2012

DRAFT VVSG 1.1

U.S. Election Assistance Commission

Volume II

MARCH 31, 2015

Table of Contents

Volume I Voting System Performance Guidelines

Overview	Voluntary Voting System Guidelines Overview
Section 1	Voting System Performance Guidelines Introduction
Section 2	Functional Requirements
Section 3	Usability and Accessibility Requirements
Section 4	Hardware Requirements
Section 5	Software Requirements
Section 6	Telecommunications Requirements
Section 7	Security Requirements
Section 8	Quality Assurance and Configuration Management
Appendix A	Glossary
Appendix B	References

Volume II National Certification Testing Guidelines

Section 1	National Certification Testing Guidelines Introduction
Section 2	Quality and Configuration Management Manual
Section 3	Description of the Technical Data Package
Section 4	Functionality Testing
Section 5	Hardware Testing
Section 6	Software Testing
Section 7	System Integration Testing
Section 8	Quality Assurance and Configuration Management
Appendix A	National Certification Test Plan
Appendix B	National Certification Test Report
Appendix C	Assessing Conformity to Benchmarks

Voluntary Voting System Guidelines Overview

Guide to Section Locations

1	Introduction	2
2	Quality and Configuration Management Manual	18
3	Description of the Technical Data Package	23
4	Functionality Testing	53
5	Hardware Testing	59
6	Software Testing	71
7	System Integration Testing	74
8	Quality Assurance and Configuration Management	81
Appendix A:	National Certification Test Plan	A-2
Appendix B:	National Certification Test Report	B-2
Appendix C:	Assessing Conformity to Benchmarks	C-2

1 Introduction

Table of Contents

1	Introduction	2
1.1	**Overview of the National Certification Testing Guidelines**	**2**
1.2	**Overview of the National Certification Testing Process**	**2**
1.3	**Testing Scope**	**3**
1.3.1	Test Categories	3
1.4	**Testing Sequence**	**6**
1.5	**Documentation Submitted by Manufacturer**	**7**
1.6	**Voting Equipment Submitted by Manufacturer**	**7**
1.7	**Test Applicability**	**8**
1.7.1	General Applicability	8
1.7.2	Modifications to Certified Systems	9
1.8	**Certification Test Process**	**10**
1.8.1	Pre-test Activities	10
1.8.2	Certification Testing	11
1.8.3	Post-test Activities	15
1.8.4	Resolution of Testing Issues	16

1 Introduction

1.1 Overview of the National Certification Testing Guidelines

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

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

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

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

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

1.2 Overview of the National Certification Testing Process

Certification testing encompasses the examination and testing of software; tests of hardware under conditions simulating the intended storage, operation, transportation, and maintenance environments; the inspection and evaluation of system documentation; and operational tests to validate system performance and functioning under normal and abnormal conditions. The testing also evaluates the completeness of the 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.

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

The Help America Vote Act (HAVA) directs the U.S. Election Assistance Commission (EAC) to provide for the testing, certification, decertification, and recertification of voting system hardware and software by accredited laboratories. HAVA also introduces different terminology for these functions. Under the EAC process, test labs are "accredited" and voting systems are "certified." The term "standards" has been replaced with the term "*Guidelines*." As prescribed by HAVA, the EAC process was initially based on the 2002 Voting Systems Standards and will transition to the revised standards issued through *Voluntary Voting System Guidelines 1.1*.

1.3 Testing Scope

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

- 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

1.3.1 Test Categories

The certification test procedure is presented in several parts:

- Functionality testing
- Hardware testing
- Software evaluation
- System level integration tests, including audits
- Examination of documented manufacturer practices for quality assurance and for configuration management

In practice, there may be concurrent indications of hardware and software function, or failure to function, during certain examinations and tests. Operating tests of hardware partially exercise the

software as well and therefore supplement software testing. Security tests exercise hardware, software and communications capabilities. Documentation review conducted during software qualification supplements the review undertaken for system-level testing.

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

1.3.1.1 Focus of Functionality Tests

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

1.3.1.2 Focus of Hardware Tests

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

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

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

1.3.1.3 Focus of Software Evaluation

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

The applicability of different categories of requirements and tests to different kinds of logic (application logic, border logic, third-party logic, and COTS) are explained further in Volume I, Section 5.2.1.

1.3.1.4 Focus of System Integration Tests

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

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

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

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

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

The Functional Configuration Audit (FCA) is an exhaustive verification of every system function and combination of functions cited in the manufacturer's documentation. Through use, the FCA verifies the accuracy and completeness of the system Technical Data Package (TDP). The various options of software counting logic that are claimed in the 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.

1.3.1.5 Focus of Manufacturer Documentation Examination

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

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

1.4 Testing Sequence

The overall testing process progresses through several stages involving pre-testing, testing, and post-testing activities. National certification testing involves a series of physical tests and other examinations that are conducted in a particular sequence. The sequence is intended to maximize overall testing effectiveness, as well as conduct testing in as efficient a manner as possible. The VSTL will follow the general sequence outlined below. 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 Certification Authority.
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 National Certification Test Report
m. Delivery of the National Certification Test Report to the EAC

1.5 Documentation Submitted by Manufacturer

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

1.6 Voting Equipment Submitted by Manufacturer

Manufacturers may seek to market a complete voting system or an interoperable component of a voting system. In all instances, manufacturers **shall** submit for testing the specific system configuration that will be offered to jurisdictions or that comprises the component to be marketed

plus the other components with which the manufacturer recommends that the component be used. The system submitted for testing **shall** meet the following requirements:

a. The hardware submitted for certification testing **shall** be equivalent, in form and function, to the actual production version of the hardware units or the COTS hardware specified for use in the TDP
b. The software submitted for certification testing **shall** be the exact software that will be used in production units
c. Engineering or developmental prototypes are not acceptable, unless the manufacturer can show that the equipment to be tested is equivalent to standard production units both in performance and construction
d. Benchmark directory listings **shall** be submitted for all software/firmware elements (and associated documentation) included in the manufacturer's release as they would normally be installed upon setup and installation

1.7 Test Applicability

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

1.7.1 General Applicability

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

1.7.1.1 Hardware

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

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

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

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

1.7.1.2 Software

The applicability of different categories of requirements and tests to different kinds of logic (application logic, border logic, third-party logic, and COTS) is described in Volume I, Section 5.2.1. Further background is provided in Volume II, Section 5.2.

1.7.2 Modifications to Certified Systems

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

1.7.2.1 General Requirements for Modifications

The VSTL 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, the VSTL may:

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

1.7.2.2 Basis for Limited Testing Determinations

The VSTL 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 with these *Guidelines* for:

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

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

1.8 Certification Test Process

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

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

Whether one or more VSTLs are used, the testing generally consists of three phases:

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

1.8.1 Pre-test Activities

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

1.8.1.1 Initiation of Testing

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

a. Request the performance of certification testing from among the accredited testing laboratories
b. Enter into formal agreement with the VSTL for the performance of testing
c. Prepare and submit materials required for testing consistent with the requirements of the *Guidelines*

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

1.8.1.2 Pre-test Preparation

Pre-test preparation encompasses the following activities:

a. The manufacturer **shall** prepare and submit a complete TDP to the VSTL. The TDP should consist of the materials described in Section 3
b. The VSTL **shall** perform an initial review of the TDP for completeness and clarity and request additional information as required
c. The manufacturer **shall** provide additional information, if requested by the VSTL
d. The manufacturer and VSTL **shall** enter into an agreement for the testing to be performed by the VSTL in exchange for payment by the manufacturer
e. The manufacturer **shall** deliver to the VSTL all hardware and software needed to perform testing

1.8.2 Certification Testing

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

1.8.2.1 National Certification Test Plan

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

a. Verifying or checking equipment operational status by means of manufacturer operating procedures
b. Establishing the test environment or the special environment required to perform the test
c. Initiating and completing operating modes or conditions necessary to evaluate the specific performance characteristic under test
d. Measuring and recording the value or range of values for the characteristic to be tested, demonstrating expected performance levels
e. Verifying, as above, that the equipment is still in normal condition and status after all required measurements have been obtained
f. Confirming that documentation submitted by the manufacturer corresponds to the actual configuration and operation of the system
g. Confirming that documented manufacturer practices for quality assurance and configuration management comply with the *Guidelines* and the Quality and Configuration Manual

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

1.8.2.2 Certification Test Conditions

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

a. Preparations for testing, arrangement of equipment, verification of equipment status, and the execution of procedures **shall** be witnessed by at least one independent, qualified observer in the form of an accredited testing laboratory, which **shall** certify that all test and data acquisition requirements have been satisfied
b. When a test is to be performed at “standard” or “ambient” conditions, this requirement **shall** refer to a nominal laboratory or office environment, with a temperature in the range of 68 to 75 degrees Fahrenheit, and prevailing atmospheric pressure and relative humidity
c. Otherwise, all tests **shall** be performed at the required temperature and electrical supply voltage, regulated within the following tolerances:
   i. Temperature ±4 degrees F
   ii. Electrical supply voltage ±2 volts alternating current
d. 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.

1.8.2.3 Certification Test Fixtures

The VSTL **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 VSTL 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 VSTL 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 VSTL 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.

1.8.2.4 Witness of System Build and Installation

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

1.8.2.5 Certification Test Data Requirements

The following test data practices **shall** be employed:

a. A test log of the procedure **shall** be maintained. This log **shall** identify the system and equipment by model and serial number
b. Test environment conditions **shall** be noted
c. All operating steps, the identity and quantity of simulated ballots, annotations of output reports, the elapsed time for each procedure step, and observations of equipment performance and, in the case of non-operating hardware tests, the condition of the equipment **shall** be recorded

1.8.2.6 Certification Test Practices

The VSTL **shall** conduct the examinations and tests defined in the test plan to determine compliance with the voting system requirements described in the VVSG. 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 VSTL does not have the opportunity to test can be expected to conceal similar faults. Therefore,

a. If a logic defect is found to be responsible for the incorrect recording, tabulation, or reporting of a vote, testing **shall** be halted and a report on the anomaly **shall** be delivered to the EAC without delay.
b. If the VSTL finds such a profusion of logic defects as to indicate that the manufacturer's quality assurance was inadequate, testing **shall** be halted and a report on the anomalies delivered to the EAC.
c. 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 b 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 (see Volume II, Section 5.7.2). Nevertheless, the manufacturer will be given the opportunity to correct noncritical software defects. 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 conformity assessment process is resumed. When it is resumed, the regression testing that the VSTL 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 just 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 (see Volume II, Section 5.7.2).

d. 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 VSTL to categorize the anomaly, then testing may be resumed at the point of suspension.
e. Otherwise (i.e., if the previous paragraph does not apply), the VSTL **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.
f. Testing may resume after a nonconformity is found if:

i. 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;
ii. The examiner of the equipment agrees that the proposed change is responsive to the full scope of the nonconformity;
iii. Any previously failed tests are passed by the revised system; and
iv. 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.

1.8.3 Post-test Activities

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

a. The VSTL may issue interim reports to the manufacturer, informing the manufacturer of the testing status, findings to date, and other information.
b. The VSTL **shall** prepare a National Certification Test Report that confirms the voting system has passed the required testing. This report **shall** include the date testing was completed, the specific system version addressed by the report, the version numbers of all system elements separately identified with a version number by the manufacturer, and the scope of tests conducted. A recommended outline for the test report is contained in Appendix B.
c. Where a system is tested by multiple VSTLs, the lead VSTL **shall** prepare a consolidated National Certification Test Report.
d. The VSTL **shall** deliver the report to the manufacturer and to the EAC.
e. Upon review and acceptance of the test report, EAC **shall** issue a Certification Number for the system to the manufacturer and to the VSTL. The issuance of a Certification Number indicates that the system has been tested by the VSTL for compliance with the *Guidelines.*
f. This number applies to the system as a whole only for the configuration and versions of the system elements tested and identified in the National Certification Test Report. The Certification Number does not apply to individual system components or untested configurations.
g. The EAC Certification Number is intended for use by the states and their jurisdictions to support state and jurisdiction processes concerning voting systems. States and their jurisdictions **shall** request National Certification Test Reports based on the EAC Certification Number to support their voting system certification and procurement processes.

1.8.4 Resolution of Testing Issues

The EAC has a process for the VSTLs, manufacturers and election officials to request an interpretation of the *Guidelines*. The interpretation is publicly documented for reference by interested parties. The EAC periodically assesses the interpretations provided to determine which topics should be reflected in a future version of the *Guidelines*.

2 Description of the Quality and Configuration Management Manual

Table of Contents

2 Quality and Configuration Management Manual 18

2.1 Quality and Configuration Management Manual 18

2 Quality and Configuration Management Manual

2.1 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 Certification Authority a complete Quality and Configuration Management Manual. The Manual **shall** detail the manufacturer's Quality and Configuration Management processes and procedures required by the VVSG. These processes and procedures **shall** conform to all requirements of the VVSG and the standards listed in Volume I Section 8.1.
b. The Manual **shall** declare that meeting the requirements of the entire VVSG 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 – Requirements Section 8.3.1.
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 Certification Authority or the VSTL. "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 VVSG. 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 VVSG.
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 VVSG.
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.

3 Description of the Technical Data Package

Table of Contents

3	Description of the Technical Data Package	23
3.1	**Scope**	**23**
3.1.1	Content and Format	23
3.1.2	Other Uses for Documentation	27
3.1.3	Protection of Proprietary Information	27
3.2	**System Overview**	**28**
3.2.1	System Description	28
3.2.2	System Performance	29
3.3	**System Functionality Description**	**29**
3.4	**System Hardware Specification**	**30**
3.4.1	System Hardware Characteristics	30
3.4.2	Design and Construction	30
3.5	**Software Design and Specification**	**31**
3.5.1	Purpose and Scope	31
3.5.2	Applicable Documents	31
3.5.3	Software Overview	31
3.5.4	Software Standards and Conventions	32
3.5.5	Software Operating Environment	32
3.5.6	Software Functional Specification	33
3.5.7	Programming Specifications	33
3.5.8	System Database	35
3.5.9	Interfaces	35
3.5.10	Appendices	36
3.6	**System Security Specification**	**37**
3.6.1	Access Control	38
3.6.2	Equipment and Data Security	39
3.6.3	Software Installation and Security	39
3.6.4	System Event Logging	39
3.6.5	Physical Security	40
3.6.6	Setup Inspection	40
3.6.7	Cryptography	40
3.6.8	Telecommunications and Data Transmission Security	41
3.6.9	Other Elements of an Effective Security Program	41
3.7	**System Test and Verification Specification**	**42**
3.7.1	Development Test Specifications	42

3.7.2	National Certification Test Specifications	43
3.8	**System Operations Procedures**	**43**
3.8.1	Introduction	43
3.8.2	Operational Environment	44
3.8.3	System Installation and Test Specification	44
3.8.4	Operational Features	44
3.8.5	Operating Procedures	44
3.8.6	Operations Support	45
3.8.7	Appendices	45
3.9	**System Maintenance Manual**	**46**
3.9.1	Introduction	46
3.9.2	Maintenance Procedures	47
3.9.3	Maintenance Equipment	47
3.9.4	Parts and Materials	48
3.9.5	Maintenance Facilities and Support	48
3.9.6	Appendices	49
3.10	**Personnel Deployment and Training Requirements**	**49**
3.10.1	Personnel	49
3.10.2	Training	50
3.11	**Configuration Audits**	**50**
3.11.1	Physical Configuration Audit	50
3.11.2	Functional Configuration Audit	51
3.12	**System Change Notes**	**51**

3 Description of the Technical Data Package

3.1 Scope

This subsection contains a description of manufacturer documentation relating to the voting system that **shall** be submitted with the system as a precondition of national certification testing. These items are necessary to define the product and its method of operation; to provide technical and test data supporting the manufacturer's claims of the system's functional capabilities and performance levels; and to document instructions and procedures governing system operation and field maintenance. Any information relevant to the system evaluation **shall** be submitted to include source code, object code, and sample output report formats.

Both formal documentation and notes of the manufacturer's system development process **shall** be submitted for qualification tests. Documentation describing the system development process permits assessment of the manufacturer's systematic efforts to develop and test the system and correct defects. Inspection of this process also enables the design of a more precise test plan. If the manufacturer's developmental test data are incomplete, the VSTL **shall** design and conduct the appropriate tests to cover all elements of the system and to ensure conformance with all system requirements.

3.1.1 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

The manufacturer **shall** provide a list of all documents submitted controlling the design, construction, operation, and maintenance of the system. Documents **shall** be listed in order of precedence.

3.1.1.1 Required Content for Initial Certification

Technical Data Package, main part

The main part of the TDP is relevant for conformity assessment and certification and has the VSTL and the EAC as its target audience. 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 VVSG 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 VVSG.

1 Implementation Statement - Formal declaration of which standard options were implemented in the system, as defined in the Conformance Clause.

2 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.

3 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.

3.1 Overview

3.2 Standards and conventions

3.3 Operating environment

3.4 Functional specification

3.5 Programming specifications

3.6 System database

3.7 Interfaces

4 System Security Specification - Addresses the security requirements of Volume I, Section 7.

4.1 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).

4.2 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.

4.3 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.

4.4 Security Threats Controls - Identifies the threats the voting system protects against and the implemented security controls on voting system and system components.

4.5 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.

5 System Test Specification - Development tests, usability test reports, etc.

6 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.

7 Configuration for Testing - The configuration actions necessary to obtain conforming behavior from the voting system.

8 A copy of the Quality and Configuration Management Manual previously submitted to the Certification Authority.

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:

1 System Overview

2 System Functionality Description

3 System Security Manual

3.1 Access control

3.2 System event logging

3.3 Software installation

3.4 Setup inspection

3.5 Communications

3.6 Voter Verifiable Paper Audit Trail (VVPAT)

3.7 Physical security

3.8 Audit

4 System Operations Manual

4.1 Introduction

4.2 Operational environment

4.3 System installation and test specification

4.4 Operational features

4.5 Operating procedures

4.6 Documentation for poll workers

4.7 Operations support

4.8 Transportation and storage

5 System Maintenance Manual

5.1 Introduction

5.2 Maintenance procedures

5.3 Maintenance equipment

5.4 Parts and materials

5.5 Maintenance facilities and support

6 Personnel Deployment and Training Requirements

3.1.1.2 Required Content for System Changes and Re-certification

For systems seeking re-certification, manufacturers **shall** submit System Change Notes as described in Subsection 3.12, 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.

3.1.1.3 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.

3.1.2 Other Uses for Documentation

Although all of the TDP documentation is required for national certification testing, some of these same items may also be required during the state certification process and local level acceptance testing. Therefore, it is recommended that the technical documentation required for certification and acceptance testing be deposited in escrow.

3.1.3 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 Federal 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.

3.2 System Overview

In the system overview, the manufacturer **shall** provide information that enables the VSTL to identify the functional and physical components of the system, how the components are structured, and the interfaces between them.

3.2.1 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
   iv. Communications routers
   v. Modem drivers
   vi. Dial-up networking software
f. Interfaces among internal components, and interfaces with external systems. For components that interface with other components for which multiple products may be used, the TDP **shall** provide an identification of:
   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

3.2.2 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.

3.3 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 Guidelines and any additional capabilities provided by the system. This listing **shall** provide a simple description of each capability. Detailed specifications **shall** be provided in other documentation required for the TDP.

a. The manufacturer **shall** organize the presentation of required capabilities in a manner that corresponds to the structure and sequence of functional capabilities indicated in Volume I, Section 2. The contents of Volume I, Section 2 may be used as the basis for a checklist to indicate the specific functions provided and those not provided by the system
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

3.4 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.

3.4.1 System Hardware Characteristics

The manufacturer **shall** provide a detailed discussion of the characteristics of the system, indicating how the hardware meets individual requirements defined in Volume I, Section 4, including:

Performance characteristics: This discussion addresses basic system performance attributes and operational scenarios that describe the manner in which system functions are invoked, describe environmental capabilities, describe life expectancy, and describe any other essential aspects of system performance

Physical characteristics: This discussion addresses suitability for intended use, requirements for transportation and storage, health and safety criteria, security criteria, and vulnerability to adverse environmental factors

Reliability: This discussion addresses system and component reliability stated in terms of the system's operating functions, and identification of items that require special handling or operation to sustain system reliability. The manufacturer **shall** include in the TDP a reliability analysis, such as a failure modes and effects analysis (FMEA), that satisfies the requirements of Volume I Section 4.3.3.4.

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

3.4.2 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

3.5 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.

3.5.1 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.

3.5.2 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.

3.5.3 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.

3.5.4 Software Standards and Conventions

The manufacturer **shall** provide information that can be used by a VSTL or state certification board 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

3.5.5 Software Operating Environment

This section **shall** describe or make reference to all operating environment factors that influence the software design.

3.5.5.1 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

3.5.5.2 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.

3.5.6 Software Functional Specification

The manufacturer **shall** provide a description of the operating modes of the system and of software capabilities to perform specific functions.

3.5.6.1 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)

3.5.6.2 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

3.5.7 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.

3.5.7.1 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.

3.5.7.2 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. (Subsection 3.5.9 describes the requirements for documenting system interfaces.) Data local to the software module or unit **shall** be described separately from data input to, or output from, the software module or unit
f. If the software module or unit contains logic, the logic to be used by the software unit, including, as applicable:
    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:
        1. The method for sequence control
        2. The logic and input conditions of that method, such as timing variations, priority assignments
        3. Data transfer in and out of memory
        4. 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 3.5.8

3.5.8 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

3.5.9 Interfaces

The manufacturer **shall** identify and provide a complete description of all internal and external interfaces, using a combination of text and diagrams.

3.5.9.1 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)

3.5.9.2 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)

3.5.10 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

3.6 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 found in Volume I, Section 7
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.

3.6.1 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.

3.6.1.1 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 indicated in Volume I, Subsection 7.2.

3.6.1.2 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 of Volume I, Subsection 7.2.

3.6.2 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 of Volume I, Subsection 7.3. This information **shall** address measures for polling place security and central count location security.

3.6.3 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 the specific requirements of Volume I, Subsection 7.4. 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.

3.6.4 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.

3.6.5 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.

3.6.6 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. The registers and variables of the voting system to be inspected are specified in Volume I, Sections 2.2.5 Verification at the Polling Place, 2.2.6 Verification at the Central Location, 2.3.3.3 DRE System and EBM System Requirements, and 7.4.6 Software Setup Validation.

3.6.7 Cryptography

a. Manufacturers **shall** provide a list of all cryptographic algorithms and key sizes employed by the voting system.
b. Manufacturers **shall** provide the technical specification of all cryptographic protocols employed 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 the corresponding NIST FIPS 140-2 validation certificate number for all cryptographic modules that implement the cryptographic algorithms of the voting systems. These may be previously approved 3rd party COTS modules or they may be unique to the voting system manufacturer.

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.

3.6.8 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 the specific requirements of Volume I, Subsection 7.5:

a. For all systems, this information **shall** address access control, and prevention of data interception
b. For systems that use public communications networks as defined in Volume I, Section 6, this information **shall** also include:
    i. Capabilities used to provide protection against threats to third party products and services
    ii. Policies and processes used by the manufacturer to ensure that such protection is updated to remain effective over time
    iii. Policies and procedures used by the manufacturer to ensure that current versions of such capabilities are distributed to user jurisdictions and are installed effectively by the jurisdiction
    iv. A detailed description of the system capabilities and procedures to be employed by the jurisdiction to diagnose the occurrence of a denial of service attack, to use an alternate method of voting, to determine when it is appropriate to resume voting over the network, and to consolidate votes cast using the alternate method
    v. A detailed description of all activities to be performed in setting up the system for operation that are mandatory to ensure effective system security, including testing of security before an election
    vi. A detailed description of all activities that should be prohibited during system setup and during the timeframe for voting operations, including both the hours when polls are open and when polls are closed

3.6.9 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.

3.7 System Test and Verification Specification

The manufacturer **shall** provide test and verification specifications for:

a. Development test specifications
b. National certification test specifications

3.7.1 Development Test Specifications

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. This description **shall** include:

a. 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 VSTL **shall** design test cases and procedures equivalent to those ordinarily used during product verification.

3.7.2 National Certification 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.

3.8 System Operations Procedures

System Operations Procedures documentation **shall** provide all information necessary for system use by all personnel who support pre-election and election preparation, polling place activities and central counting activities, as applicable, with regard to all system functions and operations identified in Subsection 3.3 above. The nature of the instructions for operating personnel will depend upon the overall system design and required skill level of system operations support personnel.

The system operations procedures **shall** contain all information that is required for the preparation of detailed system operating procedures, and for operator training, as described below.

3.8.1 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.

3.8.2 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

3.8.3 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 in Subsection 3.3 above, 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.

3.8.4 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

3.8.5 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 of Volume I Sections 2.1.10, 4.1.3.2, 4.1.6.1.b, 4.1.6.2.c, 4.1.7.1 and 5.3.

3.8.6 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

3.8.7 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

3.9 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.

3.9.1 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

3.9.2 Maintenance Procedures

The manufacturer **shall** describe preventive and corrective maintenance procedures for hardware and software.

3.9.2.1 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)

3.9.2.2 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

3.9.3 Maintenance Equipment

The manufacturer **shall** identify and describe any special purpose test or maintenance equipment recommended for fault isolation and diagnostic purposes.

3.9.4 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.

3.9.4.1 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

3.9.4.2 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.

3.9.5 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

3.9.6 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

3.10 Personnel Deployment and Training Requirements

The manufacturer **shall** describe the personnel resources and training required for a jurisdiction to operate and maintain the system.

3.10.1 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.

3.10.2 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

3.11 Configuration Audits

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

3.11.1 Physical Configuration Audit

The Physical Configuration Audit is conducted by the VSTL 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

3.11.2 Functional Configuration Audit

The Functional Configuration Audit is conducted by the VSTL 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

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

3.12 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 VSTL 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

4 Functionality Testing

Table of Contents

4	Functionality Testing	53
4.1	**Scope**	**53**
4.2	**Breadth of Functionality Testing**	**53**
4.2.1	Basic Functionality Testing Requirements	53
4.2.2	Testing to Reflect Technologies	54
4.2.3	Testing to Reflect Additional Capabilities	54
4.2.4	Testing to Reflect Previously Tested Capabilities	54
4.3	**General Test Sequence**	**55**
4.3.1	Testing in Parallel with Precinct Count Systems	55
4.3.2	Testing in Parallel with Central Count Systems	56
4.4	**Functionality Testing for Accessibility**	**57**
4.5	**Testing for Systems that Operate on Personal Computers**	**57**

4 Functionality Testing

4.1 Scope

This section contains a description of the testing to be performed to confirm the functional capabilities of a voting system submitted for national certification. It describes the scope and basis for functionality testing, outlines the general sequence of tests within the overall test process, and provides guidance on testing for accessibility.

4.2 Breadth of Functionality Testing

In order to best complement the diversity of the voting systems industry, the certification testing process is not rigidly defined. Although there are basic functionality testing requirements, additions or variations in testing are appropriate to the use of specific technologies and configurations, system capabilities, and the outcomes of previous testing.

4.2.1 Basic Functionality Testing Requirements

The VSTL **shall** design and perform procedures to test a voting system against the functional requirements outlined in Volume I, Section 2. Test procedures **shall** be designed and performed that address:

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 National Certification Test Plan prepared by the VSTL. 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 VSTL **shall** design test procedures that account for such variations and reflect the system-specific functional capabilities in Volume I, Section 2.

The testing of the components and system readiness by the VSTL **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.

4.2.2 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. Such variation is recognized in the definitions of voting systems in Volume I, Section 1, and serves as the basis for delineating various functional capability requirements.

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

4.2.3 Testing to Reflect Additional Capabilities

The requirements for voting system functionality provided by Volume I, Section 2 reflect a minimum set of capabilities. 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, as described in Volume II, Section 3. Based on this information, the VSTL **shall** design and perform system functionality testing for these additional functional capabilities.

4.2.4 Testing to Reflect Previously Tested Capabilities

The required functional capabilities of voting systems defined in Volume I, Section 2 reflect a broad range of system functionality needed to support the full life cycle of an election, including post election activities. Many systems submitted for certification are designed to address this scope, and are to be tested accordingly.

However, some new systems using a combination of new subsystems or system components interfaced with the components of a previously certified system. For example, a 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 VSTL 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 VSTL 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

4.3 General Test Sequence

There is no required sequence for performing the system certification tests. For a system not previously certified, the VSTL 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 VSTL will usually conduct functionality testing as an integral element of the system integration testing described in Section 6.

Some functionality tests for the voting functions defined in Volume I, Section 2.may be performed as an integral part of hardware testing, enabling a more efficient testing process. Ballots processed and counted during hardware operating tests for precinct count and central count systems may serve to satisfy part of the functionality testing, provided that the ballots were cast using a test procedure that is equivalent to the procedures indicated below.

4.3.1 Testing in Parallel with Precinct Count Systems

For testing voting functions defined in Volume I, Sections 2, the following procedures **shall** be performed during the functionality tests of voting equipment and precinct counting equipment.

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 as specified in Volume II, Section 4
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 as specified in Volume I, Sections 2 and 5
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.

4.3.2 Testing in Parallel with Central Count Systems

For testing voting functions defined in Volume I, Section 2, 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 as specified in Volume I, Sections 2 and 5
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

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

4.4 Functionality Testing for Accessibility

Volume I, Section 3 prescribes the requirements for voting system accessibility to satisfy the provisions of HAVA 301(a)(4) and 241(b)(5). To demonstrate conformance to these requirements, manufacturers **shall** conduct summative usability tests of accessible voting equipment with blind and visually impaired individuals and individuals lacking fine motor control. A description of the testing performed, the population of test subjects participating, and the results **shall** be documented using the Common Industry Format (CIF) by the manufacturer and submitted as part of the Technical Data Package. The test labs **shall** review this information during the system certification documentation review.

4.5 Testing for Systems that Operate on Personal Computers

For systems intended to use non-standard voting devices, such as a personal computer, provided by the local jurisdiction, the VSTL **shall** conduct functionality tests using hardware provided by the manufacturer that meets the minimum configuration specifications defined by the manufacturer.

Section 5 provides additional information on hardware to be used to conduct functionality testing of such voting devices, as well as hardware to be used to conduct security testing and other forms of testing.

5 Hardware Testing

Table of Contents

5	Hardware Testing	59
5.1	**Scope**	**59**
5.2	**Basis of Hardware Testing**	**59**
5.2.1	Testing Focus and Applicability	59
5.2.2	Hardware Provided by Manufacturer	60
5.3	**Test Conditions**	**60**
5.4	**Test Log Data Requirements**	**60**
5.5	**Test Fixtures**	**61**
5.6	**Non-operating Environmental Tests**	**61**
5.6.1	General	61
5.6.2	Bench Handling Test	63
5.6.3	Vibration Test	64
5.6.4	Low Temperature Test	65
5.6.5	High Temperature Test	66
5.6.6	Humidity Test	66
5.7	**Operational Tests**	**67**
5.7.1	Operating Temperature and Humidity Tests	67
5.7.2	Reliability Assessment	68
5.8	**Other Environmental Tests**	**68**

5 Hardware Testing

5.1 Scope

This section contains a description of the testing to be performed to confirm the proper functioning of the hardware components of a voting system. It describes the scope and basis for functionality testing, required test conditions for conducting hardware testing, guidance for the use of test fixtures, test log data requirements, and test practices for specific non-operating and operating environmental tests.

5.2 Basis of Hardware Testing

This section addresses the focus and applicability of hardware testing and specifies the manufacturer's obligations to produce hardware to conduct such tests.

5.2.1 Testing Focus and Applicability

The VSTL **shall** design and perform procedures that test the voting system hardware requirements identified in Volume I, Section 4. Test procedures **shall** be designed and performed for both operating and non-operating environmental tests:

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 Guidelines.

The specific testing procedures to be used **shall** be identified in the National Certification Test Plan prepared by the VSTL. 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 VSTL.

5.2.2 Hardware Provided by Manufacturer

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

5.3 Test Conditions

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

When a test is to be performed at "standard" or "ambient" conditions, this requirement **shall** refer to a nominal laboratory environment at prevailing atmospheric pressure and relative humidity.

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

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

5.4 Test Log Data Requirements

The VSTL **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 VSTL 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.

5.5 Test Fixtures

The VSTL **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 VSTL 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 VSTL 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 VSTL 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.

5.6 Non-operating Environmental Tests

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

5.6.1 General

Environmental tests of non-operating equipment are intended to simulate exposure to physical shock and vibration associated with handling and transportation of voting equipment and precinct counters between a jurisdiction's storage facility and precinct polling places. These tests additionally simulate the temperature and humidity conditions that may be encountered during storage in an uncontrolled warehouse environment or precinct environment. The procedures and conditions of these tests correspond generally

to those of MIL-STD-810D, "Environmental Test Methods and Engineering Guidelines," 19 July 1983. In most cases, the severity of the test conditions has been reduced to reflect commercial, rather than military, practice.

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

Prior to each test, the equipment **shall** be shown to be operational by means of the procedure contained in Subsection 5.6.1.5. The equipment may then be prepared as if for actual transportation or storage, and subjected to appropriate test procedures outlined. After each procedure has been completed, the equipment status will again be verified as in Subsection 5.6.1.5.

The following requirements (5.6.1.1 through 5.6.1.6) for equipment preparation, functional tests, and inspections **shall** apply to each of the non-operating test procedures.

5.6.1.1 Pretest Data

The test technician **shall** verify that the equipment is capable of normal operation. Equipment identification, environmental conditions, equipment configuration, test instrumentation, operator tasks, time-of-day or test time, and test results **shall** be recorded.

5.6.1.2 Preparation for Test

The equipment **shall** be prepared as for the expected non-operating use, as noted below. When preparation for transport between the storage site and the polling place is required, the equipment **shall** be prepared with any protective enclosures or internal restraints that the 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.

5.6.1.3 Mechanical Inspection and Repair

After the test has been completed, the devices **shall** be removed from their containers, and any internal restraints **shall** be removed. The exterior and interior of the devices **shall** be inspected for evidence of mechanical damage, failure, or dislocation of internal components. Devices **shall** be adjusted or repaired, if necessary.

5.6.1.4 Electrical Inspection and Adjustment

After completion of the mechanical inspection and repair, routine electrical maintenance and adjustment may be performed, according to the manufacturer's standard procedure.

5.6.1.5 Operational Status Check

When all tests, inspections, repairs, and adjustments have been completed, normal operation **shall** be verified by conducting an operational status check.

During this process, all equipment **shall** be operated in a manner and under environmental conditions that simulate election use to verify the functional status of the system. Prior to the conduct of each of the environmental hardware non-operating tests, a supplemental test **shall** be made to determine that the operational state of the equipment is within acceptable performance limits.

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

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

5.6.1.6 Failure Criteria

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

5.6.2 Bench Handling Test

The bench handling test simulates stresses faced during maintenance and repair of voting machines and ballot counters.

5.6.2.1 Applicability

All systems and components, regardless of type, **shall** meet the requirements of this test. This test is equivalent to the procedure of MIL-STD-810D, Method 516.3, Procedure VI.

5.6.2.2 Procedure

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

5.6.3 Vibration Test

The vibration test simulates stresses faced during transport of voting machines and ballot counters between storage locations and polling places.

5.6.3.1 Applicability

All systems and components, regardless of type, **shall** meet the requirements of this test. This test is equivalent to the procedure of MIL-STD-810D, Method 514.3, Category 1-Basic Transportation, Common Carrier.

5.6.3.2 Procedure

Step 1: Install the test item in its transit or combination case as prepared for transport.
Step 2: Attach instrumentation as required to measure the applied excitation.
Step 3: Mount the equipment on a vibration table with the axis of excitation along the vertical axis of the equipment.

Step 4: Apply excitation as shown in MIL-STD-810D, Method 514.3-1, "Basic transportation, common carrier, vertical axis", with low frequency excitation cutoff at 10 Hz, for a period of 30 minutes.
Step 5: Repeat steps 2 and 3 for the transverse and longitudinal axes of the equipment with the excitation profiles shown in Figures 514.3-2 and 514.3-3, respectively. (Note: The total excitation period equals 90 minutes, with 30 minutes excitation along each axis.)
Step 6: Remove the test item from its transit or combination case and verify its continued operability.

5.6.4 Low Temperature Test

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

5.6.4.1 Applicability

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

5.6.4.2 Procedure

Step 1: Arrange the equipment as for storage. Install it in the test chamber.
Step 2: Lower the internal temperature of the chamber at any convenient rate, but not so rapidly as to cause condensation in the chamber, and in any case no more rapidly than 10 degrees F per minute, until an internal temperature of -4 degrees F has been reached.
Step 3: Allow the chamber temperature to stabilize. Maintain this temperature for a period of 4 hours after stabilization.
Step 4: Allow the internal temperature of the chamber to return to standard laboratory conditions, at a rate not exceeding 10 degrees F per minute.
Step 5: Allow the internal temperature of the equipment to stabilize at laboratory conditions before removing it from the chamber.
Step 6: Remove the equipment from the chamber and from its containers, and inspect the equipment for evidence of damage.
Step 7: Verify continued operability of the equipment.

5.6.5 High Temperature Test

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

5.6.5.1 Applicability

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

5.6.5.2 Procedure

Step 1: Arrange the equipment as for storage. Install it in the test chamber.
Step 2: Raise the internal temperature of the chamber at any convenient rate, but in any case no more rapidly than 10 degrees F per minute, until an internal temperature of 140 degrees F has been reached.
Step 3: Allow the chamber temperature to stabilize. Maintain this temperature for a period of 4 hours after stabilization.
Step 4: Allow the internal temperature of the chamber to return to standard laboratory conditions, at a rate not exceeding 10 degrees F per minute.
Step 5: Allow the internal temperature of the equipment to stabilize at laboratory conditions before removing it from the chamber.
Step 6: Remove the equipment from the chamber and from its containers, and inspect the equipment for evidence of damage.
Step 7: Verify continued operability of the equipment.

5.6.6 Humidity Test

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

5.6.6.1 Applicability

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

5.6.6.2 Procedure

Step 1: Arrange the equipment as for storage. Install it in the test chamber.
Step 2: Adjust the chamber conditions to those given in MIL-STD-810D Table 507.2-I, for the time 0000 of the HotHumid cycle (Cycle 1).
Step 3: Perform a 24-hour cycle with the time and temperature-humidity values specified in Figure 507.2-1, Cycle 1.
Step 4: Repeat Step 2 until 5, 24-hour cycles have been completed.
Step 5: Continue with the test commencing with the conditions specified for time = 0000 hours.
Step 6: At any convenient time in the interval between time = 120 hours and time = 124 hours, place the equipment in an operational configuration, and perform a complete operational status check as defined in Subsection 5.6.1.5.
Step 7: If the equipment satisfactorily completes the status check, continue with the sixth 24-hour cycle.
Step 8: Perform 4 additional 24-hour cycles, terminating the test at time = 240 hours.
Step 9: Remove the equipment from the test chamber and inspect it for any evidence of damage.
Step 10: Verify continued operability of the equipment.

5.7 Operational Tests

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

5.7.1 Operating Temperature and Humidity Tests

All voting systems **shall** be tested in accordance with the appropriate procedures of MIL-STD-810D, "Environmental Test Methods and Engineering Guidelines".

5.7.1.1 Operating Temperature

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.

5.7.1.2 Operating Humidity

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

5.7.2 Reliability Assessment

There is no longer a separate operational test for reliability. Instead, the manufacturer's reliability engineering **shall** be validated by the VSTL in two ways:

a. The VSTL'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 of Volume I Section 4.3.3.4, and conformity to best practices.
b. 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 VSTL **shall** report a finding on whether the observed performance validates or refutes the manufacturer's reliability analysis, or falls short of statistical significance.

5.8 Other Environmental Tests

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

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.*[1]

---

[1] The italicized text is based on EAC Decision on Request for Interpretation 2010-01, http://www.eac.gov/assets/1/Page/EAC%20Decision%20on%20Voltage%20Levels%20and%20ESD%20Test.pdf.

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).

6 Software Testing

Table of Contents

6	Software Testing	71
6.1	**Scope**	**71**
6.2	**Basis of Software Testing**	**71**
6.3	**Initial Review of Documentation**	**72**
6.4	**Source Code Review**	**72**

6 Software Testing

6.1 Scope

This section contains a description of the testing to be performed by the VSTL to confirm the proper functioning of the software components of a voting system submitted for certification testing. It describes the scope and basis for software testing, the initial review of documentation to support software testing, and the review of the voting system source code. Further testing of the voting system software is addressed in the following sections:

a. Section 4 for specific tests of voting system functionality
b. Section 7 for testing voting system security and for testing the operation of the voting system software together with other voting system components

6.2 Basis of Software Testing

The VSTL **shall** design and perform procedures that test the voting system software requirements identified in Volume I, Section 5.

The applicability of different categories of requirements and tests to different kinds of logic (application logic, border logic, third-party logic, and COTS) is described in Volume I, Section 5.2.1. 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 VSTL **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 VSTL. The VSTL 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 National Certification Test Plan prepared by the VSTL. 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 VSTL.

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

6.3 Initial Review of Documentation

Prior to initiating the software review, the VSTL **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

6.4 Source Code Review

Although the following requirements are scoped to application logic (see Volume I, Section 5.2.1), 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 of Volume I, Section 5.2. This **shall** include an assessment of the extent to which the application logic adheres to the published, credible coding standard chosen by the manufacturer in accordance with Volume I, Section 5.2.3.

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.

7 System Integration Testing

Table of Contents

7	System Integration Testing	74
7.1	**Scope**	**74**
7.2	**Basis of Integration Testing**	**74**
7.2.1	Testing Breadth	74
7.2.2	System Baseline for Testing	75
7.2.3	Testing Volume	75
7.3	**Testing Interfaces of System Components**	**75**
7.4	**Security Testing**	**76**
7.4.1	Access Control	77
7.4.2	Data Interception and Disruption	77
7.5	**Usability and Accessibility Testing**	**78**
7.6	**Physical Configuration Audit**	**78**
7.7	**Functional Configuration Audit**	**79**

7 System Integration Testing

7.1 Scope

This section contains a description of the testing to be performed by the VSTL to confirm the proper functioning of the fully integrated components of a voting system submitted for national certification testing. It describes the scope and basis for integration testing, testing of internal and external system interfaces, testing of security capabilities, and the configuration audits, including the testing of system documentation.

System level certification tests address the integrated operation of both hardware and software, along with any telecommunications capabilities. The system level certification tests **shall** include the tests (functionality, volume, stress, usability, security, performance, and recovery) indicated in the National Certification Test Plan, described in Appendix A. These tests assess the system's response to a range of both normal and abnormal conditions initiated in an attempt to compromise the system. These tests may be part of the audit of the system's functional attributes, or may be conducted separately.

The system integration tests include two audits: a Physical Configuration Audit that focuses on physical attributes of the system, and a Functional Configuration Audit that focuses on the system’s functional attributes, including attributes that go beyond the specific requirements of the Standards.

7.2 Basis of Integration Testing

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

7.2.1 Testing Breadth

The VSTL **shall** design and perform procedures that test the voting system capabilities for the system as a whole. These procedures follow the testing of the systems hardware and software, and address voting system requirements defined in Volume I, Sections 2, 4, 5 and 6. These procedures **shall** also address the requirements for testing system functionality provided in Volume I, Section 3. 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 VSTL **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 VSTL. 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 VSTL **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 National Certification 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 VSTL.

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

7.2.2 System Baseline for Testing

The system level certification tests are conducted using the version of the system intended to be sold by the manufacturer and delivered to jurisdictions. To ensure that the system version tested is the correct version, the VSTL **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 VSTL **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.

7.2.3 Testing Volume

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

7.3 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 National Certification 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 Guidelines.

Some voting systems may use components or subsystems from previously tested and qualified systems, such as ballot preparation. For these scenarios, the VSTL **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

Some systems use telecommunications capabilities. For those systems that do use such capabilities, components that are located at the polling place or separate vote counting location **shall** be tested for effective interface, accurate vote transmission, failure detection, and failure recovery. For voting systems that use telecommunications lines or networks that are not under the control of the election official (e.g., public telephone networks), the VSTL **shall** test the interface of manufacturer-supplied components with these external components for effective interface, vote transmission, failure detection, and failure recovery.

7.4 Security Testing

The VSTL **shall** design and perform test procedures that test the security capabilities of the voting system against the requirements defined in Volume I, Section 7. These procedures **shall** focus on the ability of the system to detect, prevent, log, and recover from the broad range of security risks identified. These procedures **shall** also examine system capabilities and safeguards claimed by the 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.

For systems that use public telecommunications networks, including the Internet, to transmit election management data or official election results (such as ballots or tabulated results), the VSTL **shall** conduct tests to ensure that the system provides the necessary identity-proofing, confidentiality, and integrity of transmitted data. These tests **shall** be designed to confirm that the system is capable of detecting, logging, preventing, and recovering from types of attacks known at the time the system is submitted for certification.

The VSTL 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 VSTL may conduct or simulate attacks on the system to confirm the effectiveness of the system's security capabilities, employing test procedures approved by the EAC.

7.4.1 Access Control

The accredited testing laboratory **shall** conduct tests of system capabilities and review the access control policies and procedures submitted by the 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 VSTL **shall** design tests to confirm that these security elements work as specified.

Specific activities to be conducted by the accredited testing laboratory **shall** include:

a. A review of the manufacturer's access control policies, procedures and system capabilities to confirm that all requirements of Volume I, Subsection 7.2 have been addressed completely
b. Specific tests designed by the VSTL 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 (as described in Volume I, Subsection 7.4)
    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.

7.4.2 Data Interception and Disruption

For systems that use telecommunications to transmit official voting data, the VSTL **shall** review, and conduct tests of, the data interception and prevention safeguards specified by the manufacturer in its TDP. The VSTL **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.

For systems that use public communications networks the VSTL **shall** also review the manufacturer's documented procedures for maintaining protection against newly

discovered external threats to the telecommunications network. This review **shall** assess the adequacy of such procedures in terms of:

a. Identification of new threats and their impact
b. Development or acquisition of effective countermeasures
c. System testing to ensure the effectiveness of the countermeasures
d. Notification of client jurisdictions that use the system of the threat and the actions that should be taken
e. Distribution of new system releases or updates to current system users
f. Confirmation of proper installation of new system releases

7.5 Usability and Accessibility Testing

The manufacturer **shall** design and perform procedures that test the usability and accessibility of the voting system as defined in Volume I, Section 3. Test procedures **shall** confirm that:

a. All voting machines meet the usability requirements specified in Volume I, Subsection 3.2
b. Voting machines intended for use by voters with disabilities provide the capabilities required by Volume I, Subsection 3.3
c. Voting machines intended for use by voters with disabilities operate consistently with manufacturer specifications and documentation

7.6 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 test agency **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 VSTL **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.

7.7 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 VSTL **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 VSTL **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 VSTL **shall** design and conduct all appropriate module and integrated functional tests. The functional configuration audit may be performed in the facility either of the VSTL or of the manufacturer, 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.

8 Quality Assurance and Configuration Management

Table of Contents

8 Quality Assurance and Configuration Management 81

8.1 Examination of the Quality and Configuration Management Manual 81

8.2 Configuration Management Testing 81

8 Quality Assurance and Configuration Management

8.1 Examination of the Quality and Configuration Management Manual

Upon its receipt by the Certification Authority, the Quality and Configuration Management Manual **shall** be reviewed for its fulfillment of Volume I, Section 8.1.a and the requirements specified in Volume II, Section 2.1 "Quality and Configuration Management Manual."

8.2 Configuration Management Testing

These requirements deal with the configuration management examination of voting systems submitted for testing to a test lab.

a. The VSTL **shall** verify that the voting system components have appropriate an identification tags attached to the main body as described in Volume I, 8.2.a.
b. The VSTL **shall** verify that the voting system components have a Voting System Configuration Log, as defined in Volume I, Section8.2.b.

Appendix A: National Certification Test Plan

Table of Contents

Appendix A:	National Certification Test Plan	2
A.1	**Test Plan Format**	**2**
A.2	**Required Content of Test Plan**	**4**
A.3	**Test Case Design**	**8**
A.3.1	Hardware Qualitative Examination Design	9
A.3.2	Hardware Environmental Test Case Design	9
A.3.3	Software Module Test Case Design and Data	10
A.3.4	Software Functional Test Case Design	10
A.3.5	System-level Test Case Design	12

Appendix A: National Certification Test Plan

The primary purpose of the test plan is to document the VSTL's development of the certification tests conducted on a voting system submitted as a candidate for certification. Although this appendix serves as a general guide to preparing test plans, VSTLs may tailor the scope and detail of these requirements to the design of the specific voting system submitted for testing, the type of hardware components submitted for testing, and the complexity of the software submitted for testing.

A.1 Test Plan Format

The outline below is provided as an aid to Test Plan development. The outline (in particular, the lower-level subsections) may change significantly depending on the specific project planned.

1. Introduction

    1.1 References

    1.2 Terms and Abbreviations

    1.3 Testing Responsibilities

        1.3.1 Project schedule

            1.3.1.1 Owner assignments

            1.3.1.2 Test case development

            1.3.1.3 Test procedure development and validation

            1.3.1.4 3rd party tests

            1.3.1.5 EAC and Manufacturer dependencies

    1.4 Target of Evaluation Description

        1.4.1 System Overview

        1.4.2 Block diagram

        1.4.3 System Limits

        1.4.4 Supported Languages

1.4.5 Supported Functionality

1.4.5.1 Standard (VVSG) Functionality

1.4.5.2 Manufacturer Extensions

2 Pre-Certification Testing and Issues

2.1 Evaluation of prior VSTL testing

2.2 Evaluation of prior non-VSTL testing

2.3 Known field issues

3. Materials Required for Testing

3.1 Software

3.2 Equipment

3.3 Test materials

3.4 Deliverable materials

4. Test Specifications

4.1 Requirements

4.1.1 Mapping of requirements to equipment type and features

4.1.2 Rationale for why some requirements are NA for this campaign

4.2 Hardware configuration and design

4.3 Software system functions

4.4 Test Case Design

4.4.1 Hardware Qualitative Examination Design

4.4.1.1 Mapping of requirements to specific interfaces

4.4.2 Hardware Environmental Test Case Design

4.4.3 Software Module Test Case Design and Data

4.4.4 Software Functional Test Case Design and Data

4.4.5 System-level Test Case Design

4.5 Security functions

4.6 TDP evaluation

4.7 Source code review

4.8 QA & CM system review

5. Test Data

5.1 Test data recording

5.2 Test data criteria

5.3 Test data reduction

6. Test Procedure and Conditions

6.1 Facility requirements

6.2 Test set-up

6.3 Test sequence

7. Proprietary Data

A.2 Required Content of Test Plan

Introduction

This section of the plan **shall** include:

- A statement indicating the scope of the VSTL's accreditation;
- The scope of the testing engagement;
- A copy of the implementation statement provided by the manufacturer and any interpretations made by the VSTL to fully identify the system under test;
- Identification of applicable voting system standards and a description of the testing proposed to verify conformance.

References. Test Plan references **shall** list all documents containing materials used to prepare the test plan. This **shall** include specific references to applicable portions of the guidelines and to the manufacturer's TDP.

Terms and Abbreviations. The VSTL **shall** list and define all terms and phrases relevant to the hardware, the software, or the test plan.

Testing Responsibilities. The VSTL **shall** identify all parties responsible for conducting testing of the candidate voting system, including all subcontracted testing laboratories and all engineers assigned to the test engagement, and supply a project schedule. The schedule **shall** highlight any dependencies on the level of system development, the testability of the voting system, and the VSTL's assessment of risks associated with the test campaign.

Target of Evaluation Description. The VSTL **shall** describe the system under test.

Pre-Certification Testing and Issues

The VSTL **shall** document all previous certifications, reviews or other testing that may impact the VSTL's determination of the scope of the conformity assessment testing for the candidate voting system. The VSTL may recognize certifications, and tests conducted by other labs, including non-VSTLs, as making some portions of the voting system testing redundant. For example, a COTS computer should already have been certified to comply with the rules and regulations of the Federal Communications Commission (FCC), Part 15, Subpart B requirements for both radiated and conducted emissions and need not be retested for this requirement. Also, if a slightly modified system is submitted for reassessment, the VSTL's argument that some of the previous testing need not be repeated would be documented in this section of the Test Plan.

Evaluation of prior VSTL testing. The VSTL **shall** include the reasons for testing, results, and listings of modifications from the previous to the current systems.

Evaluation of prior non-VSTL testing. Similarly, for relevant non-VSTL testing (e.g., for states or other 3rd party entities), the VSTL **shall** include the reasons for testing, results, and listings of modifications from the previous to the current systems.

Known field issues. The VSTL **shall** list relevant issues uncovered during field operations.

Materials Required for Testing

The VSTL **shall** enumerate all materials needed to enable the test engagement to occur. These materials include not only the applicable hardware and software, but also the Technical Data Package (TDP), test ballots, test data, and all other materials necessary to conduct appropriate testing. All materials delivered to the VSTL **shall** be identified by specific version number, product number, serial number, etc., if appropriate, and the quantity of each item delivered **shall** be noted.

Software. The VSTL **shall** list all software required for the performance of hardware, software, telecommunications, security and system integration tests. If the test environment requires supporting software such as operating systems, compilers, assemblers, or database managers, then this software **shall** also be listed.

Equipment. The VSTL **shall** list all equipment required for the performance of the hardware, software, telecommunications, security and system integration tests. This list **shall** include system hardware, general purpose data processing and communications equipment, and test instrumentation, as required.

Test materials. The VSTL **shall** list all test materials required in the performance of the test including, as applicable, test ballot layout and generation materials, test ballot sheets, test ballots and control cards, standard and optional output data report formats, and any other materials used to simulate preparation for, and conduct of, elections.

Deliverable materials. The VSTL **shall** list all documents and materials to be delivered as a part of the system, such as:

Hardware specification
Software specification
Voter, operator, hardware, and software maintenance manuals
Program listings, facsimile ballots, media
Sample output report formats

Test Specifications

For all applicable tests specified in the VVSG, the VSTL **shall** document the implementation details that determine how the standard tests are realized for the system under test. For all tests that the VSTL is adopting from publicly available test suites, the VSTL **shall** identify the public reference and document the implementation details that determine how the public tests are realized for the voting system under test. For all other tests, the VSTL **shall** incorporate all relevant information into the test plan as needed to identify the test methods and document the implementation details that determine how the test methods are to be applied to the voting system under test.

The VSTL **shall** cite the pertinent hardware qualitative examinations and quantitative tests that follow from Volume I, Sections 2, 4, 5, 6, 7 and 8. The VSTL **shall** also describe the specific test requirements that follow from the design of the software and telecommunications capabilities under test.

The certification tests **shall** include hardware, software and telecommunications design and the development and conduct of all tests to demonstrate satisfactory performance. Environmental, non-operating tests **shall** be performed in the categories of simulated environmental conditions specified by the manufacturer or user requesting the tests. Environmental operating tests **shall** be performed under varying temperatures. Other functional tests **shall** be conducted in an environment that simulates, as nearly as possible, the intended use environment.

Test hardware and software **shall** be identical to that designed to be used together in the voting system, except that software intended for use with general purpose off-the-shelf hardware may be tested using any equivalent equipment capable of supporting its operation and functions.

Hardware Configuration and Design. The VSTL **shall** document the hardware configuration and design in detail sufficient to identify the specific equipment being tested. This document **shall** provide a basis for the specific test design and include a brief description of the intended use of the hardware.

Software System Functions. The VSTL **shall** describe the software functions in sufficient detail to provide a foundation for selecting test case designs and conditions. On the basis of this test case design, the VSTL **shall** prepare a table delineating software functions and how each **shall** be tested.

Test Case Design. See Section A.3 for details on the Test Case Design portion of the Test Plan.

Security functions.

TDP evaluation.

Source code review.

QA & CM system review.

Test Data

Test Data Recording. The VSTL **shall** identify what data is to be measured, and how tests and results are recorded. The VSTL **shall** supply any special instrumentation needed to satisfy the data requirements.

Test Data Criteria. The VSTL **shall** describe the criteria against which the results will be evaluated, including but not limited to criteria defining the acceptable range for voting system conformance (tolerances); criteria defining the minimum number of combinations or alternatives of input and output conditions that can be exercised to constitute an acceptable test of the parameters involved (sampling); and criteria defining the maximum number of interrupts, halts or other system breaks that may occur due to non-test conditions (events).

Test Data Reduction. The VSTL **shall** describe the techniques to be used for processing test data. These techniques may include manual, semi-automatic, or fully automatic reduction procedures. However, semi-automatic and automatic procedures must be demonstrated to be capable of handling the test data accurately and properly. They **shall** also produce an item-by-item comparison of the data and the embedded acceptance criteria as output.

Test Procedures and Conditions

The VSTL **shall** provide the information necessary to specify the testing that it performs. This information includes facility requirements, test set-up, test sequence, and pass criteria. Any description of a test procedure **shall** contain a statement of the criteria by which readiness and successful completion **shall** be indicated and measured.

Facility Requirements. The VSTL **shall** describe the space, equipment, instrumentation, utilities, manpower, and other resources required to support the test program.

Test Set-up. The VSTL **shall** describe the procedure for arranging and connecting the system hardware with the supporting hardware and telecommunications equipment, if applicable. It **shall** also describe the procedure required to initialize the system, and to verify that it is ready to be tested.

Test Sequence. The VSTL **shall** state any restrictions on the grouping or sequence of tests in this section.

Proprietary Data

The VSTL **shall** list and describe in this section all documentation and data that are proprietary to the Manufacturer and hence subject to restrictions on use, release, or disclosure. All proprietary data and information must be included in this section, preferably as a separate electronic file, in order to easily publish the test plans on the EAC Web site while withholding information considered proprietary or confidential by Federal law.

VSTLs **shall** identify protected information by taking the following action:

a. *Submitting a Notice of Protected Information*. This notice **shall** identify the document, document page, or portion of a page that the VSTL believes should be protected from release. This identification must be done with specificity. For each piece of information identified, the VSTL 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 VSTL 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. *Label 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.

A.3 Test Case Design

The VSTL **shall** examine the test case design of the following aspects of the voting system:

- Hardware qualitative examination design
- Hardware environmental test case design
- Software module test case design and data

- Software functional test case design
- System level test case design

A.3.1 Hardware Qualitative Examination Design

The VSTL **shall** review the results, submitted by the manufacturer, of any previous examinations of the equipment to be tested. The results of these examinations **shall** be compared to the performance characteristics specified by Volume I, Chapter 2 of the Guidelines concerning the requirements for:

- Overall system capabilities
- Pre-voting functions
- Voting functions
- Post-voting functions

In the event that a review of the results of previous examinations indicates problem areas, the VSTL **shall** provide a description of further examinations required prior to conducting the environmental and system level tests. If no previous examinations have been performed, or records of these tests are not available, the VSTL **shall** specify the appropriate tests to be used in the examination.

A.3.2 Hardware Environmental Test Case Design

The VSTL **shall** review the documentation, submitted by the manufacturer, of the results and design of any previous environmental tests of the equipment submitted for testing. The test design and results **shall** be compared to the tests described in Volume II, Section 5. The VSTL **shall** cite any additional tests required, based on this review and those tests requested by the manufacturer or the state. The VSTL **shall** also cite any environmental tests that are not to be conducted, and note the reasons why.

For complete certification, environmental tests **shall** include the following tests, depending upon the design and intended use of the hardware:

- Non-operating tests, including the:
    - Bench handling test
    - Vibration test
    - Low temperature test
    - High temperature test
- Operating tests involving a series of procedures that test system reliability and accuracy under various temperatures, humidities and voltages relevant to election use

A.3.3 Software Module Test Case Design and Data

The VSTL **shall** review the manufacturer's program analysis, documentation, and module test case design. The VSTL **shall** evaluate the test cases for each module, with respect to flow control parameters and data on both entry and exit. All discrepancies between the Software Specifications and the test case design **shall** be corrected by the manufacturer prior to initiation of certification testing.

The VSTL **shall** design additional test cases as needed to satisfy the coverage criteria specified in Volume II, Section 7.2.1

The VSTL **shall** also review the manufacturer's module test data in order to verify that the requirements of the Software Specifications have been demonstrated by the data. In the event that the manufacturer's module test data are insufficient, the VSTL **shall** provide a description of additional module tests, prerequisite to the initiation of functional tests.

A.3.4 Software Functional Test Case Design

The VSTL **shall** review the manufacturer's test plans and data to verify that the individual performance requirements specified in the VVSG (Volume I) and the TDP (Volume II, Section 4.4, Functional Specification) are reflected in the software.

As a part of this process, the VSTL **shall** review the manufacturer's functional test case designs. The VSTL **shall** prepare a detailed matrix of system functions and the test cases that exercise them. The VSTL **shall** also prepare a test procedure describing all test ballots, operator procedures, and the data content of output reports. Abnormal input data and operator actions **shall** be defined. Test cases **shall** also be designed to verify that the system is able to handle and recover from these abnormal conditions.

The manufacturer's test case design may be evaluated by any standard or special method appropriate; however, emphasis **shall** be placed on those functions where the manufacturer data on module development reflects significant debugging problems, and on functional tests that resulted in disproportionately high error rates.

The VSTL **shall** define ACCEPT/REJECT criteria for certification using the Software Specifications and, if the software runs on special hardware, the associated Hardware Specifications to determine acceptable ranges of performance.

The VSTL **shall** describe the functional tests to be performed. Depending upon the design and intended use of the voting system, all or part of the functions listed below **shall** be tested.

Ballot preparation subsystem

Test operations performed prior to, during, and after processing of ballots, including:

Logic tests to verify interpretation of ballot styles, and recognition of precincts to be processed

Accuracy tests to verify ballot reading accuracy

Status tests to verify equipment statement and memory contents

Report generation to produce test output data

Report generation to produce audit data records

Procedures applicable to equipment used in the polling place for:

Opening the polling place and enabling the acceptance of ballots and maintaining a count of processed ballots

Monitoring equipment status

Verifying equipment response to operator input commands

Generating real-time audit messages

Closing the polling place and disabling the acceptance of ballots

Generating election data reports

Transfer of ballot counting equipment, or a detachable memory module, to a central counting location

Electronic transmission of election data to a central counting location

Procedures applicable to equipment used in a central counting place:

Initiating the processing of a ballot deck or programmable memory device for one or more precincts

Monitoring equipment status

Verifying equipment response to operator input commands

Verifying interaction with peripheral equipment, or other data processing systems

Generating real-time audit messages

Generating precinct-level election data reports

Generating summary election data reports

Transfer of a detachable memory module to other processing equipment

Electronic transmission of data to other processing equipment

Producing output data for interrogation by external display devices

A.3.5 System-level Test Case Design

The VSTL **shall** provide a description of system tests of both the software and hardware. For software, these tests **shall** be designed according to the stated design objective without consideration of its functional specification. The VSTL **shall** independently prepare the system test cases to assess the response of the hardware and software to a range of conditions, such as:

Volume tests: These tests investigate the system's response to processing more than the expected number of ballots/voters per precinct, to processing more than the expected number of precincts, or to any other similar conditions that tend to overload the system's capacity to process, store, and report data.

Stress tests: These tests investigate the system's response to transient overload conditions. Polling place devices **shall** be subjected to ballot processing at the high volume rates at which the equipment can be operated to evaluate software response to hardware-generated interrupts and wait states. Central counting systems **shall** be subjected to similar overloads, including, for systems that support more than one card reader, continuous processing through all readers simultaneously.

Usability tests: These tests are designed to exercise characteristics of the software such as response to input control or text syntax errors, error message content, audit message content, and other features contained in the software design objectives but not directly related to a functional specification.

Accessibility tests: The VSTL **shall** review the manufacturer’s documentation of the usability and accessibility testing performed during system development.

Security tests: These tests are designed to defeat the security provisions of the system including modification or disruption of pre-voting, voting, and post voting processing; unauthorized access to, deletion, or modification of data, including audit trail data; and modification or elimination of security mechanisms.

Performance tests: These tests verify accuracy, processing rate, ballot format handling capability, and other performance attributes claimed by the manufacturer.

Recovery tests: These tests verify the ability of the system to recover from hardware and data errors.

A.4 Test Plans for Modifications to Previously Certified Systems

Test Plans submitted for modifications to previously EAC certified voting systems should be brief and structured to minimize test plan development and review, while enabling the EAC to maintain solid control of the certification process. The test plan **shall** *concisely* document the strategy and plan for testing those sections of the VVSG applicable to the modification or modifications submitted. The test plan **shall** be written with clarity that will allow all constituents to understand what testing will be conducted, to verify compliance to VVSG requirements, and to assure that the test plan will remain a living document throughout the life of the test campaign for the modification.

For changes and modifications of previously EAC certified voting systems, the purpose of a test plan is to communicate the extent of testing activities to be undertaken by an EAC accredited VSTL. Care should be taken to clearly communicate the scope and requirements of testing, the test strategies, and the resource needs. In order to accomplish these goals the following general topics **shall** be included in all modification test plans.

- Complete definition of the baseline certified system.
- Detailed description of all the engineering changes and/or modifications to the certified system and why the modification was implemented.
- An initial assessment of the impact that the changes have on the system and past certification.
- An initial assessment of the impact the changes have on various TDP documents.
- A table or list indicating how each of existing NOC's/RFI's will be addressed and why this plan is valid for this test campaign.
- Description of what will be tested (regression) to establish assurance that the change(s) have no adverse impact on the compliance, integrity or the performance of the equipment.
- Description of what will be tested (regression) to establish assurance that the change(s) create no inconsistencies with the TDP and further are correctly documented and reflected in the TDP.
- A summary of the test methods that will be used to validate compliance. This summary may include, existing, modified or new test methods, test cases or test sequences.
- Titles of test lab personnel who will be responsible for each aspect of the test campaign.
- Detailed project schedule including what the critical path is for timely project completion.

It should be noted that depending on the nature of the change and the extent of testing to be performed, some of the topics in a full certification test plan may be appropriate to enable the modification test plan to be complete. In order to keep the test plan focused on the modification, these should only be included if they add clarity and completeness to the test plan. So items may include:

- Precertification testing and issues
- Materials required for testing

- Test data
- Test procedure and conditions

Appendix B: National Certification Test Report

Table of Contents

Appendix B: National Certification Test Report 2
B.1 Test Report Format 2
B.2 Required Content of Test Report 3

Appendix B: National Certification Test Report

The primary purpose of the test report is to facilitate the presentation of conclusions and recommendations regarding voting system conformance to the VVSG. The test report also provides a summary of test operations, test results, test data records and analysis to support the conclusions and recommendations presented by the VSTL. Although this appendix serves as a general guide to preparing the test reports, VSTLs may tailor the scope and detail of the testing conducted on the candidate voting system.

All test reports **shall** document the testing process, including the documentation and justification of any divergence from the approved test plan, methods, or cases and the identification of all failures and/or anomalies along with any remedial action taken. Test reports **shall** also document any prescribed maintenance or modifications performed by the manufacturer to a voting system under test.

To the greatest extent possible, VSTLs **shall** write reports such that they are understandable to non-technical persons. As the certifying authority may publish these reports (bar portions prohibited by law), VSTLs **shall** refrain from including in them trade secrets or other commercial information protected from release unless substantively required. Where information protected from release may be included, it **shall** be identified consistent with the discussion of proprietary data in Volume II Appendix A.2.

B.1 Test Report Format

Test Reports produced by VSTLs **shall** follow the format outlined below:

1. System Identification and Overview

2. Certification Test Background

    2.1 Revision History

    2.2 Implementation Statement

3. Test Findings and Recommendation

    3.1 Summary Finding and Recommendation

    3.2 Benchmarks

    3.3 Reasons for Recommendation to Reject

    3.4 Anomalies

3.5 Correction of Nonconformities

Appendix A. Additional Findings

Appendix B. Warrant of Accepting Change Control Responsibility

Appendix C. Trusted Build

Appendix D. Test Plan

Appendix E. State Test Reports

B.2 Required Content of Test Report

System Identification and Overview

The VSTL **shall** provide basic information about the voting system software and supporting hardware including the system name and major subsystems or their equivalent and their version numbers. In addition, this section **shall** describe the design and structure of the voting system, technologies used, processing capacity claimed by the Manufacturer for system components such as ballot counters, and vote consolidation equipment. The description of the voting system, both software and hardware, **shall** have enough detail and specificity to allow the identification of a voting system in the field as being either identical to that tested or a modified version of the system. This section may also identify other products that interface with the voting system.

Certification Test Background

For modifications to previously tested voting systems, the VSTL **shall** include references to the test reports that are precedential to the current testing engagement. The VSTL **shall** also include the implementation statement submitted by the manufacturer, amended to reflect any changes that were necessitated during the course of the testing engagement.

Test Findings and Recommendation

This section provides a summary of the results of the testing engagement and indicates any special considerations that affect the conclusions derived from the test results.

The VSTL **shall** present a summary finding of whether or not the voting system, as tested, satisfied all applicable mandatory ("**shall**") requirements of the VVSG. The VSTL **shall** also provide a specific recommendation for approval or rejection of the candidate system.

For requirements that specify benchmarks, the VSTL **shall** report the result of the measurement for the implementation under test. This includes the observed cumulative report total error rate and the report total error rate that was demonstrated with 90 % confidence for the system as a whole, and, for paper-based tabulators and EBMs, the

observed cumulative misfeed rate and the misfeed rate that was demonstrated with 90 % confidence for each type of device.

If the VSTL finds that the voting system under test does not satisfy all applicable mandatory requirements of the VVSG, the VSTL **shall** identify each of the specific requirements that were not satisfied, include a description of the inspections or tests that detected the nonconformities and include any applicable evidence (e.g., vote data report, citation of logic error in source code, etc.). The VSTL **shall** also summarize all failures, errors, nonconformities and anomalies that were observed during the testing engagement. Finally, the VSTL **shall** identify any nonconformities corrected during the course of the test engagement and identify inspections or tests that confirm that the nonconformities were corrected.

Additional Findings

The VSTL **shall** include as Appendix A of the Test Report identification of each applicable non-mandatory test ("shoulds") for which conformity was demonstrated during the testing engagement. Appendix A **shall** also include identification of all tests that were identified as non-applicable to the voting system under test and therefore waived during the test engagement. Appendix A **shall** also include the VSTL response to any additional information, report or review provided by the certifying authority regarding the voting system under testing, and whether or not the items noted in the materials presented have any relevance to the system under test.

Warrant of Accepting Change Control Responsibility

If the manufacturer must make changes to the voting system to successfully complete the conformance testing, the VSTL **shall** include as Appendix B of the Test Report a signed warrant from the manufacturer that those changes will be included in the product that is delivered to customers.

Trusted Build

The VSTL **shall** include as Appendix C of the Test Report a copy of the record of the trusted build, as defined in the current version of the EAC's Voting System Testing & Certification Program Manual, to provide sufficient description of the build process to enable reproduction of the build.

Test Plan

The VSTL **shall** include a copy of the voting system Test Plan, amended to reflect any deviations from the original, approved, test plan during the course of testing.

State Test Reports

The VSTL **shall** include the results or reports from any testing engagement requested by a State to the candidate system conducted concurrent to the certification testing engagement. The results of State test reports **shall** not impact the certification of the

voting system if the system successfully meets all requirements of the VVSG and the Testing and Certification Program.

Appendix C: Assessing Conformity to Benchmarks

Table of Contents

Appendix C: Assessing Conformity to Benchmarks

C.1	**General Method**	**2**
C.2	**Critical Values**	**3**
C.3	**Accuracy**	**8**
C.4	**Misfeed Rate**	**9**
C.5	**Validation of Manufacturer's Reliability Analysis**	**10**

Appendix C: Assessing Conformity to Benchmarks for Accuracy and Misfeed Rate

C.1 General Method

Accuracy and misfeed rate are measured using a ratio of the number of a specific kind of event (errors or misfeeds, respectively) divided by a measure of voting volume (report total volume or ballots). The test method discussed here is applicable generically to any such ratio; hence, this discussion will refer to events and volume without specifying a particular definition of either.

By keeping track of the number of events and the volume over the course of testing, one can trivially calculate the observed cumulative event rate by dividing the number of events by the volume. However, the *observed* event rate is not necessarily a good indication of the *true* event rate.

The *true* event rate describes the expected performance of the system in the field, but it cannot be observed in a test engagement of finite duration, using a finite-sized sample. Consequently, the true event rate must be estimated using statistical methods.

In accordance with the current practice in voting system testing, the system submitted for testing is assumed to be a representative sample, so the variability of devices of the same type is out of scope.

The test method makes the simplifying assumption that the probability of an event occurring is the same for each unit of volume processed. For additional simplicity, all cases are modeled using a Poisson distribution rather than a binomial distribution. When the probability of an event occurring within a unit of volume is small, the difference in results from the two different models is negligible; but if more than one event can occur within a single unit of volume, as is possible both for errors and for misfeeds, the binomial distribution is not applicable.

The problem is approached through classical hypothesis testing. The null hypothesis (H_0) is that the true event rate, r_t, is greater than the benchmark event rate, r_b (which means that the system is non-conforming).

H_0: $r_t > r_b$

The alternative hypothesis (H_1) is that the true event rate, r_t, is less than or equal to the benchmark event rate, r_b (which means that the system is conforming).

H_1: $r_t \leq r_b$

Assuming an event rate of r, the probability of observing n or fewer events for volume v is the value of the Poisson cumulative distribution function,

$$P(n, rv) = \sum_{x=0}^{n} \frac{e^{-rv}(rv)^x}{x!}$$

Let n_o be the number of events observed during testing and v_o be the volume produced during testing. The probability α of rejecting the null hypothesis when it is in fact true is limited to be less than 0.1. Thus, H_0 is rejected only if the probability of n_o or fewer events occurring given a (marginally) conforming system is less than 0.1. So H_0 is rejected only if $P(n_o, r_b v_o)<0.1$. This corresponds to the 10th percentile of the distribution of the number of events that would be expected to occur in a marginally conforming system.

If at the conclusion of testing the null hypothesis is not rejected, this does not necessarily mean that non-conformity has been demonstrated. It merely means that the evidence is insufficient to demonstrate conformity with 90 % confidence.

Calculating what *has* been demonstrated with 90 % confidence, after the fact, is completely separate from the test described above, but the logic is similar. Suppose there are n_o observed events after volume v_o. Solving the equation $P(n_o, r_d v_o)=0.1$ for r_d finds the "demonstrated rate" r_d such that if the true rate r_t were greater than r_d, then the probability of having n_o or fewer events would be less than 0.1. The value of r_d could be greater or less than the benchmark event rate r_b mentioned above.

Please note that the length of testing is determined by the approved test plan. The test plan may be revised, subject to approval, to incorporate regression testing or other needed changes. However, it must never be revised based on the observed accuracy or misfeed rate as this would bias the results. A Probability Ratio Sequential Test (PRST) as was specified in VVSG 1.0 varies the length of testing without introducing bias, but practical difficulties result when the length of testing determined by the PRST disagrees with the length of testing that is otherwise required by the test plan.

C.2 Critical Values

For a fixed probability p and a fixed value of n, the value of rv satisfying $P(n,rv)=p$ is a constant. The table below provides the values of rv for p=0.1 for $0 \leq n \leq 299$.

Since the condition for rejecting H_0 is $P(n_o, r_b v_o)<0.1$, the critical value v_c, which is the maximum volume at which H_0 is not rejected for n_o observed events and event rate benchmark r_b, is found by solving $P(n_o, r_b v_c)=0.1$ for v_c. The pertinent factor is in the second column (rv satisfying $P(n,rv) = 0.1$) in the row for $n=n_o$; dividing this factor by r_b

yields v_c. For example, if a test with event rate benchmark r_b=8×10^{-6} resulted in one observed event, then the system would be rejected unless the actual volume was more than 3.889720/8×10^{-6}, or 486 215.

Similarly, given n_o observed events after volume v_o, the demonstrated event rate r_d is found by dividing the *rv* factor in the row for n=n_o by v_o. For example, a volume of 600 with no events demonstrates an event rate of 2.302585/600, or 3.837642×10^{-3}.

n	***rv* satisfying P(*n*,*rv*) = 0.1**	***n***	***rv* satisfying P(*n*,*rv*) = 0.1**	***n***	***rv* satisfying P(*n*,*rv*) = 0.1**	***n***	***rv* satisfying P(*n*,*rv*) = 0.1**	***n***	***rv* satisfying P(*n*,*rv*) = 0.1**
0	2.302585	**60**	71.19887	**120**	135.2938	**180**	198.4414	**240**	261.0969
1	3.889720	**61**	72.28078	**121**	136.3520	**181**	199.4890	**241**	262.1381
2	5.322320	**62**	73.36203	**122**	137.4100	**182**	200.5365	**242**	263.1793
3	6.680783	**63**	74.44263	**123**	138.4677	**183**	201.5839	**243**	264.2204
4	7.993590	**64**	75.52260	**124**	139.5252	**184**	202.6311	**244**	265.2614
5	9.274674	**65**	76.60196	**125**	140.5825	**185**	203.6781	**245**	266.3023
6	10.53207	**66**	77.68071	**126**	141.6395	**186**	204.7251	**246**	267.3431
7	11.77091	**67**	78.75888	**127**	142.6963	**187**	205.7719	**247**	268.3839
8	12.99471	**68**	79.83647	**128**	143.7529	**188**	206.8186	**248**	269.4246
9	14.20599	**69**	80.91350	**129**	144.8093	**189**	207.8652	**249**	270.4652

10	15.40664	**70**	81.98997	**130**	145.8655	**190**	208.9117	**250**	271.5057
11	16.59812	**71**	83.06591	**131**	146.9214	**191**	209.9580	**251**	272.5461
12	17.78159	**72**	84.14132	**132**	147.9771	**192**	211.0043	**252**	273.5864
13	18.95796	**73**	85.21622	**133**	149.0326	**193**	212.0504	**253**	274.6267
14	20.12801	**74**	86.29061	**134**	150.0880	**194**	213.0963	**254**	275.6669
15	21.29237	**75**	87.36450	**135**	151.1431	**195**	214.1422	**255**	276.7070
16	22.45158	**76**	88.43790	**136**	152.1980	**196**	215.1879	**256**	277.7470
17	23.60609	**77**	89.51083	**137**	153.2527	**197**	216.2336	**257**	278.7870
18	24.75629	**78**	90.58329	**138**	154.3072	**198**	217.2791	**258**	279.8269
19	25.90253	**79**	91.65529	**139**	155.3615	**199**	218.3245	**259**	280.8667
20	27.04510	**80**	92.72684	**140**	156.4156	**200**	219.3698	**260**	281.9064
21	28.18427	**81**	93.79795	**141**	157.4695	**201**	220.4150	**261**	282.9460
22	29.32027	**82**	94.86863	**142**	158.5233	**202**	221.4600	**262**	283.9856
23	30.45330	**83**	95.93888	**143**	159.5768	**203**	222.5050	**263**	285.0251

24	31.58356	**84**	97.00871	**144**	160.6302	**204**	223.5498	**264**	286.0645
25	32.71121	**85**	98.07813	**145**	161.6834	**205**	224.5945	**265**	287.1039
26	33.83639	**86**	99.14714	**146**	162.7364	**206**	225.6392	**266**	288.1432
27	34.95926	**87**	100.2158	**147**	163.7892	**207**	226.6837	**267**	289.1824
28	36.07992	**88**	101.2840	**148**	164.8418	**208**	227.7281	**268**	290.2215
29	37.19850	**89**	102.3518	**149**	165.8943	**209**	228.7724	**269**	291.2605
30	38.31510	**90**	103.4193	**150**	166.9465	**210**	229.8166	**270**	292.2995
31	39.42982	**91**	104.4864	**151**	167.9987	**211**	230.8607	**271**	293.3384
32	40.54274	**92**	105.5531	**152**	169.0506	**212**	231.9047	**272**	294.3773
33	41.65395	**93**	106.6195	**153**	170.1024	**213**	232.9485	**273**	295.4160
34	42.76352	**94**	107.6855	**154**	171.1540	**214**	233.9923	**274**	296.4547
35	43.87152	**95**	108.7512	**155**	172.2054	**215**	235.0360	**275**	297.4934
36	44.97802	**96**	109.8165	**156**	173.2567	**216**	236.0796	**276**	298.5319
37	46.08308	**97**	110.8815	**157**	174.3078	**217**	237.1231	**277**	299.5704

38	47.18676	**98**	111.9462	**158**	175.3587	**218**	238.1664	**278**	300.6088
39	48.28910	**99**	113.0105	**159**	176.4095	**219**	239.2097	**279**	301.6472
40	49.39016	**100**	114.0745	**160**	177.4601	**220**	240.2529	**280**	302.6855
41	50.48999	**101**	115.1382	**161**	178.5106	**221**	241.2960	**281**	303.7237
42	51.58863	**102**	116.2016	**162**	179.5609	**222**	242.3390	**282**	304.7618
43	52.68612	**103**	117.2647	**163**	180.6111	**223**	243.3819	**283**	305.7999
44	53.78250	**104**	118.3275	**164**	181.6611	**224**	244.4247	**284**	306.8379
45	54.87781	**105**	119.3899	**165**	182.7109	**225**	245.4674	**285**	307.8758
46	55.97209	**106**	120.4521	**166**	183.7606	**226**	246.5100	**286**	308.9137
47	57.06535	**107**	121.5140	**167**	184.8102	**227**	247.5525	**287**	309.9515
48	58.15765	**108**	122.5756	**168**	185.8596	**228**	248.5949	**288**	310.9893
49	59.24900	**109**	123.6369	**169**	186.9089	**229**	249.6372	**289**	312.0269
50	60.33944	**110**	124.6980	**170**	187.9580	**230**	250.6795	**290**	313.0646
51	61.42899	**111**	125.7587	**171**	189.0069	**231**	251.7216	**291**	314.1021

52	62.51768	**112**	126.8192	**172**	190.0558	**232**	252.7636	**292**	315.1396
53	63.60553	**113**	127.8794	**173**	191.1045	**233**	253.8056	**293**	316.1770
54	64.69257	**114**	128.9394	**174**	192.1530	**234**	254.8475	**294**	317.2144
55	65.77881	**115**	129.9991	**175**	193.2014	**235**	255.8893	**295**	318.2517
56	66.86429	**116**	131.0586	**176**	194.2497	**236**	256.9310	**296**	319.2889
57	67.94901	**117**	132.1177	**177**	195.2978	**237**	257.9726	**297**	320.3261
58	69.03300	**118**	133.1767	**178**	196.3458	**238**	259.0141	**298**	321.3632
59	70.11628	**119**	134.2354	**179**	197.3937	**239**	260.0555	**299**	322.4002

C.3 Accuracy

All tests executed during conformity assessment **shall** be considered “pertinent” for assessment of accuracy, with the following exceptions:

a. Tests in which errors are forced;
b. Tests in which portions of the system that would be exercised during an actual election are bypassed (see Volume II, Section 1.8.2.3).

The VSTL **shall** record the report total error and report total volume for each pertinent test execution. When operational testing is complete, the VSTL **shall** calculate the report total error and report total volume accumulated across all pertinent tests. If, using the test method in C.1, these values indicate rejection of the null hypothesis, the verdict on conformity to the requirements of Volume I, Section 4.1.1 **shall** be Pass. Otherwise, the verdict **shall** be Fail.

C.4 Misfeed Rate

This benchmark applies only to paper-based tabulators and EBMs.

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.

All tests executed during conformity assessment **shall** be considered "pertinent" for assessment of misfeed rate, with the exception of tests in which misfeeds are forced.

The VSTL **shall** record the misfeed total and total ballot volume for each pertinent test execution, for each type of device (each different model of paper-based tabulator or EBM submitted for testing). When operational testing is complete, the VSTL **shall** calculate the misfeed total and total ballot volume accumulated across all pertinent tests, for each applicable type of device. If, using the test method in C.1, these values indicate rejection of the null hypothesis, the verdict on conformity to the misfeed rate requirements of Volume I, Section 4.1.5.1 **shall** be Pass. Otherwise, the verdict **shall** be Fail.

C.5 Validation of Manufacturer's Reliability Analysis

Requirement Vol. II, 5.7.2.b requires the VSTL to report a finding on whether the observed performance validates or refutes the manufacturer's reliability analysis, or falls short of statistical significance. This finding is obtained using a two-tailed version of the test method that was applied in Appendix C. The null hypothesis in this case is that the

$$H_0 : r_t = r_b$$

true event rate is equal to the benchmark event rate.

The null hypothesis is rejected if the observed number of failures does not fall within a probabilistically symmetric 80 % coverage interval for the number of failures that would be expected given those conditions. If the probability of observing n_o or fewer events given a (marginally) conforming system is less than 0.1, then the manufacturer's reliability analysis is validated by the observed performance. If the probability of observing n_o or more events given a (marginally) conforming system is less than 0.1, then the failure rate was too high and the manufacturer's reliability analysis was refuted by the observed performance. If neither of those two conditions applies, then the observed performance fell short of statistical significance.

The condition for validation uses the same critical values as in Appendix C. The manufacturer's reliability analysis is rejected (refuted) if $1-P(n_o-1,r_bv_o)<0.1$, which is equivalent to $P(n_o-1,r_bv_o)>0.9$. Table X provides the values of rv for $p=0.9$ for $0\leq n\leq 299$.

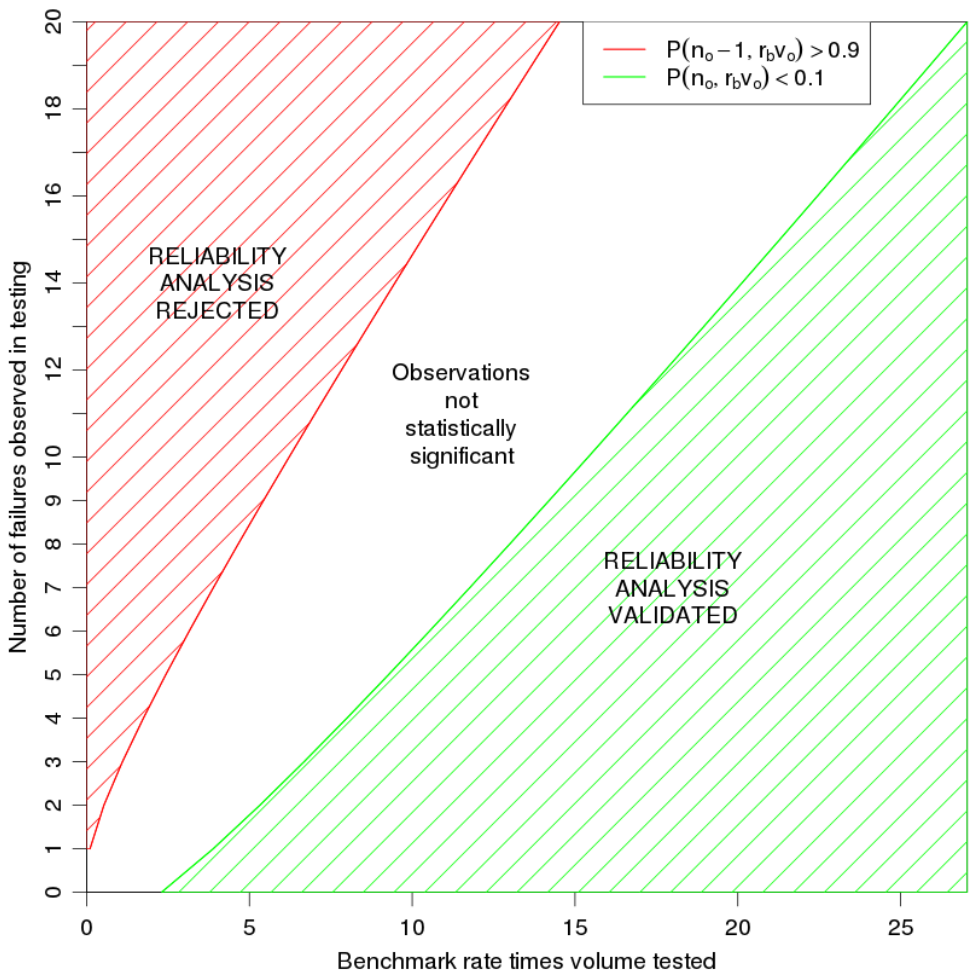

Figure X provides a visualization of the resulting criteria.

n	***rv* satisfying P(*n*,*rv*) = 0.9**	***n***	***rv* satisfying P(*n*,*rv*) = 0.9**	***n***	***rv* satisfying P(*n*,*rv*) = 0.9**	***n***	***rv* satisfying P(*n*,*rv*) = 0.9**	***n***	***rv* satisfying P(*n*,*rv*) = 0.9**
0	0.1053605	**60**	51.22923	**120**	107.1344	**180**	163.9868	**240**	221.3314
1	0.5318116	**61**	52.14733	**121**	108.0762	**181**	164.9392	**241**	222.2901

2	1.102065	**62**	53.06608	**122**	109.0182	**182**	165.8917	**242**	223.2489
3	1.744770	**63**	53.98548	**123**	109.9605	**183**	166.8443	**243**	224.2078
4	2.432591	**64**	54.90551	**124**	110.9030	**184**	167.7971	**244**	225.1668
5	3.151898	**65**	55.82616	**125**	111.8457	**185**	168.7501	**245**	226.1259
6	3.894767	**66**	56.74741	**126**	112.7887	**186**	169.7031	**246**	227.0851
7	4.656118	**67**	57.66924	**127**	113.7318	**187**	170.6563	**247**	228.0443
8	5.432468	**68**	58.59165	**128**	114.6753	**188**	171.6096	**248**	229.0037
9	6.221305	**69**	59.51463	**129**	115.6189	**189**	172.5630	**249**	229.9631
10	7.020747	**70**	60.43815	**130**	116.5627	**190**	173.5165	**250**	230.9226
11	7.829342	**71**	61.36221	**131**	117.5068	**191**	174.4702	**251**	231.8821
12	8.645942	**72**	62.28680	**132**	118.4511	**192**	175.4239	**252**	232.8418
13	9.469621	**73**	63.21191	**133**	119.3955	**193**	176.3778	**253**	233.8015
14	10.29962	**74**	64.13753	**134**	120.3402	**194**	177.3319	**254**	234.7613
15	11.13530	**75**	65.06364	**135**	121.2851	**195**	178.2860	**255**	235.7212

16	11.97613	**76**	65.99023	**136**	122.2302	**196**	179.2403	**256**	236.6812
17	12.82165	**77**	66.91731	**137**	123.1755	**197**	180.1946	**257**	237.6412
18	13.67148	**78**	67.84485	**138**	124.1210	**198**	181.1491	**258**	238.6013
19	14.52526	**79**	68.77285	**139**	125.0667	**199**	182.1037	**259**	239.5615
20	15.38271	**80**	69.70130	**140**	126.0126	**200**	183.0584	**260**	240.5218
21	16.24356	**81**	70.63019	**141**	126.9586	**201**	184.0133	**261**	241.4822
22	17.10758	**82**	71.55951	**142**	127.9049	**202**	184.9682	**262**	242.4426
23	17.97457	**83**	72.48927	**143**	128.8514	**203**	185.9232	**263**	243.4031
24	18.84432	**84**	73.41944	**144**	129.7980	**204**	186.8784	**264**	244.3637
25	19.71669	**85**	74.35002	**145**	130.7448	**205**	187.8337	**265**	245.3243
26	20.59152	**86**	75.28100	**146**	131.6918	**206**	188.7890	**266**	246.2851
27	21.46867	**87**	76.21239	**147**	132.6390	**207**	189.7445	**267**	247.2459
28	22.34801	**88**	77.14416	**148**	133.5864	**208**	190.7001	**268**	248.2067
29	23.22944	**89**	78.07631	**149**	134.5339	**209**	191.6558	**269**	249.1677

30	24.11285	**90**	79.00885	**150**	135.4816	**210**	192.6116	**270**	250.1287
31	24.99815	**91**	79.94175	**151**	136.4295	**211**	193.5675	**271**	251.0898
32	25.88523	**92**	80.87502	**152**	137.3776	**212**	194.5235	**272**	252.0509
33	26.77403	**93**	81.80865	**153**	138.3258	**213**	195.4797	**273**	253.0122
34	27.66447	**94**	82.74263	**154**	139.2742	**214**	196.4359	**274**	253.9735
35	28.55647	**95**	83.67695	**155**	140.2228	**215**	197.3922	**275**	254.9349
36	29.44998	**96**	84.61162	**156**	141.1715	**216**	198.3486	**276**	255.8963
37	30.34493	**97**	85.54663	**157**	142.1204	**217**	199.3051	**277**	256.8578
38	31.24126	**98**	86.48197	**158**	143.0695	**218**	200.2618	**278**	257.8194
39	32.13892	**99**	87.41764	**159**	144.0187	**219**	201.2185	**279**	258.7810
40	33.03786	**100**	88.35362	**160**	144.9681	**220**	202.1753	**280**	259.7428
41	33.93804	**101**	89.28993	**161**	145.9176	**221**	203.1322	**281**	260.7046
42	34.83941	**102**	90.22655	**162**	146.8673	**222**	204.0892	**282**	261.6664
43	35.74192	**103**	91.16347	**163**	147.8171	**223**	205.0463	**283**	262.6283

44	36.64555	**104**	92.10070	**164**	148.7671	**224**	206.0035	**284**	263.5903
45	37.55024	**105**	93.03823	**165**	149.7173	**225**	206.9608	**285**	264.5524
46	38.45597	**106**	93.97605	**166**	150.6676	**226**	207.9182	**286**	265.5145
47	39.36271	**107**	94.91416	**167**	151.6180	**227**	208.8757	**287**	266.4767
48	40.27042	**108**	95.85256	**168**	152.5686	**228**	209.8333	**288**	267.4390
49	41.17907	**109**	96.79124	**169**	153.5193	**229**	210.7910	**289**	268.4013
50	42.08863	**110**	97.73020	**170**	154.4702	**230**	211.7488	**290**	269.3637
51	42.99909	**111**	98.66944	**171**	155.4213	**231**	212.7066	**291**	270.3261
52	43.91040	**112**	99.60895	**172**	156.3724	**232**	213.6646	**292**	271.2886
53	44.82255	**113**	100.5487	**173**	157.3237	**233**	214.6226	**293**	272.2512
54	45.73552	**114**	101.4888	**174**	158.2752	**234**	215.5807	**294**	273.2138
55	46.64928	**115**	102.4291	**175**	159.2268	**235**	216.5390	**295**	274.1765
56	47.56380	**116**	103.3696	**176**	160.1785	**236**	217.4973	**296**	275.1393
57	48.47908	**117**	104.3104	**177**	161.1304	**237**	218.4557	**297**	276.1021

58	49.39509	**118**	105.2515	**178**	162.0824	**238**	219.4141	**298**	277.0650
59	50.31182	**119**	106.1928	**179**	163.0345	**239**	220.3727	**299**	278.0280