment such that data accessible to interactive queries resides in an external file or database created and maintained by the elections software under the restrictions applying to any other output report:
    i. The output file or database has no provision for write access back to the system
    ii. Persons whose only authorized access is to the file or database are denied write access, both to the file or database, and to the system

7.7 Voter Verifiable Paper Audit Trail Requirements

This section contains requirements for DREs with a Voter Verifiable Paper Audit Trail (VVPAT) component, henceforth referred to as VVPAT voting systems. A VVPAT voting system **shall** consist minimally of the following fundamental components:

- A voting device, on which a voter makes selections and prepares to cast a ballot;
- A printer that prints a paper record summary of the voter's ballot selections, and that allows the voter to compare it with the electronic ballot selections;
- A mechanism by which the voter may indicate acceptance or rejection of the paper record;
- Ballot box/cartridge to contain accepted and voided paper records; and
- A paper record for each electronic ballot image. The paper record may be printed on a separate sheet for each record ("cut-sheet VVPAT") or on a continuous paper roll ("paper-roll VVPAT").

These requirements will be applied for certification testing of DRE systems because California law requires DREs to provide VVPAT capability. The manufacturer's certification testing application must indicate whether the system being presented for testing includes this capability.

7.7.1 Display and Print a Paper Record

a. VVPAT voting systems **shall** provide capabilities for the voter to review a paper record of ballot selections and a summary of the voter's electronic ballot selections prior to casting a ballot.
b. VVPAT voting systems **shall** create a paper record that election officials can use to reconstruct the full set of totals from the election.
c. Each paper record **shall** contain a human-readable summary of the electronic ballot image record. In addition, all paper records **shall** contain audit-related information including:

i. Machine ID;
ii. Reporting context, such as precinct or election district;
iii. Ballot style;
iv. Date of election or date record printed; and
v. Complete summary of voter's choices.

7.7.2 Approve or Void the Paper Record

a. The VVPAT voting system format and presentation of the paper record and electronic summaries of ballot selections **shall** be designed to facilitate the voter's comparison between the electronic summaries of ballot selections displayed on the screen and the paper record.
b. When a voter indicates that the paper record is to be accepted, the VVPAT voting system **shall**:
    i. Immediately print an indication that the vote has been accepted, in view of the voter;
    ii. Electronically store the electronic ballot image record as a cast vote; and
    iii. Deposit the paper record into a secure receptacle.

c. When a voter indicates that the paper record is to be rejected, the VVPAT voting system **shall**:
    i. Immediately print an unambiguous indication that the vote has been rejected, in view of the voter;
    ii. Electronically store a record that the paper record was rejected; and
    iii. Deposit the rejected paper record into the secure receptacle.
d. The VVPAT voting system **shall** have the capacity to be configured to limit the number of times a single voter may reject a paper record without election official intervention. The VVPAT voting system **shall** support limits between zero (any rejected paper record requires election official intervention) to two times of rejections without election official intervention.
e. The VVPAT voting system **shall** have the capacity to limit the total number of paper records that a machine may reject before election official intervention is required. The VVPAT voting system **shall** have a default limit of two rejected paper records before election official intervention is required. The VVPAT voting system **shall** permit the setting of no limit, so that no number of total rejected paper records requires immediate election official intervention.
f. The VVPAT voting system **shall** have the capacity to be configured to remove any indication of the voter's choices from the screen when the configured limit of rejected paper records per voter or per machine is reached.
g. When a VVPAT voting system reaches a configured limit of rejected paper records per voter or per machine, it **shall** do the following:
    i. Place the paper record that has been rejected into the ballot box or other receptacle;
    ii. Clearly display that a paper record has been rejected and indicate the need for election official intervention; and
    iii. Suspend normal operations until re-enabled by an authorized election official.

7.7.3 Electronic and Paper Record Structure

a. Electronic ballot images **shall** be recorded in a randomized order by the voting system for the election. NIST Special Publication 800-90: Recommendation for Random Number Generation Using Deterministic Random Bit Generators specifies techniques for the generation of random numbers that can be used to randomize the order of ballot images in a cryptographically sound way. For each voted ballot, this includes:
   i. Ballot style and reporting context such as precinct or election district;
   ii. For each contest:
   iii. The choice recorded, including undervotes and write-ins; and
   iv. Any information collected by the vote-capture device electronically about each write-in;
   v. Information specifying whether the ballot is provisional, early voting or election day voting. Types of provisional ballots (such as "regular provisional", "extended hours provisional", and "regular extended hours") are jurisdiction-dependent.
   vi. Information linking the electronic ballot image to a paper record, if such functionality is enabled in the voting system.

b. The voting system **shall** provide the capability to export the collection of electronic ballot images in a publicly documented format, such as XML, or include a utility to export the records into a publicly documented format for offline viewing.

c. Electronic ballot images **shall** be digitally signed by the voting system. The digital signature **shall** be generated using a NIST-approved digital signature algorithm with a security strength of at least 112 bits implemented within a FIPS 140-2 validated cryptographic module operating in FIPS mode.

d. The human-readable contents of the paper record should be created in a manner that is machine-readable by optical character recognition.

e. Paper-roll VVPAT voting systems **shall** mark paper rolls with the following:
   i. Machine ID;
   ii. Reporting context, such as precinct or election district;
   iii. Date of election or date record printed;
   iv. If multiple paper rolls were produced during this election on this device, the number of the paper roll (e.g., Roll #2).

f. Paper-roll VVPAT voting systems **shall** include the following on each paper record:
   i. Ballot style;
   ii. Type of voting (e.g., provisional, early, etc.);
   iii. Complete summary of voter's choices;
   iv. For each ballot contest:
      - Contest name (e.g., "Governor");
      - Any additional information needed for unambiguous interpretation of the paper record;
      - An indication, if the contest was undervoted; and
      - An indication, if the choice is a write-in vote.
   v. An indication of whether the paper record has been accepted or rejected by the voter.

g. Paper-roll VVPAT voting systems **shall** not split paper records across rolls; each paper record must be contained in its entirety by the paper roll.
h. Cut-sheet VVPAT voting systems **shall** include the following on each paper record:
    i. Machine ID;
    ii. Reporting context, such as precinct or election district;
    iii. Date of election or date record printed;
    iv. Ballot style
    v. Type of voting (e.g., provisional, early, etc.);
    vi. Complete summary of voter's choices;
    vii. For each ballot contest:
        - Contest name (e.g., "Governor");
        - Any additional information needed for unambiguous interpretation of the paper record;
        - An indication, if the contest was undervoted; and
        - o An indication, if the choice is a write-in vote.
    viii. An indication of whether each sheet has been accepted or rejected by the voter.
i. If a cut-sheet VVPAT voting system splits paper records across multiple sheets of paper, each sheet **shall** include:
    i. Page number of this sheet and total number of sheets (e.g., page 1 of 4);
    ii. Ballot style
    iii. Reporting context, such as precinct or election district
    iv. An indication that the sheet's contents have been accepted or rejected by the voter; and
    v. Any correspondence information included to link the paper record to its corresponding electronic ballot image record.
j. If a cut-sheet VVPAT voting system splits paper record across multiple sheets of paper, it **shall** not split ballot contests across sheets.
k. If a cut-sheet VVPAT voting system splits paper records across multiple sheets of paper, the ballot choices on each sheet **shall** be submitted to the voter for verification separately according to the following:
    i. The voter **shall** be presented a verification screen for the contents of each sheet separately at the same time as the voter is able to verify the contents of the part of the paper record on the sheet;
    ii. When a voter accepts or rejects the contents of a sheet, the votes contained on that sheet and verification screen **shall** be committed to memory, regardless of the verification of any other sheet by the same voter;
    iii. Configurable limits on rejected paper records per voter **shall** count each rejected sheet as a rejected paper record;
    iv. Configurable limits on rejected paper records per machine **shall** not count more than one rejected paper record per voter; and
    v. When a rejected paper record requires election official intervention, the VVPAT voting system **shall** indicate which sheets have been accepted and which rejected.
l. The VVPAT voting system **shall** provide a capability to print information on each paper record sufficient for auditors to identify from an electronic ballot image record its corresponding paper record and from a paper records its corresponding

electronic ballot image. This capability **shall** be possible for election officials to enable or disable.

m. Any information on the paper record that identifies the corresponding electronic ballot image should not be practical for the voter to read or copy by hand.
n. The VVPAT voting system manufacturer **shall** include a capability for auditors to verify the correspondence between the electronic ballot image and paper record pairs, if the correspondence information is printed on the paper record.

7.7.4 Equipment Security and Reliability

a. The VVPAT printer **shall** be physically connected via a standard, publicly documented printer port using a standard communications protocol.
b. Tamper-evident seals or physical security measures **shall** protect the connection between the printer and the voting machine.
c. If the electronic connection between the voting machine and the printer has been broken or interrupted, the voting machine **shall** detect this event and record it in the system event log.
d. The VVPAT voting system **shall** detect printer errors that may prevent paper records from being correctly displayed, printed or stored, such as lack of consumables such as paper, ink, or toner, paper jams/misfeeds, and memory errors.
e. If a printer error or malfunction is detected, the VVPAT voting system **shall**:
    i. Present a clear indication to the voter and election officials of the malfunction. This must indicate clearly whether the current voter's vote has been cast, discarded, or is waiting to be completed;
    ii. Suspend voting operations until the problem is resolved;
    iii. Allow canceling of the current voter's electronic ballot image by election officials in the case of an unrecoverable error; and
    iv. Protect the privacy of the voter while the error is being resolved.
f. Procedures for recovery from printer errors on paper-roll VVPAT voting systems **shall** not expose the contents of previously cast paper records.
g. Paper-roll VVPAT voting systems **shall** be designed so that when the rolls are removed from the voting device according to the following:
    i. All paper records are contained inside the secure container;
    ii. The container supports being tamper-sealed and locked; and
    iii. The container supports being labeled with the device serial number, precinct, and other identifying information to support audits and recounts
h. If a continuous paper spool is used to store paper records, the manufacturer **shall** provide a mechanism for an auditor to unspool the paper, view each paper record in its entirety, and then respool the paper, without modifying the paper in any way.
i. The printer **shall** not be permitted to communicate with any system or machine other than the voting machine to which it is connected.
j. The printer **shall** only be able to function as a printer; it **shall** not contain any other services (e.g., provide copier or fax functions) or network capability.
k. Protective coverings intended to be transparent on voting equipment **shall** be maintainable via a predefined cleaning process. If the coverings become damaged such that they obscure the paper record, they **shall** be replaceable.

l. The paper record **shall** be of sufficient durability to remain unchanged for minimally 22 months to be used for verifications, reconciliations, and recounts conducted manually or by automated processing.

7.7.5 Preserving Voter Privacy

VVPAT records can be printed and stored by two different methods:

- Printed and stored on a continuous spool-to-spool paper roll where the voter views the paper record in a window
- Printed on separate pieces of paper, which are deposited in a secure receptacle.

If a requirement applies to only one method, that will be specified. Otherwise, the requirement applies to both.

a. Voter privacy **shall** be preserved during the process of recording, verifying and auditing his or her ballot selections.
b. When a VVPAT with a spool-to-spool continuous paper record is used, a means **shall** be provided to preserve the secrecy of the paper record of voter selections.
c. When a VVPAT with a spool-to-spool continuous paper record is used, no record **shall** be maintained of which voters used which voting machine or the order in which they voted.
d. The electronic and paper records **shall** be created and stored in ways that preserve the privacy of the voter.
e. The privacy of voters whose paper records contain an alternative language **shall** be maintained.
f. Both paper rolls and paper record secure receptacles **shall** be controlled, protected, and preserved with the same security as a ballot box.

7.7.6 VVPAT Usability

a. All usability requirements **shall** apply to voting machines with VVPAT.
b. The voting equipment **shall** be capable of showing the information on the paper in a font size of at least 3.0 mm and should be capable of showing the information in at least two font ranges; 3.0–4.0 mm, and 6.3–9.0 mm, under control of the voter or poll worker.
c. The voting equipment **shall** display, print and store the paper record in any of the written alternative languages chosen for the ballot.
    i. To assist with manual auditing, candidate names on the paper record **shall** be presented in the same language as used on the DRE summary screen.
    ii. Information on the paper record not needed by the voter to perform verification **shall** be in English. In addition to the voter ballot selections, the marking of the paper record as accepted or void, and the indication of the ballot page number need to be printed in the alternative language. Other information, such as precinct and election identifiers, **shall** be in English to facilitate use of the paper record for auditing.
d. The paper and electronic records **shall** be presented to allow the voter to read and compare the records without the voter having to shift his or her position.
e. If the paper record cannot be displayed in its entirety on a single page, each page of the record **shall** be numbered and **shall** include the total count of pages for the

record, e.g. “Page X of Y. A means **shall** be provided to allow the voter to view each page of the record.

f. The instructions for performing the verification process **shall** be made available to the voter in a location on the voting machine.

7.7.7 VVPAT Accessibility

a. If the normal voting procedure includes VVPAT, the accessible voting equipment should provide features that enable voters who are visually impaired and voters with an unwritten language to perform this verification. Since the California Elections Code designates the paper record produced by the VVPAT to be the official ballot or the determinative record on a recount, the accessible voting equipment **shall** provide features that enable visually impaired voters and voters with an unwritten language to review the paper record.

7.8 Testing - Security

The S-ATA **shall** design and perform test procedures that test the security capabilities of the voting system against the requirements. These procedures **shall** focus on the ability of the system to detect, prevent, log, and recover from the broad range of security risks identified. These procedures **shall** also examine system capabilities and safeguards claimed by the manufacturer in the TDP to go beyond these risks. The range of risks tested is determined by the design of the system and potential exposure to risk. Regardless of system design and risk profile, all systems **shall** be tested for effective access control and physical data security.

The S-ATA may meet these testing requirements by confirming proper implementation of proven commercial security software. In this case, the manufacturer must provide the published standards and methods used by the U.S. Government to test and accept this software, or it may provide references to free, publicly available publications of these standards and methods, such as government web sites.

At its discretion, the S-ATA may conduct or simulate attacks on the system to confirm the effectiveness of the system's security capabilities.

7.8.1 Access Control

The accredited testing laboratory **shall** conduct tests of system capabilities and review the access control policies and procedures submitted by the manufacturer to identify and verify the access control features implemented as a function of the system. For those access control features built in as components of the voting system, the S-ATA **shall** design tests to confirm that these security elements work as specified.

Specific activities to be conducted by the S-ATA **shall** include:

a. A review of the manufacturer’s access control policies, procedures and system capabilities to confirm that all requirements have been addressed completely

b. Specific tests designed by the S-ATA to verify the correct operation of all documented access control procedures and capabilities, including tests designed to circumvent controls provided by the manufacturer. These tests **shall** include:
    i. Performing the activities that the jurisdiction will perform in specific accordance with the manufacturer's access control policy and procedures to create a secure system, including procedures for software and firmware installation
    ii. Performing tests intended to bypass or otherwise defeat the resulting security environment. These tests **shall** include simulation of attempts to physically destroy components of the voting system in order to validate the correct operation of system redundancy and backup capabilities

This review applies to the full scope of system functionality. It includes functionality for defining the ballot and other pre-voting functions, as well as functions for casting and storing votes, vote canvassing, vote reporting, and maintenance of the system's audit trail.

7.8.2 Data Interception and Disruption

For systems that use telecommunications, as provided for in section 6 of the Standards and consistent with California law, to transmit official voting data, the S-ATA **shall** review, and conduct tests of, the data interception and prevention safeguards specified by the manufacturer in its TDP. The S-ATA **shall** evaluate safeguards provided by the manufacturer to ensure their proper operation, including the proper response to the detection of efforts to monitor data or otherwise compromise the system.

8 Quality Assurance and Configuration Management

The quality assurance and configuration management requirements discussed in this section help assure that voting systems conform to the requirements of the Standards. Quality Assurance is a manufacturer function with associated practices that is initiated prior to system development and continues throughout the maintenance life cycle of the voting system. Quality Assurance focuses on building quality into a system and reducing dependence on system tests at the end of the life cycle to detect deficiencies, thus helping ensure that the system:

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

Configuration management is a set of activities and associated practices that ensures full knowledge and control of the components of a system, starting with its initial development progressing through its ongoing maintenance and enhancement, and including its operational life cycle.

8.1 Standards Based Framework for Quality Assurance and Configuration Management

The requirement in this section establishes the quality assurance and configuration standards for a voting system to which manufacturers must conform. The requirement to develop a Quality and Configuration Management manual, and the detailed requirements on that manual.

a. Voting system manufacturers **shall** implement a quality assurance and configuration management program that is conformant with the recognized ISO standards in these areas:
   i. ISO 9000:2005;
   ii. ISO 9001:2000; and
   iii. ISO 10007:2003.

8.2 Configuration Management Requirements

This section specifies the key configuration management requirements for voting system manufacturers. The requirements include those of equipment tags and configuration logs. Continuation of the program, in the form of usage logs, is the responsibility of State and local officials.

a. Each voting system **shall** have an identification tag that is attached to the main body. The tag **shall** be tamper-resistant and difficult to remove. The tag **shall** contain the following information:

i. The voting system model identification in the form of a model number and possibly a model name. The model identification identifies the exact variant or version of the system;
ii. The serial number that uniquely identifies the system;
iii. Identification of the manufacturer, including address and contact information for technical service, and manufacturer certification information; and
iv. Date of manufacture of the voting system.
v. The system's power requirements, if applicable.

b. For each voting system manufactured, a Voting System Configuration Log **shall** be established. The Log is initialized by the configuration data supplied by the manufacturer. From that point on, it functions like a diary of the system. Entries are made by election officials whenever any change occurs. Every exception, disruption, anomaly, and every failure is recorded. Every time the cover is opened for inspection or a repair or maintenance is performed, an entry details what was done, and what component was changed against what other component, as well as any diagnosis of failures or exceptions. The Log **shall** be kept on a medium that allows the writing, but not the modification or deletion, of records. The Log **shall** contain the following information:
    i. The information on the system tag described in Requirement a;
    ii. The identification of all critical parts, components, and assemblies of the system; and
    iii. The complete historical record, as developed by the manufacturer per Requirement II.2.11.l, of all critical parts, components, and assemblies included in the voting system.

The list of critical parts, components, and assemblies should be consistent with the rules for determining which of these entities is critical, as specified in the Quality and Configuration Manual.

8.3 Quality and Configuration Management Manual

This section contains requirements on the content of the quality assurance and configuration management documentation that manufacturers must supply.

a. All voting system manufacturers **shall** develop and present to the Secretary of State a complete Quality and Configuration Management Manual (Manual). The Manual **shall** detail the manufacturer's Quality and Configuration Management processes and procedures required by the Standards. These processes and procedures **shall** conform to all requirements of the Standards.
b. The Manual **shall** declare that meeting the requirements of the entire Standards is a binding commitment for the entire manufacturer organization.
c. The Manual **shall** provide for the formulation of a project plan for the design and development of a voting system. It **shall** require the project plan to be clearly and unambiguously documented. The project plan should be consistent with the Design and Development Planning requirements, as specified in ISO 9001:2000, Quality management systems.

d. The Manual **shall** require the project plan to include, at a minimum, one quality check at the end of the design phase, and one quality check at the end of the development phase. The project plan **shall** define the progress that is required before each quality check can be passed. A "quality check" is the sum of the activities Design and Development Review, Design and Development Verification, and Design and Development Validation, as defined in ISO 9001:2000 Sections 7.3.4. through 7.3.6.
e. The Manual **shall** require the manufacturer to maintain a log in which all difficulties encountered during the design and development phase for a voting system are required to be recorded. Any remedial action taken to correct a difficulty **shall** also be recorded. The log **shall** be available for inspection by the Secretary of State or the S-ATA, upon request of the Secretary of State. "Difficulties" are any occasions when it is recognized that changes in past design decisions or in the project plan (see Requirement c) are necessary to complete the project.
f. The Manual **shall** specify rules that define what parts, components, and assemblies of the voting system are to be considered as critical. As used here, "components" include, but are not limited to, software modules. A part, component, or assembly **shall** be defined as critical if its failure may:
    i. Cause a faulty display of options;
    ii. Cause an uncertainty if voter's choice has been recorded;
    iii. Cause a false recording of vote cast;
    iv. Cause the change of stored votes;
    v. Cause the false transmission for polling station totals;
    vi. Cause injury to voters or staff;
    vii. Provide an opening for tampering;
    viii. Violate a voter's privacy;
    ix. Cause a false accumulation of polling station totals;
    x. Cause a false transmission for regional totals;
    xi. Give the appearance of irregularity;
    xii. Violate a voter's ability to vote independently; and
    xiii. Impede the usability of the polling station for all voters.
g. The Manual **shall** require that the design and development process of a voting system produce statements for every part, component, and assembly, whether to be manufactured by the manufacturer or obtained elsewhere, that impacts conformity to the Standards. These statements **shall** define verifiable requirements against which the part, component, or assembly can be tested at the end of its manufacturing process, or upon delivery, as appropriate. The requirements **shall** be defined in such a way that any part, component, or assembly that meets the requirements will provide the functionality and reliability required of it for the voting system to meet the overall functionality and reliability requirements specified in the Standards.
h. The Manual **shall** require that the design and development process define or identify processes by which all parts, components, and assemblies, defined as critical, of a voting system can be tested for compliance with requirements developed under Requirement g.

i. The Manual **shall** require that the design and development process of a voting system produce a statement that defines verifiable requirements against which any voting system can be tested at the end of its manufacturing and assembly process in such a way that passing the test provides assurance that the voting system meets all requirements defined in the Standards.
j. The Manual **shall** require that all purchased parts, components and assemblies, defined as critical, are tested according to the testing requirements developed under Requirement g and the processes developed under Requirement h before they are incorporated into a voting system. The records **shall** be maintained until such time as the certification of the voting system model expires or is revoked.
k. The Manual **shall** require that all manufactured parts, components, and assemblies, defined as critical, are tested according to the testing requirements developed under Requirement g and the processes developed under Requirement h before they are incorporated into a voting system. The records **shall** be maintained until such time as the certification of the voting system model expires or is revoked.
l. The Manual **shall** require that for each part, component, or assembly, whether purchased or manufactured by the manufacturer, that has been defined as critical (Requirement f), records **shall** be kept that document the complete history of the part, component, or assembly. These records **shall** be available for inspection. The records **shall** document:
    i. The source of raw materials;
    ii. The processes used in the manufacture;
    iii. The time when critical manufacturing steps were taken;
    iv. The organization or person that performed each critical manufacturing step, and
    v. The persons who performed the required inspections.
    vi. Any failures, discrepancies or anomalies that occurred during manufacture;
    vii. Any actions taken to correct the failure, discrepancy or anomaly; and
    viii. The final determination that the problem has been corrected.
m. The Manual **shall** require the manufacturer to identify and maintain the technical capability to monitor the in-service performance of each voting system sold throughout the life cycle of the voting system's model. For the purpose of this and subsequent requirements in this section, the term life cycle of a voting system model is defined as the time period from the delivery of the first voting system of that model to the time when the certification of the model expires or is revoked.
n. The Manual **shall** require the manufacturer to identify and maintain the technical capability to develop and implement remedies that are suitable to correct any defects that lead to in-service difficulties in all voting systems sold, throughout the life cycle of the voting system model.
o. The Manual **shall** require the manufacturer to identify and maintain the financial capability to provide product support, as defined in Requirements m and n, throughout the life cycle of the voting system model.

8.4 Examination of the Quality and Configuration Management Manual

Upon receipt, the Quality and Configuration Management Manual **shall** be reviewed for its fulfillment of Section 8.

8.5 Testing - Configuration Management

a. The S-ATA **shall** verify that the voting system has an identification tag attached to the main body.
b. The S-ATA **shall** verify that the voting system has associated with it a Configuration Log.

9. The Technical Data Package (TDP)

9.1 Scope

This section contains a description of the documentation relating to the voting system that **shall** be submitted with the system as a precondition of testing. These items are necessary to define the product and its method of operation; to provide technical and test data supporting the claims of the system's functional capabilities and performance levels; and to document instructions and procedures governing system operation and field maintenance. Any information relevant to the system evaluation **shall** be submitted to include source code, object code, and sample output report formats.

Both formal documentation and notes of the system development process **shall** be submitted for qualification tests. Documentation describing the system development process permits assessment of the efforts to develop and test the system and correct defects. Inspection of this process also enables the design of a more precise test plan. If the manufacturer's developmental test data are incomplete, the S-ATA **shall** design and conduct the appropriate tests to cover all elements of the system and to ensure conformance with all system requirements.

9.1.1 Content and Format

The content of the Technical Data Package (TDP) is intended to provide clear, complete descriptions of the following information about the system:

a. Overall system design, including subsystems, modules and the interfaces among them
b. Specific functional capabilities provided by the system
c. Performance and design specifications
d. Design constraints, applicable standards, and compatibility requirements
e. Personnel, equipment, and facility requirements for system operation, maintenance, and logistical support
f. Manufacturer practices for assuring adherence to system quality during the system’s development and subsequent maintenance

A list of all documents submitted **shall** be provided. Documents **shall** be listed in order of precedence.

9.1.1.1 Required Content for Initial Certification

a. Technical Data Package, main part - The main part of the TDP is relevant for conformity assessment and certification. Information that is also relevant to end users of the voting system should be included in the voting equipment user documentation.

Since the user documentation is part of the TDP submission, information appearing in the user documentation need not be repeated in the main part of the TDP. Manufacturers are encouraged to cite specific sections of the user documentation whenever they are responsive to requirements. However, if the manufacturer finds that repeating certain information in the main part of the TDP helps with its clarity or flow, there is no prohibition on doing so.

The main part of the TDP **shall** follow the format outlined below. The details of the content **shall** be as specified by the pertinent requirements of the Standards.

i. Implementation Statement - Formal declaration of which standard options were implemented in the system, as defined in the Conformance Clause.
ii. System Hardware Specification - Detailed specifications of the non-COTS hardware components of the system, including hardware characteristics, design, and construction. Precise identification of all COTS hardware that is included.
iii. Application Logic Design and Specification - Detailed specifications of all non-COTS software, firmware, and hardwired logic in the system. Precise identification of all COTS software, firmware, and hardwired logic that is included.
    - Overview
    - Standards and conventions
    - Operating environment
    - Functional specification
    - Programming specifications
    - System database
    - Interfaces
iv. System Security Specification - Addresses the security requirements of the Standards.
    - Design and Interface Specification - Provides a high-level design of the overall voting system and of each voting system component. It **shall** also describe external interfaces (programmatic, human, and network) provided by each of the computer components of the voting system (examples of components are DRE, Central Tabulator, Independent Audit machine).
    - Security Architecture - Documents an architecture level description of how the security requirements are met, and includes the various authentication, access control, audit, confidentiality, integrity, and availability requirements.
    - Development Environment Specification - Provide descriptions of the physical, personnel, procedural, and technical security of the development environment including configuration management, tools used, coding standards used, software engineering model used, and description of developer and independent testing.
    - Security Threats Controls - Identifies the threats the voting system protects against and the implemented security controls on voting

system and system components.
    - Security Testing and Vulnerability Analysis Documentation - Documents and describes security tests performed to identify vulnerabilities and the results of the testing. This also includes testing performed as part of software development, such as unit, module, and subsystem testing.
  v. System Test Specification - Development tests, usability test reports, etc.
  vi. System Change Notes - If the system under test is a revision of a previously tested system, the manufacturer shall supply detailed specifications of the changes that occurred.
  vii. Configuration for Testing - The configuration actions necessary to obtain conforming behavior from the voting system.
  viii. A copy of the Quality and Configuration Management Manual previously submitted to the SOS.

b. Voting equipment user documentation - The voting equipment user documentation is part of the TDP submission. However, unlike the main part of the TDP, it is ultimately intended to be delivered to end users of the voting system. Its formatting and production values should therefore reflect that end users form the target audience. The following topics **shall** be covered in the voting equipment user documentation:
  i. System Overview
  ii. System Functionality Description
  iii. System Security Manual
    - Access control
    - System event logging
    - Software installation
    - Setup inspection
    - Communications
    - Voter Verifiable Paper Audit Trail (VVPAT)
    - Physical security
    - Audit
  iv. System Operations Manual
    - Introduction
    - Operational environment
    - System installation and test specification
    - Operational features
    - Operating procedures
    - Documentation for poll workers
    - Operations support
    - Transportation and storage
  v. System Maintenance Manual
    - Introduction
    - Maintenance procedures
    - Maintenance equipment
    - Parts and materials
    - Maintenance facilities and support
  vi. Personnel Deployment and Training Requirements

9.1.1.2 Required Content for System Changes and Re-certification

For systems seeking re-certification, manufacturers **shall** submit System Change Notes, as well as current versions of all documents that have been updated to reflect system changes.

Manufacturers may also submit other information relevant to the evaluation of the system, such as test documentation, and records of the system's performance history, failure analysis and corrective actions.

9.1.1.3 Format

The requirements for formatting the TDP are general in nature; specific format details are of the manufacturer's choosing. The TDP **shall** include a detailed table of contents for the required documents, an abstract of each document and a listing of each of the informational sections and appendices presented. A cross-index **shall** be provided indicating the portions of the documents that are responsive to documentation requirements for any item presented.

9.1.2 Protection of Proprietary Information

The manufacturer is responsible for identifying any document or portion of a document that it believes is protected from release by State law. Manufacturers **shall** identify protected information by taking the following actions:

a. *Submitting a Notice of Protected Information*. This notice **shall** identify the document, document page, or portion of a page that the manufacturer believes should be protected from release. This identification must be done with specificity. For each piece of information identified, the manufacturer must state the legal basis for its protected status.
   i. Cite the applicable law that exempts the information from release.
   ii. Clearly discuss why that legal authority applies and why the document must be protected from release.
   iii. If necessary, provide additional documentation or information. For example, if the manufacturer claims a document contains confidential commercial information, it would also have to provide evidence and analysis of the competitive harm that would result upon release.

b. *Labeling Submissions*. Label all submissions identified in the notice as "Proprietary Commercial Information." Label only those submissions identified as protected. Attempts to indiscriminately label all materials as proprietary will render the markings moot.

9.2 System Overview

In the system overview, the manufacturer **shall** provide information that enables the S-ATA to identify the functional and physical components of the system, how the components are structured, and the interfaces between them.

9.2.1 System Description

The system description **shall** include written descriptions, drawings and diagrams that present:

a. A description of the functional components (or subsystems) as defined by the manufacturer (e.g., environment, election management and control, vote recording, vote conversion, reporting, and their logical relationships)
b. A description of the operational environment of the system that provides an overview of the hardware, software, and communications structure
c. A concept of operations that explains each system function, and how the function is achieved in the design
d. Descriptions of the functional and physical interfaces between subsystems and components
e. Identification of all COTS hardware and software products and communications services used in the development and/or operation of the voting system, identifying the name, manufacturer, and version used for each such component, including:
    i. Operating systems
    ii. Compilers and interpreters
    iii. Database software
f. Interfaces among internal components, and interfaces with external systems. For components that interface with other components for which multiple products may be used, the TDP **shall** provide an identification of:
    i. File specifications, data objects, or other means used for information exchange
    ii. The public standard used for such file specifications, data objects, or other means
g. Benchmark directory listings for all software (including firmware elements) and associated documentation included in the manufacturer's release in the order in which each piece of software would normally be installed upon system setup and installation

9.2.2 System Performance

The manufacturer **shall** provide system performance information including:

a. The performance characteristics of each operating mode and function in terms of expected and maximum speed, throughput capacity, maximum volume

(maximum number of voting positions and maximum number of ballot styles supported), and processing frequency
b. Quality attributes such as reliability, maintainability, availability, usability, and portability
c. Provisions for safety, security, privacy, and continuity of operation
d. Design constraints, applicable standards, and compatibility requirements
e. For optical scanners, the specification of what constitutes a reliably detectable mark versus a marginal mark. The specification may be parameterized by configuration values and should state the uncertainty.

9.3 System Functionality Description

The manufacturer **shall** declare the scope of the system's functional capabilities, thereby establishing the performance, design, test, manufacture, and acceptance context for the system.

The manufacturer **shall** provide a listing of the system's functional processing capabilities, encompassing capabilities required by the Standards and any additional capabilities provided by the system. This listing **shall** provide a simple description of each capability. Detailed specifications **shall** be provided in other documentation required for the TDP.

a. The manufacturer **shall** organize the presentation of required capabilities in a manner that corresponds to the structure and sequence of functional capabilities.
b. Additional capabilities **shall** be clearly indicated. They may be presented using the same structure as that used for required capabilities (i.e., overall system capabilities, pre-voting functions, voting functions, post-voting functions), or may be presented in another format of the manufacturer's choosing
c. Required capabilities that may be bypassed or deactivated during installation or operation by the user **shall** be clearly indicated
d. Additional capabilities that function only when activated during installation or operation by the user **shall** be clearly indicated
e. Additional capabilities that normally are active but may be bypassed or deactivated during installation or operation by the user **shall** be clearly indicated

9.4 System Hardware Specification

The manufacturer **shall** expand on the system overview by providing detailed specifications of the hardware components of the system, including specifications of hardware used to support the telecommunications capabilities of the system, if applicable.

9.4.1 System Hardware Characteristics

The manufacturer **shall** provide a detailed discussion of the characteristics of the system, indicating how the hardware meets individual requirements including:

Performance characteristics: This discussion addresses basic system performance attributes and operational scenarios that describe the manner in which system functions are invoked, describe environmental capabilities, describe life expectancy, and describe any other essential aspects of system performance

Physical characteristics: This discussion addresses suitability for intended use, requirements for transportation and storage, health and safety criteria, security criteria, and vulnerability to adverse environmental factors

Reliability: This discussion addresses system and component reliability stated in terms of the system's operating functions, and identification of items that require special handling or operation to sustain system reliability. The manufacturer **shall** include in the TDP a reliability analysis, such as a failure modes and effects analysis (FMEA), that satisfies the requirements.

Environmental conditions: This discussion addresses the ability of the system to withstand natural environments, and operational constraints in normal and test environments, including all requirements and restrictions regarding electrical service, telecommunications services, environmental protection, and any additional facilities or resources required to install and operate the system

9.4.2 Design and Construction

The manufacturer **shall** provide sufficient data, or references to data, to identify unequivocally the details of the system configuration submitted for testing. The manufacturer **shall** provide a list of materials and components used in the system and a description of their assembly into major system components and the system as a whole. Paragraphs and diagrams **shall** be provided that describe:

a. Materials, processes, and parts used in the system, their assembly, and the configuration control measures to ensure compliance with the system specification
b. The electromagnetic environment generated by the system
c. Operator and voter safety considerations, and any constraints on system operations or the use environment
d. Human factors considerations, including provisions for access by disabled voters

9.5 Software Design and Specification

The manufacturer **shall** expand on the system overview by providing detailed specifications of the software components of the system, including software used to support the telecommunications capabilities of the system, if applicable.

9.5.1 Purpose and Scope

The manufacturer **shall** describe the function or functions that are performed by the software programs that comprise the system, including software used to support the telecommunications capabilities of the system, if applicable.

9.5.2 Applicable Documents

The manufacturer **shall** list all documents controlling the development of the software and its specifications. Documents **shall** be listed in order of precedence.

9.5.3 Software Overview

The manufacturer **shall** provide an overview of the software that includes the following items:

a. A description of the software system concept, including specific software design objectives, and the logic structure and algorithms used to accomplish these objectives
b. The general design, operational considerations, and constraints influencing the design of the software
c. Identification of all software items, indicating items that were:
    i. Written in-house
    ii. Procured and not modified
    iii. Procured and modified, including descriptions of the modifications to the software and to the default configuration options
d. Additional information for each item that includes:
    i. Item identification
    ii. General description
    iii. Software requirements performed by the item
    iv. Identification of interfaces with other items that provide data to, or receive data from, the item
    v. Concept of execution for the item

The manufacturer **shall** also include a certification that procured software items were obtained directly from the manufacturer or a licensed dealer or distributor.

9.5.4 Software Standards and Conventions

The manufacturer **shall** provide information that can be used by the SOS and S-ATA to support software analysis and test design. The information **shall** address standards and conventions developed internally by the manufacturer as well as published industry standards that have been applied by the manufacturer. The manufacturer **shall** provide information that addresses the following standards and conventions:

a. Software System development methodology
b. Software design standards, including internal manufacturer procedures
c. Software specification standards, including internal manufacturer procedures
d. Software coding standards, including internal manufacturer procedures
e. Testing and verification standards, including internal manufacturer procedures, that can assist in determining the program's correctness and ACCEPT/REJECT criteria
f. Quality assurance standards or other documents that can be used to examine and test the software. These documents include standards for program flow and control charts, program documentation, test planning, and test data acquisition and reporting

9.5.5 Software Operating Environment

This section **shall** describe or make reference to all operating environment factors that influence the software design.

9.5.5.1 Hardware Environment and Constraints

The manufacturer **shall** identify and describe the hardware characteristics that influence the design of the software, such as:

a. The logic and arithmetic capability of the processor
b. Memory read-write characteristics
c. External memory device characteristics
d. Peripheral device interface hardware
e. Data input/output device protocols
f. Operator controls, indicators, and displays

9.5.5.2 Software Environment

The manufacturer **shall** identify the compilers or assemblers used in the generation of executable code, identify the interpreters used to run interpreted code, and describe the operating system or system monitor.

9.5.6 Software Functional Specification

The manufacturer **shall** provide a description of the operating modes of the system and of software capabilities to perform specific functions.

9.5.6.1 Configurations and Operating Modes

The manufacturer **shall** describe all software configurations and operating modes of the system, such as ballot preparation, election programming, preparation for opening the polling place, recording votes and/or counting ballots, closing the polling place, and

generating reports. For each software function or operating mode, the manufacturer **shall** provide:

a. A definition of the inputs to the function or mode (with characteristics, tolerances or acceptable ranges, as applicable)
b. An explanation of how the inputs are processed
c. A definition of the outputs produced (again, with characteristics, tolerances, or acceptable ranges, as applicable)

9.5.6.2 Software Functions

The manufacturer **shall** describe the software's capabilities or methods for detecting or handling:

a. Exception conditions
b. System failures
c. Data input/output errors
d. Error logging for audit record generation
e. Production of statistical ballot data
f. Data quality assessment
g. Security monitoring and control

9.5.7 Programming Specifications

The manufacturer **shall** provide in this section an overview of the software design, its structure, and implementation algorithms and detailed specifications for individual software modules.

9.5.7.1 Programming Specifications Overview

This overview **shall** include such items as flowcharts, data flow diagrams, and other graphical techniques that facilitate understanding of the programming specifications. This section **shall** be prepared to facilitate understanding of the internal functioning of the individual software modules. Implementation of the functions **shall** be described in terms of the software architecture, algorithms, and data structures.

9.5.7.2 Programming Specifications Details

The programming specifications **shall** describe individual software modules and their component units, if applicable. For each module and unit, the manufacturer **shall** provide the following information:

a. Module and unit design decisions, if any, such as algorithms used
b. Any constraints, limitations, or unusual features in the design of the software module or unit

c. The programming language used and rationale for its use, if other than the specified module or unit language
d. If the software module or unit consists of, or contains, procedural commands (such as menu selections in a database management system for defining forms and reports, on-line queries for database access and manipulation, input to a graphical user interface builder for automated code generation, commands to the operating system, or shell scripts), a list of the procedural commands and reference to user manuals or other documents that explain them
e. If the software module or unit contains, receives, or outputs data, a description of its inputs, outputs, and other data elements as applicable. Data local to the software module or unit **shall** be described separately from data input to, or output from, the software module or unit
f. If the software module or unit contains logic, the logic to be used by the software unit, including, as applicable:
    i. Conditions in effect within the software module or unit when its execution is initiated
    ii. Conditions under which control is passed to other software modules or units
    iii. Response and response time to each input, including data conversion, renaming, and data transfer operations
    iv. Sequence of operations and dynamically controlled sequencing during the software module's or unit's operation, including:
        - The method for sequence control
        - The logic and input conditions of that method, such as timing variations, priority assignments
        - Data transfer in and out of memory
        - The sensing of discrete input signals, and timing relationships between interrupt operations within the software module or unit
g. Exception and error handling
h. If the software module is a database, provide the information described in Subsection 9.5.8

9.5.8 System Database

The manufacturer **shall** identify and provide a diagram and narrative description of the system's databases, and any external files used for data input or output. The information provided **shall** include for each database or external file:

a. The number of levels of design and the names of those levels (such as conceptual, internal, logical, and physical)
b. Design conventions and standards (which may be incorporated by reference) needed to understand the design
c. Identification and description of all database entities and how they are implemented physically (e.g., tables, files)
d. Entity relationship diagrams and description of relationships
e. Details of table, record or file contents (as applicable) to include individual data

elements and their specifications, including:
   i. Names/identifiers
   ii. Data type (alphanumeric, integer, etc.)
   iii. Size and format (such as length and punctuation of a character string)
   iv. Units of measurement (such as meters, dollars, nanoseconds)
   v. Range or enumeration of possible values (such as 0-99)
   vi. Accuracy (how correct) and precision (number of significant digits)
   vii. Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether business rules apply
   viii. Security and privacy constraints
   ix. Sources (setting/sending entities) and recipients (using/receiving entities)
f. For external files, a description of the procedures for file maintenance, management of access privileges, and security

9.5.9 Interfaces

The manufacturer **shall** identify and provide a complete description of all internal and external interfaces, using a combination of text and diagrams.

9.5.9.1 Interface Identification

For each interface identified in the system overview, the manufacturer **shall**:

a. Provide a unique identifier assigned to the interface
b. Identify the interfacing entities (systems, configuration items, users, etc.) by name, number, version, and documentation references, as applicable
c. Identify which entities have fixed interface characteristics (and therefore impose interface requirements on interfacing entities) and which are being developed or modified (thus having interface requirements imposed on them)

9.5.9.2 Interface Description

For each interface identified in the system overview, the manufacturer **shall** provide information that describes:

a. The type of interface (such as real-time data transfer, storage-and-retrieval of data) to be implemented
b. Characteristics of individual data elements that the interfacing entity(ies) will provide, store, send, access, receive, etc., such as:
   i. Names/identifiers
   ii. Data type (alphanumeric, integer, etc.)
   iii. Size and format (such as length and punctuation of a character string)
   iv. Units of measurement (such as meters, dollars, nanoseconds)
   v. Range or enumeration of possible values (such as 0-99)
   vi. Accuracy (how correct) and precision (number of significant digits)

vii. Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether business rules apply
viii. Security and privacy constraints
ix. Sources (setting/sending entities) and recipients (using/receiving entities)

c. Characteristics of communication methods that the interfacing entity(ies) will use for the interface, such as:
   i. Communication links/bands/frequencies/media and their characteristics
   ii. Message formatting
   iii. Flow control (such as sequence numbering and buffer allocation)
   iv. Data transfer rate, whether periodic/aperiodic, and interval between transfers
   v. Routing, addressing, and naming conventions
   vi. Transmission services, including priority and grade
   vii. Safety/security/privacy considerations, such as encryption, user authentication, compartmentalization, and auditing
d. Characteristics of protocols the interfacing entity(ies) will use for the interface, such as:
   i. Priority/layer of the protocol
   ii. Packeting, including fragmentation and reassembly, routing, and addressing
   iii. Legality checks, error control, and recovery procedures
   iv. Synchronization, including connection establishment, maintenance, termination
   v. Status, identification, and any other reporting features
e. Other characteristics, such as physical compatibility of the interfacing entity(ies) (such as dimensions, tolerances, loads, voltages and plug compatibility)

9.5.10 Appendices

The manufacturer may provide descriptive material and data supplementing the various sections of the body of the Software Specifications. The content and arrangement of appendices **shall** be at the discretion of the manufacturer. Topics recommended for amplification or treatment in appendix form include:

Glossary: A listing and brief definition of all software module names and variable names, with reference to their locations in the software structure. Abbreviations, acronyms, and terms should be included, if they are either uncommon in data processing and software development or are used in an unorthodox semantic

References: A list of references to all related manufacturer documents, data, standards, and technical sources used in software development and testing

Program Analysis: The results of software configuration analysis algorithm analysis and selection, timing studies, and hardware interface studies that are reflected in the final software design and coding

9.6 System Security Specification

Manufacturers **shall** document in the TDP all aspects of system design, development, and proper usage that are relevant to system security. This includes, but is not limited to the following:

a. System security specification that addresses the security requirements
b. The means used to keep the security capabilities of the system current to respond to evolving threats
c. Specific security risks addressed by the system
d. All hardware and software security mechanisms
e. Development procedures employed to ensure absence of malicious code
f. Initialization, usage, and maintenance procedures necessary to secure operation
g. All attacks the system is designed to resist or detect
h. Any security vulnerabilities known to the manufacturer

Manufacturers **shall** provide at a minimum the following high-level documents:

i. Design and Interface Specification: This document **shall** identify the threats the voting system protects against. This document **shall** provide a high-level design of the overall voting system and of each voting system component. It **shall** also describe external interfaces (programmatic, human, and network) provided by each of the computer components of the voting system (examples of components are DRE, Central Tabulator, Independent Audit machine).
j. Security Architecture: This document **shall** provide an architecture level description of how the security requirements are met, and **shall** include the various authentication, access control, audit, confidentiality, integrity, and availability requirements.
k. Development Environment Specification: This document **shall** provide descriptions of the physical, personnel, procedural, and technical security of the development environment including version control, tools used, coding standards used, software engineering model used, and description of developer and independent testing.
l. Security Threat Analysis: This document **shall** identify the threats the voting system protects against and the implemented security controls on voting system and system components.
m. Security Testing and Vulnerability Analysis Documentation: These documents **shall** describe security tests performed to identify vulnerabilities and the results of the testing. This also includes testing performed as part of software development, such as unit, module, and subsystem testing.

Information provided by the manufacturer in this section of the TDP may be duplicative of information required by other sections. Manufacturers may cross reference to the relevant information in other sections if the means used provides a clear mapping to the requirements of this section. Information submitted by the manufacturer **shall** be used to assist in developing and executing the system certification test plan.

9.6.1 Access Control

a. Manufacturers **shall** provide user and TDP documentation of access control capabilities of the voting system.
b. Manufacturers **shall** provide descriptions and specifications of all access control mechanisms of the voting system including management capabilities of authentication, authorization, and passwords in the TDP.
c. Manufacturers **shall** provide descriptions and specifications of methods to prevent unauthorized access to the access control mechanisms of the voting system in the TDP.
d. Manufacturers **shall** provide descriptions and specifications of all other voting system mechanisms that are dependent upon, support, and interface with access controls in the TDP.
e. Manufacturers **shall** provide a list of all of the operations possible on the voting system and list the default roles that have permission to perform each such operation as part of the TDP.

9.6.1.1 Access Control Policy

The manufacturer **shall** specify the features and capabilities of the access control policy recommended to purchasing jurisdictions to provide effective voting system security. The access control policy **shall** address the general features and capabilities and individual access privileges.

9.6.1.2 Access Control Measures

The manufacturer **shall** provide a detailed description of all system access control measures and mandatory procedures designed to permit access to system states in accordance with the access policy, and to prevent all other types of access to meet the specific requirements.

9.6.2 Equipment and Data Security

The manufacturer **shall** provide a detailed description of system capabilities and mandatory procedures for purchasing jurisdictions to prevent disruption of the voting process and corruption of voting data to meet the specific requirements. This information **shall** address measures for polling place security and central count location security.

9.6.3 Software Installation and Security

a. The manufacturer **shall** provide a detailed description of the system capabilities and mandatory procedures for purchasing jurisdictions to ensure secure software (including firmware) installation to meet specific requirements. This information **shall** address software installation for all system components.
b. Manufacturers **shall** provide a list of all software related to the voting system in

the technical data package (TDP).

c. Manufacturers **shall** provide at a minimum in the TDP the following information for each piece of software related to the voting system: software product name, software version number, software manufacturer name, software manufacturer contact information, type of software (application logic , border logic , third party logic, COTS software, or installation software), list of software documentation, component identifier(s) (such as filename(s)) of the software, type of software component (executable code, source code, or data).
d. As part of the TDP, manufacturers **shall** provide the location (such as full path name or memory address) and storage device (such as type and part number of storage device) where each piece of software is installed on the voting system.
e. As part of the TDP, manufacturers **shall** document the functionality provided to the voting system by the installed software.
f. As part of the TDP, manufacturers **shall** map the dependencies and interactions between software installed on the voting system.
g. The manufacturer **shall** provide a detailed description of the system capabilities and mandatory procedures for purchasing jurisdictions used to provide protection against threats to third party products and services.

9.6.3.1 Air Gap

The TDP for the voting system **shall** provide full procedures and instructions, to be incorporated into the Official Use Procedures for the voting system, to implement the segregated dual-installation architecture. Those procedures and instructions **shall**:

a. Require elections officials to use the permanent installation to lay out the ballot, define the election, and program all of the memory cards, including any DRE, ballot marking device, optical scan unit, etc.
b. Require elections officials to write a backup of the election database from the permanent installation onto write-once media (e. g., CD-R or DVD-R), carry the media by hand to the sacrificial installation, and install that database onto the sacrificial installation. After this point, the permanent installation **shall not** be used for the remainder of the election.
c. Require that, after the close of the polls, memory cards or other equipment containing votes returned from polling locations are uploaded to the sacrificial installation (not the permanent installation).
d. Require that the sacrificial installation, not the permanent installation, is used to accumulate and tabulate election results, produce reports, and calculate the official election results.
e. Require that the "sacrificial" installation is treated as presumed-to-be-infected, so any machine or equipment that is ever connected to the sacrificial installation must never again be connected to the permanent installation.
f. Ensure that any media that has been connected to the sacrificial installation is securely erased or reformatted before being used with the permanent installation.

g. Require that after an election has been held and before the next election, system administrators reformat and reinstall all the software on the sacrificial installation server, optical scanners and DREs, to bring up a clean sacrificial installation.
h. Require, after the canvass is completed, that all memory cards used in optical scanners and DREs in the field are erased and reformatted using a separate laptop (not connected to either installation) that is used only for this purpose.

9.6.4 System Event Logging

a. Manufacturers **shall** provide TDP documentation of event logging capabilities of the voting devices.
b. Manufacturers **shall** provide a technical data package that describes system event logging design and implementation.
c. The technical data package **shall** provide the location (i.e. full path name or memory address) where each log is saved.

9.6.5 Physical Security

a. Manufacturers **shall** provide a list of all voting system components to which access must be restricted and a description of the function of each said component.
b. As part of the TDP, manufacturers **shall** provide a listing of all ports and access points of the voting system.
c. For each physical lock used on a voting system, manufacturers **shall** document whether the lock was installed to secure an access point.
d. Manufacturers **shall** provide a list of all physical security countermeasures that require power supplies.
e. Manufacturers **shall** provide a technical data package that documents the design and implementation of all physical security controls for the voting system.

9.6.6 Setup Inspection

a. Manufacturers **shall** provide the technical specifications of how voting systems identify installed software in the TDP.
b. Manufacturers **shall** provide a technical specification of how the integrity of software installed on the voting system is verified as part of the TDP. Software integrity verification techniques used to support the integrity verification of software installed on voting systems needs to be able to detect the modification of software.
c. Manufacturers **shall** provide a technical specification of how the inspection of all the voting system registers and variables is implemented by the voting device in the TDP

9.6.7 Cryptography

a. Manufacturers **shall** provide a list of all cryptographic algorithms and key sizes supported by the voting system.
b. Manufacturers **shall** provide the technical specification of all cryptographic protocols supported by the voting system.
c. Manufacturers **shall** provide the cryptographic module name, identification information (such as hardware/firmware/software name, model name, and revision/version number) and NIST FIPS 140-2 validation certificate number for all cryptographic modules that implement the cryptographic algorithms of the voting systems.
d. Manufacturers **shall** map the cryptographic modules to the voting system functions the modules support. This requirement documents the actions of the voting system that invoke the cryptographic module.
e. When public key information is stored in a digital certificate (such as an X.509 certificate), manufacturers **shall** provide a description of all the certificate fields (such as names, algorithm, expiration date, etc.) including the default values for the voting system. If they exist, manufacturers **shall** provide any certificate policies associated with the digital certificate.
f. Manufacturers **shall** provide documentation describing how cryptographic keys are created, stored, imported/exported, and deleted by the voting system.

9.6.8 Telecommunications and Data Transmission Security

The manufacturer **shall** provide a detailed description of the system capabilities and mandatory procedures for purchasing jurisdictions to ensure secure data transmission to meet specific requirements:

a. For all systems, this information **shall** address access control, and prevention of data interception

9.6.9 Other Elements of an Effective Security Program

The manufacturer **shall** provide a detailed description of the following additional procedures required for use by the purchasing jurisdiction:

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

This documentation **shall** be prepared such that these requirements can be integrated by the jurisdiction into local administrative and operating procedures.

9.7 System Test and Verification Specification

The manufacturer **shall** provide test and verification specifications for development test specifications.

9.7.1 Development Test Specifications

a. The manufacturer **shall** describe the plans, procedures, and data used during software development and system integration to verify system logic correctness, data quality, and security.
b. This description **shall** include test identification and design, including:
    i. Test structure
    ii. Test sequence or progression
    iii. Test conditions
c. Standard test procedures, including any assumptions or constraints
d. Special purpose test procedures including any assumptions or constraints
e. Test data; including the data source, whether it is real or simulated, and how test data are controlled
f. Expected test results
g. Criteria for evaluating test results

The details of this description **shall** be as specified in the manufacturer's Quality and Configuration Management Manual. In the event that test data are not available, the S-ATA **shall** design test cases and procedures equivalent to those ordinarily used during product verification.

9.7.2 Test Specifications

The manufacturer **shall** provide specifications for verification and validation of overall software performance. These specifications **shall** cover:

a. Control and data input/output
b. Acceptance criteria
c. Processing accuracy
d. Data quality assessment and maintenance
e. Ballot interpretation logic
f. Exception handling
g. Security
h. Production of audit trails and statistical data

The specifications **shall** identify procedures for assessing and demonstrating the suitability of the software for election use.

9.8 System Operations Procedures

This documentation **shall** provide all information necessary for system use by all personnel who support pre-election and election preparation, polling place activities and central counting activities, as applicable, with regard to all system functions and operations identified. The nature of the instructions for operating personnel will depend upon the overall system design and required skill level of system operations support personnel.

The system operations procedures **shall** contain all information that is required for the preparation of detailed system operating procedures, and for operator training, as described below.

9.8.1 Introduction

The manufacturer **shall** provide a summary of system operating functions and modes, in sufficient detail to permit understanding of the system's capabilities and constraints. The roles of operating personnel **shall** be identified and related to the operating modes of the system. Decision criteria and conditional operator functions (such as error and failure recovery actions) **shall** be described.

The manufacturer **shall** also list all reference and supporting documents pertaining to the use of the system during election operations.

9.8.2 Operational Environment

The manufacturer **shall** describe the system environment, and the interface between the user or operator and the system. The manufacturer **shall** identify all facilities, furnishings, fixtures, and utilities that will be required for equipment operations, including equipment that operates at the:

a. Polling place
b. Central count facility
c. Other locations

9.8.3 System Installation and Test Specification

The manufacturer **shall** provide specifications for validation of system installation, acceptance, and readiness. These specifications **shall** address all components of the system and all locations of installation (e.g., polling place, central count facility), and **shall** address all elements of system functionality and operations identified including:

a. Pre-voting functions
b. Voting functions
c. Post-voting functions
d. General capabilities

These specifications also serve to provide guidance to the procuring agency in developing its acceptance test plan and procedures according to the agency's contract provisions, and the election laws of the state.

9.8.4 Operational Features

The manufacturer **shall** provide documentation of system operating features that meets the following requirements:

a. A detailed description of all input, output, control, and display features accessible to the operator or voter
b. Examples of simulated interactions to facilitate understanding of the system and its capabilities
c. Sample data formats and output reports
d. Illustrate and describe all status indicators and information messages

9.8.5 Operating Procedures

The manufacturer **shall** provide documentation of system operating procedures that meets the following requirements:

a. Provides a detailed description of procedures required to initiate, control, and verify proper system operation
b. Provides procedures that clearly enable the operator to assess the correct flow of system functions (as evidenced by system-generated status and information messages)
c. Provides procedures that clearly enable the operator to intervene in system operations to recover from an abnormal system state
d. Defines and illustrates the procedures and system prompts for situations where operator intervention is required to load, initialize, and start the system
e. Defines and illustrates procedures to enable and control the external interface to the system operating environment if supporting hardware and software are involved. Such information also **shall** be provided for the interaction of the system with other data processing systems or data interchange protocols
f. Provides administrative procedures and off-line operator duties (if any) if they relate to the initiation or termination of system operations, to the assessment of system status, or to the development of an audit trail
g. Supports successful ballot and program installation and control by election officials, provides a detailed work plan or other form of documentation providing a schedule and steps for the software and ballot installation, which includes a table outlining the key dates, events and deliverables
h. Supports diagnostic testing, specifies diagnostic tests that may be employed to identify problems in the system, verifies the correction of maintenance problems; and isolates and diagnoses faults from various system states
i. Details the care and handling precautions necessary for removable media and records to satisfy the 22-month archival requirements.

9.8.6 Operations Support

The manufacturer **shall** provide documentation of system operating procedures that meets the following requirements:

a. Defines the procedures required to support system acquisition, installation, and readiness testing. These procedures may be provided by reference, if they are contained either in the system hardware specifications, or in other manufacturer documentation
b. Describes procedures for providing technical support, system maintenance and correction of defects, and for incorporating hardware upgrades and new software releases

9.8.7 Appendices

The manufacturer may provide descriptive material and data supplementing the various sections of the body of the System Operations Manual. The content and arrangement of appendices **shall** be at the discretion of the manufacturer. Topics recommended for discussion include:

Glossary: A listing and brief definition of all terms that may be unfamiliar to persons not trained in either voting systems or computer operations

References: A list of references to all manufacturer documents and to other sources related to operation of the system

Detailed Examples: Detailed scenarios that outline correct system responses to faulty operator input; Alternative procedures may be specified depending on the system state

Manufacturer's Recommended Security Procedures: This appendix **shall** contain the security procedures that are to be executed by the system operator

9.9 System Maintenance Manual

The system maintenance procedures **shall** provide information in sufficient detail to support election workers, information systems personnel, or maintenance personnel in the adjustment or removal and replacement of components or modules in the field. Technical documentation needed solely to support the repair of defective components or modules ordinarily done by the manufacturer or software developer is not required.

Recommended service actions to correct malfunctions or problems **shall** be discussed, along with personnel and expertise required to repair and maintain the system; and equipment, materials, and facilities needed for proper maintenance. This manual **shall** include the sections listed below.

9.9.1 Introduction

The manufacturer **shall** describe the structure and function of the equipment (and related software) for election preparation, programming, vote recording, tabulation, and reporting in sufficient detail to provide an overview of the system for maintenance, and for identification of faulty hardware or software. The description **shall** include a concept of operations that fully describes such items as:

a. The electrical and mechanical functions of the equipment
b. How the processes of ballot handling and reading are performed (paper-based systems)
c. How vote selection and casting of the ballot are performed (DRE systems);
d. How transmission of data over a network is performed (DRE systems, where applicable)
e. How data are handled in the processor and memory units
f. How data output is initiated and controlled
g. How power is converted or conditioned
h. How test and diagnostic information is acquired and used

9.9.2 Maintenance Procedures

The manufacturer **shall** describe preventive and corrective maintenance procedures for hardware and software.

9.9.2.1 Preventive Maintenance Procedures

The manufacturer **shall** identify and describe:

a. All required and recommended preventive maintenance tasks, including software tasks such as software backup, database performance analysis, and database tuning
b. Number and skill levels of personnel required for each task
c. Parts, supplies, special maintenance equipment, software tools, or other resources needed for maintenance
d. Any maintenance tasks that must be coordinated with the manufacturer or a third party (such as coordination that may be needed for off-the-shelf items used in the system)

9.9.2.2 Corrective Maintenance Procedures

The manufacturer **shall** provide fault detection, fault isolation, correction procedures, and logic diagrams for all operational abnormalities identified by design analysis and operating experience.

The manufacturer **shall** identify specific procedures to be used in diagnosing and correcting problems in the system hardware (or user-controlled software). Descriptions **shall** include:

a. Steps to replace failed or deficient equipment
b. Steps to correct deficiencies or faulty operations in software
c. Modifications that are necessary to coordinate any modified or upgraded software with other software modules
d. The number and skill levels of personnel needed to accomplish each procedure
e. Special maintenance equipment, parts, supplies, or other resources needed to accomplish each procedure
f. Any coordination required with the manufacturer, or other party, for off the shelf items

9.9.3 Maintenance Equipment

The manufacturer **shall** identify and describe any special purpose test or maintenance equipment recommended for fault isolation and diagnostic purposes.

9.9.4 Parts and Materials

Manufacturers **shall** provide detailed documentation of parts and materials needed to operate and maintain the system. Additional requirements apply for paper-based systems.

9.9.4.1 Common Standards

The manufacturer **shall** provide a complete list of approved parts and materials needed for maintenance. This list **shall** contain sufficient descriptive information to identify all parts by:

a. Type
b. Size
c. Value or range
d. Manufacturer's designation
e. Individual quantities needed
f. Sources from which they may be obtained

9.9.4.2 Paper-based Systems

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

The TDP **shall** specify the required paper stock, size, shape, opacity, color, watermarks, field layout, orientation, size and style of printing, size and location of punch or mark fields used for vote response fields and to identify unique ballot formats, placement of

alignment marks, ink for printing, and folding and bleed-through limitations for preparation of ballots that are compatible with the system.

9.9.5 Maintenance Facilities and Support

The manufacturer **shall** identify all facilities, furnishings, fixtures, and utilities that will be required for equipment maintenance. In addition, manufacturers **shall** specify the assumptions made with regard to any parameters that impact the mean time to repair. These factors **shall** include at a minimum:

a. Recommended number and locations of spare devices or components to be kept on hand for repair purposes during periods of system operation
b. Recommended number and locations of qualified maintenance personnel who need to be available to support repair calls during system operation
c. Organizational affiliation (i.e., jurisdiction, manufacturer) of qualified maintenance personnel

9.9.6 Appendices

The manufacturer may provide descriptive material and data supplementing the various sections of the body of the System Maintenance Manual. The content and arrangement of appendices **shall** be at the discretion of the manufacturer. Topics recommended for amplification or treatment in appendices include:

Glossary: A listing and brief definition of all terms that may be unfamiliar to persons not trained in either voting systems or computer maintenance

References: A list of references to all manufacturer documents and other sources related to maintenance of the system

Detailed Examples: Detailed scenarios that outline correct system responses to every conceivable faulty operator input; alternative procedures may be specified depending on the system state

Maintenance and Security Procedures: This appendix **shall** contain technical illustrations and schematic representations of electronic circuits unique to the system

9.10 Personnel Deployment and Training Requirements

The manufacturer **shall** describe the personnel resources and training required for a jurisdiction to operate and maintain the system.

9.10.1 Personnel

The manufacturer **shall** specify the number of personnel and skill levels required to perform each of the following functions:

a. Pre-election or election preparation functions (e.g., entering an election, contest and candidate information; designing a ballot; generating pre-election reports
b. System operations for voting system functions performed at the polling place
c. System operations for voting system functions performed at the central count facility
d. Preventive maintenance tasks
e. Diagnosis of faulty hardware or software
f. Corrective maintenance tasks
g. Testing to verify the correction of problems

A description **shall** be presented of which functions may be carried out by user personnel, and those that must be performed by manufacturer personnel.

9.10.2 Training

The manufacturer **shall** specify requirements for the orientation and training of the following personnel:

a. Poll workers supporting polling place operations
b. System support personnel involved in election programming
c. User system maintenance technicians
d. Network/system administration personnel (if a network is used)
e. Information systems personnel
f. Manufacturer personnel

9.11 Configuration Audits

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

9.11.1 Physical Configuration Audit

The Physical Configuration Audit is conducted by the S-ATA to compare the voting system components submitted for certification to the manufacturer's technical documentation.

For the PCA, a manufacturer **shall** provide:

a. Identification of all items that are to be a part of the software release
b. Specification of compiler (or choice of compilers) to be used to generate

executable programs

c. Identification of all hardware that interfaces with the software
d. Configuration baseline data for all hardware that is unique to the system
e. Copies of all software documentation intended for distribution to users, including program listings, specifications, operations manual, voter manual, and maintenance manual
f. User acceptance test procedures and acceptance criteria
g. Identification of any changes between the physical configuration of the system submitted for the PCA and that submitted for the FCA, with a certification that any differences do not degrade the functional characteristics
h. Complete descriptions of its procedures and related conventions used to support this audit by:
    i. Establishing a configuration baseline of the software and hardware to be tested
    ii. Confirming whether the system documentation matches the corresponding system components

9.11.2 Functional Configuration Audit

The Functional Configuration Audit is conducted by the S-ATA to verify that the system performs all the functions described in the system documentation. The manufacturer **shall**:

a. Completely describe its procedures and related conventions used to support this audit for all system components
b. Provide the following information to support this audit:
    i. Copies of all procedures used for module or unit testing, integration testing, and system testing
    ii. Copies of all test cases generated for each module and integration test, and sample ballot formats or other test cases used for system tests
    iii. Records of all tests performed by the procedures listed above, including error corrections and retests

9.12 System Change Notes

Manufacturers submitting modifications for a system that has been tested previously and received national certification **shall** submit system change notes. These will be used by the S-ATA to assist in developing and executing the test plan for the modified system. The system change notes **shall** include the following information:

a. Summary description of the nature and scope of the changes, and reasons for each change
b. A listing of the specific changes made, citing the specific system configuration items changed and providing detailed references to the documentation sections changed
c. The specific sections of the documentation that are changed (or completely

revised documents, if more suitable to address a large number of changes)

d. Documentation of the test plan and procedures executed by the manufacturer for testing the individual changes and the system as a whole, and records of test results