Prepared for the Election Assistance Commission

Draft Voluntary Voting System Guidelines Version 1.1

May 27, 2009 draft

This document has been prepared by the National Institute of Standards and Technology (NIST) and represents draft materials for the Election Assistance Commission (EAC). It does not represent a consensus view or recommendation from NIST, nor does it represent any policy decisions of NIST.

Volume II: *National Certification Testing Guidelines*

1 Introduction

Table of Contents

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 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 the 2005 *Voluntary Voting System Guidelines*.

1.3 Testing Scope

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

- Accuracy in the recording and processing of voting data, as measured by report total error rate
- Reliability, or the failure rate 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

- ~~Operational accuracy in the recording and processing of voting data, as measured by target error rate, for which the maximum acceptable error rate is no more than one in ten million ballot positions, with a maximum acceptable error rate in the test process of one in 500,000 ballot positions~~
- ~~Operational failures or the number of unrecoverable failures under conditions simulating the intended storage, operation, transportation, and maintenance environments for voting systems, using an actual time-based period of processing test ballots~~

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 VSTLoratory or shop environment.

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

The operating tests involve running the system for an extended period of time under varying temperatures and voltages. This period of operation ensures with confidence that the hardware meets or exceeds the minimum requirements for reliability, data reading, and processing accuracy contained in Volume I, Section 4. The procedure emphasizes equipment operability and data accuracy; it is not an exhaustive evaluation of all system functions. Moreover, the severity

of the test conditions, in most cases, has been reduced from that specified in the Military Standards to reflect commercial and industrial practice.

1.3.1.3 Focus of Software Evaluation

The software tests encompass a number of interrelated examinations, involving assessment of application source code for its compliance with the requirements spelled out in Volume I, Section 5. Essentially, the 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 VSTL may inspect COTS generated software source code in the preparation of test plans and conduct some minimal scanning or sampling to check for embedded code or unauthorized changes. Otherwise, the COTS source code is not subject to the full code review and testing. For purposes of code analysis, the COTS units shall be treated as unexpanded macros.

1.3.1.4 Focus of System Integration Tests

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

The 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, Sections 8 and 9 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 Assurance Program and Configuration Management Plan
c. Development of a detailed system test plan that reflects the scope and complexity of the system, and the status of system certification (i.e., initial certification or a re-certification to incorporate modifications)
d. Code review for selected software components
e. Witnessing of a system 'build' conducted by the 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 documents the manufacturer's configuration management plan and quality assurance program. If another version of the system was previously certified, the TDP would also include appropriate system change notes.

1.6 Voting Equipment Submitted by 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:

e. 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
f. 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

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

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

1.7.1.2 Software

Software certification is applicable to the following:

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

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

1.7.2 Modifications to Certified Systems

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

1.7.2.1 General Requirements for Modifications

The 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. As described in Subsection 1.6.2, 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 2
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:

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

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

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

1.8.2.2 Certification Test Conditions

The 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

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 exception. The VSTL may bypass the user interface of an interactive device in the case of environmental tests that

a. Would require subjecting test "voters" to unsafe or unhealthy conditions; or
b. Would be invalidated by the presence of a test "voter."

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.

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

~~a. For systems that use a light source as a means of detecting voter selections, the generation of a suitable optical signal by an external device is acceptable. For systems that rely on the physical activation of a switch, a mechanical fixture with suitable motion generators is acceptable~~
~~b. The accredited test lab may use a simulation device, and appropriate software, to speed up the process of testing and eliminate human error in casting test ballots, provided that the simulation covers all voting data detection and control paths that are used in casting an actual ballot. In the event that only partial simulation is achieved, then an independent method and test procedure shall be used to validate the proper operation of those portions of the system not tested by the simulator~~
~~c. If the vendor provides a means of simulating the casting of ballots, the simulation device is subject to the same performance, reliability, and quality requirements that apply to the voting device itself~~

1.8.2.4 Witness of System Build and Installation

Although most testing is conducted at facilities operated by the 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,

c. If a logic defect is responsible for the incorrect recording, tabulation, or reporting of a vote, the test engagement shall be terminated and the system shall be rejected. Any subsequent testing of a system based on or derived from the rejected system requires starting over with a new application to the EAC.
d. If a logic defect is found that is not responsible for the incorrect recording, tabulation, or reporting of a vote, testing shall be suspended and the system returned to the manufacturer for correction and quality assurance. The failure shall be counted in the evaluation of reliability (see Appendix C). 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 test plan should be revised to include regression testing for the change that was made.

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 counted in the evaluation of reliability (see Appendix C).

e. 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.
f. 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.

g. 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.

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

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

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

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

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

~~h. Any and all failures that occurred as a result of a deficiency shall be classified as purged, and test results shall be evaluated as though the failure or failures had not occurred, if the:~~
   ~~i. Vendor submits a design, manufacturing, or packaging change notice to correct the deficiency, together with test data to verify the adequacy of the change~~
   ~~ii. Examiner of the equipment agrees that the proposed change will correct the deficiency~~
   ~~iii. Vendor certifies that the change will be incorporated into all existing and future production units~~

~~i. If corrective action cannot be successfully taken as defined above, then the test shall be terminated, and the equipment shall be rejected~~

1.8.3 Post-test Activities

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

a. The 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

Prior to the transition of this function to the EAC, the NASED Voting Systems Board (the Board) was responsible for resolving questions about the application of the *Guidelines* in the testing of voting systems. The EAC will have a process for the VSTLs, manufacturers and election officials to request an interpretation of the *Guidelines*. The interpretation will be publicly documented for reference by interested parties. The EAC will periodically assess the interpretations provided to determine which topics should be reflected in a future version of the *Guidelines*.

2 Description of the Technical Data Package

Table of Contents

2 Description of the Technical Data Package

2.1 Scope

This subsection contains a description of 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.

2.1.1 Content and Format

The content of the Technical Data Package (TDP) is intended to provide clear, complete descriptions of the following information about the system:

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 system quality during the system’s development and subsequent maintenance
g. Manufacturer practices for managing the configuration of the system during development and for modifications to the system throughout its life cycle

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.

2.1.1.1 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 Quality Assurance Process

9 Configuration Management Procedures

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

~~At minimum, the TDP shall contain the following documentation:~~

~~a. System configuration overview~~
~~b. System functionality description~~
~~c. System hardware specifications~~
~~d. Software design and specifications~~
~~e. System test and verification specifications~~
~~f. System security specifications~~
~~g. User/system operations procedures~~
~~h. System maintenance procedures~~
~~i. Personnel deployment and training requirements~~
~~j. Configuration management plan~~
~~k. Quality assurance program~~
~~l. System change notes~~

2.1.1.2 Required Content for System Changes and Re-certification

For systems seeking re-certification, manufacturers shall submit System Change Notes as described in Subsection 2.13, 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.

2.1.1.3 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.

2.1.2 Other Uses for Documentation

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

2.1.3 Protection of Proprietary Information

The 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.

~~The vendor shall identify all documents, or portions of documents, containing proprietary information not approved for public release. Any person or accredited test lab receiving proprietary information shall agree to use it solely for the purpose of analyzing and testing the system, and shall agree to refrain from otherwise using the proprietary information or disclosing it to any other person or agency without the prior written consent of the vendor, unless disclosure is legally compelled.~~

2.2 System Overview

In the system overview, the 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.

2.2.1 System Description

The system description shall include written descriptions, drawings and diagrams that present:

a. A description of the functional components (or subsystems) as defined by the 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

ii. Database software
iii. Communications routers
iv. Modem drivers
v. 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

2.2.2 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.

2.3 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

2.4 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.

2.4.1 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

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

Environmental conditions: This discussion addresses the ability of the system to withstand natural environments, and operational constraints in normal and test environments, including all requirements and restrictions regarding electrical service,

telecommunications services, environmental protection, and any additional facilities or resources required to install and operate the system

2.4.2 Design and Construction

The 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

2.5 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.

2.5.1 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.

2.5.2 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.

2.5.3 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.

2.5.4 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

2.5.5 Software Operating Environment

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

2.5.5.1 Hardware Environment and Constraints

The 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

2.5.5.2 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.

2.5.6 Software Functional Specification

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

2.5.6.1 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)

2.5.6.2 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

2.5.7 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.

2.5.7.1 Programming Specifications Overview

This overview shall include such items as flowcharts, data flow diagrams, and other graphical techniques that facilitate understanding of the programming specifications. This section shall be prepared to facilitate understanding of the internal functioning of the individual software modules. Implementation of the functions shall be described in terms of the software architecture, algorithms, and data structures.

2.5.7.2 Programming Specifications Details

The programming specifications shall describe individual software modules and their component units, if applicable. For each module and unit, the 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 2.5.9 describes the requirements for documenting system interfaces.) Data local to the software module or unit shall be described separately from data input to, or output from, the software module or unit
f. If the software module or unit contains logic, the logic to be used by the software unit, including, as applicable:

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 2.5.8

2.5.8 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

2.5.9 Interfaces

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

2.5.9.1 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)

2.5.9.2 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)

2.5.10 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

2.6 System Security Specification

~~Vendors shall submit a system security specification that addresses the security requirements of Volume I, Section 7. This specification shall describe the level of security provided by the system in terms of the specific security risks addressed by the system, the means by which each risk is addressed, the process used to test and verify the effective operation of security capabilities and, for systems that use public telecommunications networks as defined in Volume I, Section 6, the means used to keep the security capabilities of the system current to respond to the evolving threats against these systems.~~

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. System security objectives
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 high-level documents listed in Table 1 as part of the TDP.

Table 1 High Level Voting System Documentation

Document	**Description**
Design and Interface Specification	This document shall identify the threats the voting system protects. 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).
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.
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.
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.
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 ~~provided~~ in other sections ~~provided that~~ 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. ~~The Security Specification shall contain the sections identified below.~~

2.6.1 Access Control

Manufacturers shall provide user and TDP documentation of access control capabilities of the voting system.

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.

Manufacturers shall provide descriptions and specifications of methods to prevent unauthorized access to the access control mechanisms of the voting system in the TDP.

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.

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.

2.6.1.1 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.

2.6.1.2 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.

2.6.2 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.

2.6.3 Software Installation and Security

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.

Manufacturers shall provide a list of all software related to the voting system in the technical data package (TDP).

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).

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.

As part of the TDP, manufacturers shall document the functionality provided to the voting system by the installed software.

As part of the TDP, manufacturers shall map the dependencies and interactions between software installed on the voting system.

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.

2.6.4 System Event Logging

Manufacturers shall provide TDP documentation of event logging capabilities of the voting devices.

Manufacturers shall provide a technical data package that describes system event logging design and implementation.

2.6.5 Physical Security

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.

As part of the TDP, manufacturers shall provide a listing of all ports and access points of the voting system.

For each physical lock used on a voting system, manufacturers shall document whether the lock was installed to secure an access point.

Manufacturers shall provide a list of all physical security countermeasures that require power supplies.

Manufacturers shall provide a technical data package that documents the design and implementation of all physical security controls for the voting system.

2.6.6 Setup Inspection

Manufacturers shall provide the technical specifications of how voting systems identify installed software in the TDP.

Manufacturers shall provide a technical specification of how the integrity of software installed on the voting system is verified as part of the TDP.

Discussion: 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.

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 Requirements, and 7.4.6 Software Setup Validation.

2.6.7 Cryptography

Manufacturers shall provide a list of all cryptographic algorithms and key sizes supported by the voting system.

Manufacturers shall provide the technical specification of all cryptographic protocols supported by the voting system.

Manufacturers shall provide the cryptographic module name, identification information (such as hardware/firmware/software name, model name, and revision/version number) and NIST FIPS 140-2 validation certificate number for all cryptographic modules that implement the cryptographic algorithms of the voting systems.

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.

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.

Manufacturers shall provide documentation describing how cryptographic keys are created, stored, imported/exported, and deleted by the voting system.

2.6.8 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

2.6.9 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.

2.7 System Test and Verification Specification

The manufacturer shall provide test and verification specifications for:

a. Development test specifications
b. National certification test specifications

2.7.1 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
b. Standard test procedures, including any assumptions or constraints
c. Special purpose test procedures including any assumptions or constraints
d. Test data; including the data source, whether it is real or simulated, and how test data are controlled
e. Expected test results
f. Criteria for evaluating test results

The details of this description shall be as specified in the manufacturer's Quality Manual. ~~Additional details for these requirements are provided by MIL-STD-498, Software Test Plan and Software Test Description.~~ In the event that test data are not available, the VSTL shall design test cases and procedures equivalent to those ordinarily used during product verification.

2.7.2 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.

2.8 System Operations Procedures

This documentation shall provide all information necessary for system use by all personnel who support pre-election and election preparation, polling place activities and central counting activities, as applicable, with regard to all system functions and operations identified in Subsection 2.3 above. The nature of the instructions for operating personnel will depend upon the overall system design and required skill level of system operations support personnel.

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

2.8.1 Introduction

The 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.

2.8.2 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

2.8.3 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 2.3 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.

2.8.4 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

2.8.5 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 archivalness 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.

2.8.6 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

2.8.7 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

2.9 System Maintenance Manual

The system maintenance procedures shall provide information in sufficient detail to support election workers, information systems personnel, or maintenance personnel in the adjustment or removal and replacement of components or modules in the field. Technical documentation needed solely to support the repair of defective components or modules ordinarily done by the manufacturer or software developer is not required.

Recommended service actions to correct malfunctions or problems shall be discussed, along with personnel and expertise required to repair and maintain the system; and equipment, materials, and facilities needed for proper maintenance. This manual shall include the sections listed below.

2.9.1 Introduction

The 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

2.9.2 Maintenance Procedures

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

2.9.2.1 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)

2.9.2.2 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

2.9.3 Maintenance Equipment

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

2.9.4 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.

2.9.4.1 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

2.9.4.2 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.

2.9.5 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

2.9.6 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

2.10 Personnel Deployment and Training Requirements

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

2.10.1 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.

2.10.2 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

2.11 Configuration Management Plan

Manufacturers shall submit a Configuration Management Plan that addresses the configuration management requirements of Volume I, Section 9. This plan shall describe all policies, processes, and procedures employed by the manufacturer to carry out these requirements. Information submitted by the manufacturer shall be used by the VSTL to assist in developing and executing the system certification test plan. This information is particularly important to support the design of test plans for system modifications. A well-organized, robust and detailed Configuration Management Plan will enable the VSTL to more readily determine the nature and scope of tests needed to fully test the modifications. The Configuration Management Plan shall contain the sections identified below.

2.11.1 Configuration Management Policy

The manufacturer shall provide a description of its organizational policies for configuration management, addressing the specific requirements of Volume I, Subsection 9.2. These requirements pertain to:

a. Scope and nature of configuration management program activities
b. Breadth of application of manufacturer's policy and practices to the voting system

2.11.2 Configuration Identification

The manufacturer shall provide a description of the procedures and naming conventions used to address the specific requirements of Volume I, Subsection 9.3. These requirements pertain to:

a. Classifying configuration items into categories and subcategories
b. Uniquely numbering or otherwise identifying configuration items
c. Naming configuration items

2.11.3 Baseline and Promotion

The manufacturer shall provide a description of the procedures and naming conventions used to address the specific requirements of Volume I, Subsection 9.4. These requirements pertain to:

a. Establishing a particular instance of a system component as the starting baseline
b. Promoting subsequent instances of a component to baseline throughout the system development process for the first complete version of the system submitted for testing

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

2.11.4 Configuration Control Procedures

The manufacturer shall provide a description of the procedures used by the manufacturer to approve and implement changes to a configuration item to prevent unauthorized additions, changes, or deletions to address the specific requirements of Volume I, Subsection 9.5. These requirements pertain to:

a. Developing and maintaining internally developed items
b. Developing and maintaining third party items
c. Resolving internally identified defects
d. Resolving externally identified and reported defects

2.11.5 Release Process

The manufacturer shall provide a description of the contents of a system release, and the procedures and related conventions by which the manufacturer installs, transfers, or migrates the system to accredited voting system testing laboratories and customers to address the specific requirements of Volume I, Subsection 9.6. These requirements pertain to:

a. A first release of the system to a VSTL
b. A subsequent maintenance or upgrade release of a system, or particular components, to a VSTL
c. The initial delivery and installation of the system to a customer
d. A subsequent maintenance or upgrade release of a system, or particular components, to a customer

2.11.6 Configuration Audits

The manufacturer shall provide a description of the procedures and related conventions for the two audits required by Volume I, Subsection 9.7. These requirements pertain to:

a. Physical configuration audit that verifies the voting system components submitted for certification testing to the manufacturer's technical documentation
b. Functional configuration audit that verifies the system performs all the functions described in the system documentation

2.11.7 Configuration Management Resources

The manufacturer shall provide a description of the procedures and related conventions for maintaining information about configuration management tools required by Volume I, Subsection 9.8. These requirements pertain to information regarding:

a. Specific tools used, current version, and operating environment
b. Physical location of the tools, including designation of computer directories and files
c. Procedures and training materials for using the tools

2.12 Quality Assurance Program

Manufacturers shall submit a Quality Assurance Program that addresses the quality assurance requirements of Volume I, Section 8. This plan shall describe all policies, processes, and procedures employed by the manufacturer to ensure the overall quality of the system for its initial development and release and for subsequent modifications and releases. This information is particularly important to support the design of test plans by the VSTL. A well-organized, robust and detailed Quality Assurance Program will enable the VSTL to more readily determine the nature and scope of tests needed to test the system appropriately. The Quality Assurance Program shall, at a minimum, address the topics indicated below.

2.12.1 Quality Assurance Policy

The manufacturer shall provide a description of its organizational policies for quality assurance, including:

a. Scope and nature of Quality Assurance activities
b. Breadth of application of manufacturer's policy and practices to the voting system

2.12.2 Parts and Materials Tests

The manufacturer shall provide a description of its practices for parts and materials tests and examinations that meet the requirements of Volume I, Subsection 8.5.

2.12.3 Quality Conformance Inspections

The manufacturer shall provide a description of its practices for quality conformance inspections that meet the requirements of Volume I, Subsection 8.6. For each test performed, the record of tests provided shall include:

a. Test location
b. Test date

c. Individual who conducted the test
d. Test outcomes

2.12.4 Documentation

The manufacturer shall provide a description of its practices for documentation of the system and system development process that meet the requirements of Volume I, Subsection 8.7.

2.13 System Change Notes

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

3 Functionality Testing

Table of Contents

3 Functionality Testing

3.1 Scope

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

3.2 Breadth of Functionality Testing

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

3.2.1 Basic Functionality Testing Requirements

The 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.

3.2.2 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.

3.2.3 Testing to Reflect Additional Capabilities

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

3.2.4 Testing to Reflect Previously Tested Capabilities

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

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

3.3 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.

3.3.1 Testing in Parallel with Precinct Count Systems

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

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.

3.3.2 Testing in Parallel with Central Count Systems

For testing voting functions defined in Volume I, Sections 2, the following procedures shall be performed during the functional tests.

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.

3.4 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.

3.5 Testing for Systems that Operate on Personal Computers

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

Section 4 provides additional information on hardware to be used to conduct functionality testing of such voting devices, as well as hardware to be used to conduct security testing and other forms of testing.

4 Hardware Testing

Table of Contents

4 Hardware Testing

4.1 Scope

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

4.2 Basis of Hardware Testing

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

4.2.1 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.

4.2.2 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.

4.3 Test Conditions

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

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

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

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

4.4 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.

4.5 Test Fixtures

The test lab 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 exception. The test lab may bypass the user interface of an interactive device in the case of environmental tests that

a. Would require subjecting test "voters" to unsafe or unhealthy conditions; or
b. Would be invalidated by the presence of a test "voter."

The test lab 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.

~~The use of test fixtures or ancillary devices to facilitate hardware testing is encouraged. These fixtures and devices may include arrangements for automating the operation of voting devices and the acquisition of test data.~~

~~The use of a fixture to ensure correctness in casting ballots by hand is recommended. Such a fixture may consist of a template, with apertures in the desired location, so that selections may be made rapidly. Such a template will eliminate or greatly minimize errors in activating test ballot patterns, while reducing the amount of time required to cast a test ballot.~~

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

~~To speed up the process of testing and to eliminate human error in casting test ballots the tests may use a simulation device with appropriate software. Such simulation is recommended if it covers all voting data detection and control paths that are used in casting an actual ballot. In the event that only partial simulation is achieved, then an independent method and test procedure must be used to validate the proper operation of those portions of the system not tested by the simulator.~~

~~If the manufacturer provides a means of simulating the casting of ballots, the simulation device is subject to the same performance, reliability, and quality requirements that apply to the voting device itself so as not to contribute errors to the test processes.~~

4.6 Non-operating Environmental Tests

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

4.6.1 General

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

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

Prior to each test, the equipment shall be shown to be operational by means of the procedure contained in Subsection 4.6.1.5. The equipment may then be prepared as if for actual transportation or storage, and subjected to appropriate test procedures outlined. After each procedure has been completed, the equipment status will again be verified as in Subsection 4.6.1.5.

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

4.6.1.1 Pretest Data

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

4.6.1.2 Preparation for Test

The equipment shall be prepared as for the expected non-operating use, as noted below. When preparation for transport between the storage site and the polling place is required,

the equipment shall be prepared with any protective enclosures or internal restraints that the 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.

4.6.1.3 Mechanical Inspection and Repair

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

4.6.1.4 Electrical Inspection and Adjustment

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

4.6.1.5 Operational Status Check

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

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

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

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

4.6.1.6 Failure Criteria

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

4.6.2 Bench Handling Test

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

4.6.2.1 Applicability

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

4.6.2.2 Procedure

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

4.6.3 Vibration Test

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

4.6.3.1 Applicability

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

4.6.3.2 Procedure

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

4.6.4 Low Temperature Test

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

4.6.4.1 Applicability

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

4.6.4.2 Procedure

Step 1: Arrange the equipment as for storage. Install it in the test chamber.
Step 2: Lower the internal temperature of the chamber at any convenient rate, but not so rapidly as to cause condensation in the chamber, and in any case no more rapidly than 10 degrees F per minute, until an internal temperature of -4 degrees F has been reached.

Step 3: Allow the chamber temperature to stabilize. Maintain this temperature for a period of 4 hours after stabilization.
Step 4: Allow the internal temperature of the chamber to return to standard laboratory conditions, at a rate not exceeding 10 degrees F per minute.
Step 5: Allow the internal temperature of the equipment to stabilize at laboratory conditions before removing it from the chamber.
Step 6: Remove the equipment from the chamber and from its containers, and inspect the equipment for evidence of damage.
Step 7: Verify continued operability of the equipment.

4.6.5 High Temperature Test

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

4.6.5.1 Applicability

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

4.6.5.2 Procedure

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

4.6.6 Humidity Test

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

4.6.6.1 Applicability

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

4.6.6.2 Procedure

Step 1: Arrange the equipment as for storage. Install it in the test chamber.
Step 2: Adjust the chamber conditions to those given in MIL-STD-810D Table 507.2-I, for the time 0000 of the HotHumid cycle (Cycle 1).
Step 3: Perform a 24-hour cycle with the time and temperature-humidity values specified in Figure 507.2-1, Cycle 1.
Step 4: Repeat Step 2 until 5, 24-hour cycles have been completed.
Step 5: Continue with the test commencing with the conditions specified for time = 0000 hours.
Step 6: At any convenient time in the interval between time = 120 hours and time = 124 hours, place the equipment in an operational configuration, and perform a complete operational status check as defined in Subsection 4.6.1.5.
Step 7: If the equipment satisfactorily completes the status check, continue with the sixth 24-hour cycle.
Step 8: Perform 4 additional 24-hour cycles, terminating the test at time = 240 hours.
Step 9: Remove the equipment from the test chamber and inspect it for any evidence of damage.
Step 10: Verify continued operability of the equipment.

4.7 Environmental Tests, Operating

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

4.7.1 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".

~~4.7.1 Temperature and Power Variation Tests~~

~~This test is similar to the low temperature and high temperature tests of MIL-STD-810-D, Method 502.2 and Method 501.2, with test conditions that correspond to the requirements~~

~~of the performance standards. This procedure tests system operation under various environmental conditions for at least 163 hours. During 48 hours of this operating time, the device shall be in a test chamber. For the remaining hours, the equipment shall be operated at room temperature. The system shall be powered for the entire period of this test; the power may be disconnected only if necessary for removal of the system from the test chamber.~~

~~Operation shall consist of ballot counting cycles, which vary with system type. An output report need not be generated after each counting cycle. The interval between reports, however, should be no more than 4 hours to keep to a practical minimum the time between the occurrence of a failure or data error and its detection.~~

~~Test Ballots per Counting Cycle~~

~~Precinct count systems 100 ballots/hour~~

~~Central count systems 300 ballots/hour~~

~~The recommended pattern of votes is one chosen to facilitate visual recognition of the reported totals; this pattern shall exercise all possible voting locations. System features such as data quality tests, error logging, and audit reports shall be enabled during the test.~~

~~Each operating cycle shall consist of processing the number of ballots indicated above.~~

~~a. Arrange the equipment in the test chamber. Connect as required and provide for power, control, and data service through enclosure wall.~~
~~b. Set the supply voltage at 117 voltage alternating current.~~
~~c. Power the equipment, and perform an operational status check as in Section 4.6.1.5.~~
~~d. Set the chamber temperature to 50 degrees F, observing precautions against thermal shock and condensation.~~
~~e. Begin 24 hour cycle.~~
~~f. At T=4 hrs, lower the supply voltage to 105 vac.~~
~~g. At T=8 hrs, raise the supply voltage to 129 vac.~~
~~h. At T=11:30 hrs, return the supply voltage to 117 vac and return the chamber temperature to lab ambient, observing precautions against thermal shock and condensation.~~
~~i. At T=12:00 hrs, raise the chamber temperature to 95 degrees Fahrenheit.~~
~~j. Repeat Steps 5 through 8, with temperature at 95 degrees Fahrenheit, complete at T=24 hrs.~~
~~k. Set the chamber temperature at 50 degrees Fahrenheit as in Step 4.~~
~~l. Repeat the 24 hour cycle as in Steps 5-10, complete at T=48 hrs.~~
~~m. After completing the second 24 hour cycle, disconnect power from the system and remove it from the chamber if needed.~~
~~n. Reconnect the system as in Step 2, and continue testing for the remaining period of operating time required until the ACCEPT/REJECT criteria of Subsection 4.7.1.1 have been met.~~

4.7.1.1 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.

4.7.1.2 Operating Humidity

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

~~**4.7.1.1 Data Accuracy**~~

~~As indicated in Volume I, Section 4, data accuracy is defined in terms of ballot position error rate. This rate applies to the voting functions and supporting equipment that capture, record, store, consolidate, and report the specific selections, and absence of selections, made by the voter for each ballot position. Volume I, Subsection 4.1.1 identifies the specific functions to be tested.~~

~~For each processing function, the system shall achieve a target error rate of no more than one in 10,000,000 ballot positions, with a maximum acceptable error rate in the test process of one in 500,000 ballot positions. This error rate includes errors from any source while testing a specific processing function and its related equipment.~~

~~This error rate is used to determine the vote position processing volume used to test system accuracy for each function:~~

~~a. If the system makes one error before counting 26,997 consecutive ballot positions correctly, it will be rejected. The manufacturer is then required to improve the system~~
~~b. If the system reads at least 1,549,703 consecutive ballot positions correctly, it will be accepted~~
~~c. If the system correctly reads more than 26,997 ballot positions but less than 1,549,703 when the first error occurs, the testing will have to be continued until another 1,576,701 consecutive ballot positions are counted without error (a total of 3,126,404 with one error)~~

~~Appendix C provides further details of the calculation for this testing volume.~~

4.7.2 Maintainability Test

The VSTL shall test for maintainability based on the provisions of Volume I, Section 4 for maintainability, including both physical attributes and additional attributes regarding the ease of performing maintenance activities. These tests include:

a. Examining the physical attributes of the system to determine whether significant impediments exist for the performance of those maintenance activities that are to be performed by the jurisdiction. These activities shall be identified by the manufacturer in the system maintenance procedures portion of the TDP
b. Performing activities designated as maintenance activities for the jurisdiction in the TDP, in accordance with the instructions provided by the manufacturer in the system maintenance procedures, noting any difficulties encountered

Should significant impediments or difficulties be encountered that are not remedied by the manufacturer, the VSTL shall include such findings in the certification test results of the certification test report.

4.7.3 Reliability Test

The reliability of a voting system is assessed based on its cumulative performance across *all* tests, as specified in Appendix C.

~~The accredited test lab shall test for reliability based on the provisions of Volume I, Section 4 for the acceptable Mean Time Between Failure (MBTF). The MBTF shall be measured during the conduct of other system performance tests specified in this section, and shall be at least 163 hours. Appendix C provides further details of the calculation for this testing period.~~

4.7.4 Availability Test

The VSTL shall assess the adequacy of system availability based on the provisions of Volume I, Section 4. As described in this section, availability of voting system equipment is determined as a function of reliability, and the mean time to repair the system in the event of failure.

Availability cannot be tested directly before the voting system is deployed in jurisdictions, but can be modeled mathematically to predict availability for a defined system configuration. This model shall be prepared by the manufacturer, and shall be validated by the accredited testing laboratory.

The model shall reflect the equipment used for a typical system configuration to perform the following system functions:

a. For all paper-based systems:

   i. Recording voter selections (such as by ballot marking)
   ii. Scanning the marks on paper ballots and converting them into digital data
b. For all DRE systems:
   i. Recording and storing the voter's ballot selections
c. For precinct-count systems (paper-based and DRE):
   i. Consolidation of vote selection data from multiple precinct-based systems to generate jurisdiction-wide vote counts, including storage and reporting of the consolidated vote data
d. For central-count systems (paper-based and DRE):
   i. Consolidation of vote selection data from multiple counting devices to generate jurisdiction-wide vote counts, including storage and reporting of the consolidated vote data

The model shall demonstrate the predicted availability of the equipment that supports each function. This demonstration shall reflect the equipment reliability, mean time to repair, and assumptions concerning equipment availability and deployment of maintenance personnel stated by the manufacturer in the TDP.

4.8 Other Environmental Tests

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

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 (1995-01).
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 (1995-01).
f. The test for lightning surge protection shall be conducted in compliance with the test specified in IEC 61000-4-5 (1995-02).
g. The test for conducted RF immunity shall be conducted in compliance with the test specified in IEC 61000-4-6 (1996-04).
h. The test for AC magnetic fields RF immunity shall be conducted in compliance with the test specified in IEC 61000-4-8 (1993-06).

5 Software Testing

Table of Contents

5 Software Testing

5.1 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 3 for specific tests of voting system functionality
b. Section 6 for testing voting system security and for testing the operation of the voting system software together with other voting system components

5.2 Basis of Software Testing

The VSTL shall design and perform procedures that test the voting system software requirements identified in Volume I, Section 5. All software components designed or modified for election use shall be tested in accordance with the applicable procedures contained in this section.

Unmodified, general purpose COTS non-voting software (e.g., operating systems, programming language compilers, data base management systems, and Web browsers) is not subject to the detailed examinations specified in this section. However, the VSTL shall examine such software to confirm the specific version of software being used against the design specification to confirm that the software has not been modified. Portions of COTS software that have been modified by the manufacturer in any manner are subject to review.

Unmodified COTS software is not subject to code examination. However, source code generated by a COTS package and embedded in software modules for compilation or interpretation shall be provided in human readable form to the VSTL. The VSTL may inspect COTS source code units to determine testing requirements or to verify the code is unmodified.

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

Compatibility of the voting system software components or subsystems with one another, and with other components of the voting system environment, shall be determined through functional tests integrating the voting system software with the remainder of the system.

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

5.3 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

5.4 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.

The accredited test lab shall compare the source code to the vendor's software design documentation to ascertain how completely the software conforms to the vendor's specifications. Source code inspection shall also assess the extent to which the code adheres to the requirements in Volume I, Section 5

5.4.1 Control Constructs

Voting system software shall use the control constructs identified in this section as follows:

a. If the programming language used does not provide these control constructs, the vendor shall provide them (that is, comparable control structure logic). The constructs shall be used consistently throughout the code. No other constructs shall be used to control program logic and execution
b. While some programming languages do not create programs as linear processes, stepping from an initial condition, through changes, to a conclusion, the program components nonetheless contain procedures (such as "methods" in object-oriented languages). Even in these programming languages, the procedures must execute through these control constructs (or their equivalents, as defined and provided by the vendor)
c. Operator intervention or logic that evaluates received or stored data shall not re-direct program control within a program routine. Program control may be re-directed within a routine by calling subroutines, procedures, and functions, and by interrupt service routines and exception handlers (due to abnormal error conditions). Do-While (False) constructs and intentional exceptions (used as GoTos) are prohibited
d. Conventional constructs that are inherent to the development language are permitted but must be documented in the code, adjacent to their use.

Illustrations of the following control construct techniques are provided in Figures 1 through 4.

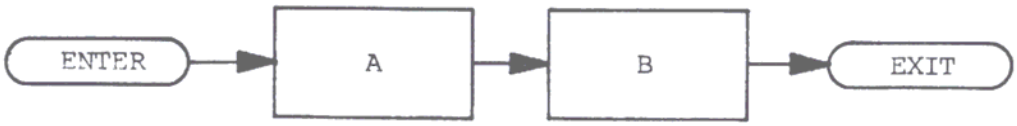
e. Fig. 1 Sequence
f. Fig. 2 If -Then -Else
g. Fig. 3 Do -While
h. Fig. 4 Do -Until
i. Fig. 5 Case
j. Fig. 6 General loop, including the special case FOR loop

5.4.1.1 Replacement Rule

In the constructs shown, any 'process' may be replaced by a simple statement, a subroutine or function call, or any of the control constructs. In Fig 4-1 for example, "Process A" may be a simple statement and "Process B" another Sequence construct.

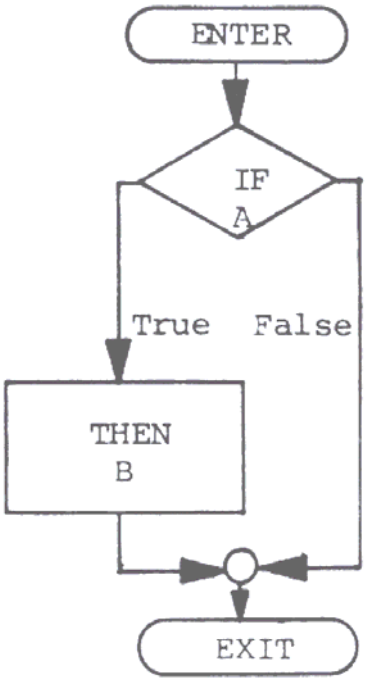
~~Using the replacement rule to replace one or both of the processes in the Sequence construct with other Sequence constructs, a large block of sequential code may be formed. The entire chain is recognized as a Sequence construct and is sometimes called a BLOCK construct. In many languages, a Sequence may need to be marked with special symbols or punctuation to delimit where it starts and where it ends. For example, a "BEGIN" and "END" may be used. This allows the scope of a Sequence used as "Process C" in the IF-THEN-ELSE (Fig 4-2) to be recognized as completing the IF-THEN-ELSE rather than part of a higher level Sequence that included the IF-THEN-ELSE as a component.~~

~~5.4.1.2 Figures 1-6~~



~~Figure 1 SEQUENCE~~

~~Control flows from "Process A" to the next in sequence, "Process B"~~



~~Figure 2 IF-THEN-ELSE~~

~~*In Figure 2, flow of control will skip a process pending the condition of "A."~~

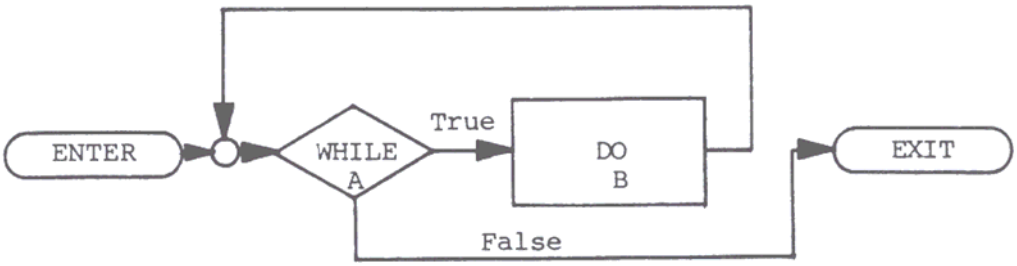


Figure 3 DO-WHILE

In Figure 4-3, condition "A" is evaluated. If found to be true, then control is passed to Process "B" and condition "A" is reevaluated. If condition "A" is found to be false, then control is passed out of the loop. Note that, if B is a BLOCK, the "DO" may be recognized as the opening symbol. A terminating symbol is needed from the language used.

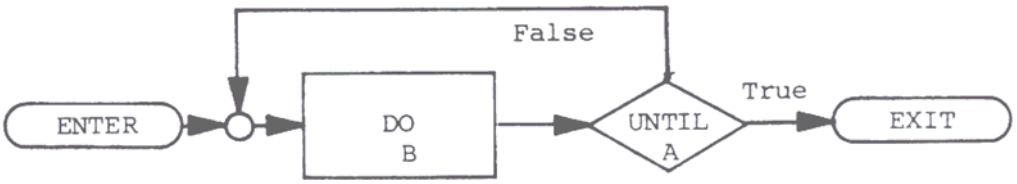
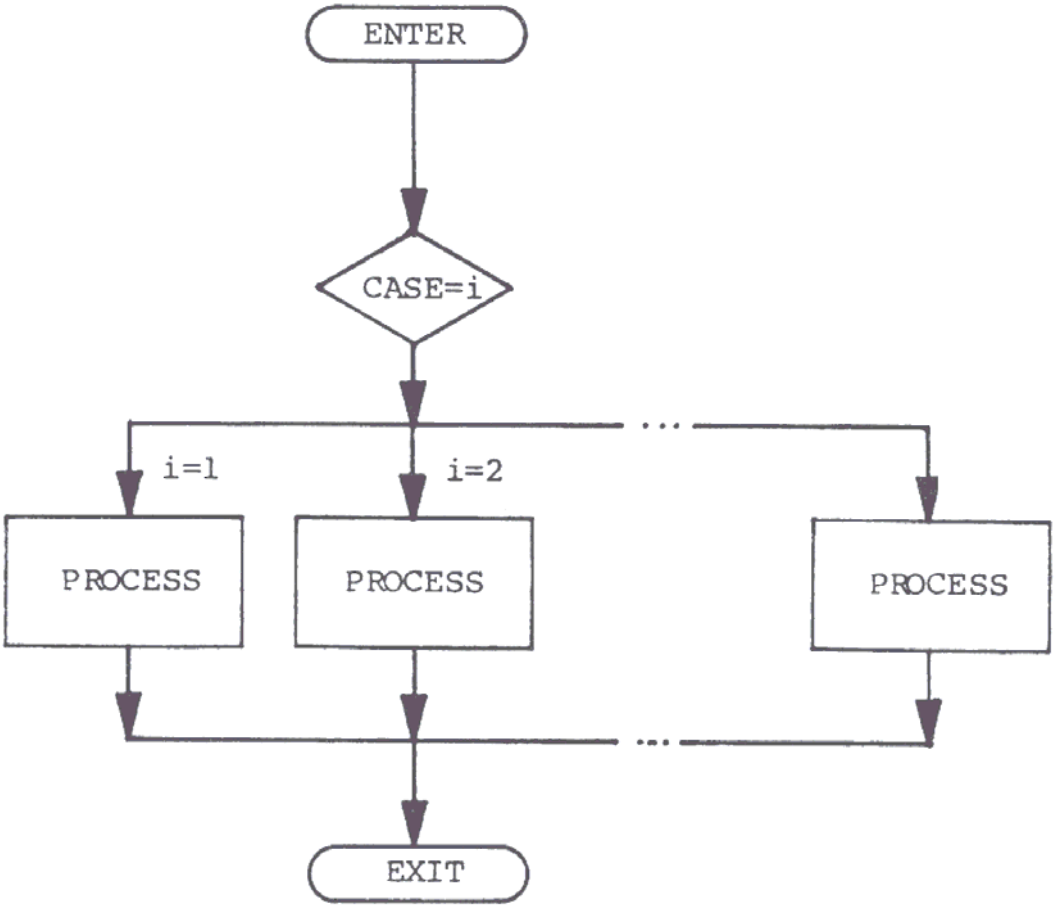


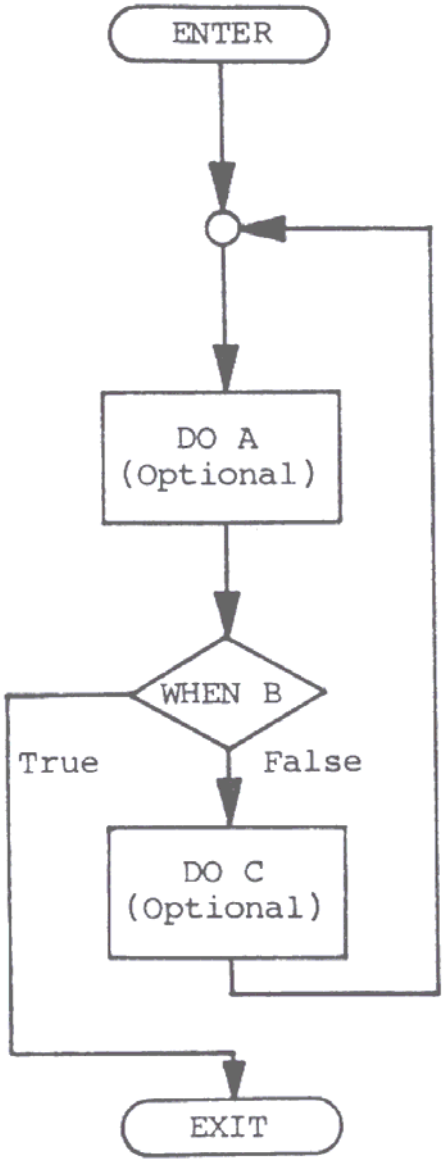
Figure 4 DO-UNTIL

Figure 4-4 is similar to a DO-WHILE, except that the test of condition A is performed after "Process B" has executed and the DO is performed upon a false "A" condition.. If condition "A" is true, control is passed out of the loop.


ENTER
CASE=i
i=1
i=2
PROCESS
PROCESS
PROCESS
EXIT

~~**Figure 5- CASE**~~

~~Control is passed to a Process based on the value of i.~~



~~**Figure 6- General LOOP**~~

~~Optional process A is executed. Condition B is then evaluated. If found to be false, optional process C is executed and control is passed to process A. Condition B is then evaluated again. If condition B is true, then control is passed out of the loop.~~

~~A special case of the GENERAL LOOP is the FOR loop. The FOR loop is not strictly essential, as it can be programmed as a DO-WHILE loop. The FOR loop executes on a counter. The control FOR statement defines a counter variable or variables, a test for~~

ending the loop, and a standard method of changing the variable(s) on each pass such as incrementing or decrementing. For example,

"FOR c = 0; c < 10; c + 1

DO Process A;"

The counter is initialized to zero, if the counter test is false, the DO process is executed and the counter is incremented (or decremented). Once the counter test is true, control exits from the loop without incrementing the counter. The implementation of the FOR loop in many languages, however, can be error prone. The use of the FOR loop shall include strictly enforced coding conventions to avoid common errors such as a loop that never ends.

The GENERAL LOOP should not be used where one of the other loop structures will serve. It is error prone and may not be supported in many languages without using GOTOs type redirections. However, if defined in the language, it may be useful in defining some loops where the exit needs to occur in the middle. Also, in other languages the GENERAL LOOP logic can be used to simulate the other control constructs. Like the special case, the use of the GENERAL LOOP shall require the strict enforcement of coding conventions to avoid problems.

5.4.2 Assessment of Coding Conventions

The accredited test lab shall test for compliance with the coding conventions specified by the vendor. If the vendor does not identify an appropriate set of coding conventions in accordance with the provisions of Volume I, Subsection 5.2.6, the accredited test lab shall review the code to ensure that it:

a. Uses uniform calling sequences. All parameters shall either be validated for type and range on entry into each unit or the unit comments shall explicitly identify the type and range for the reference of the programmer and tester. Validation may be performed implicitly by the compiler or explicitly by the programmer
b. Has the return explicitly defined for callable units such as functions or procedures (do not drop through by default) for C-based languages and others to which this applies, and in the case of functions, has the return value explicitly assigned. Where the return is only expected to return a successful value, the C convention of returning zero shall be used or the use of another code justified in the comments. If an uncorrected error occurs so the unit must return without correctly completing its objective, a non-zero return value shall be given even if there is no expectation of testing the return. An exception may be made where the return value of the function has a data range including zero
c. Does not use macros that contain returns or pass control beyond the next statement
d. For those languages with unbound arrays, provides controls to prevent writing beyond the array, string, or buffer boundaries

e. For those languages with pointers or which provide for specifying absolute memory locations, provides controls that prevent the pointer or address from being used to overwrite executable instructions or to access inappropriate areas where vote counts or audit records are stored
f. For those languages supporting case statements, has a default choice explicitly defined to catch values not included in the case list
g. Provides controls to prevent any vote counter from overflowing. Assuming the counter size is large enough such that the value will never be reached is not adequate
h. Is indented consistently and clearly to indicate logical levels
i. Excluding code generated by commercial code generators, is written in small and easily identifiable modules, with no more than 50% of all modules exceeding 60 lines in length, no more than 5% of all modules exceeding 120 lines in length, and no modules exceeding 240 lines in length. "Lines" in this context, are defined as executable statements or flow control statements with suitable formatting and comments. The reviewer should consider the use of formatting, such as blocking into readable units, which supports the intent of this requirement where the module itself exceeds the limits. The vendor shall justify any module lengths exceeding this standard
j. Where code generators are used, the source file segments provided by the code generators should be marked as such with comments defining the logic invoked and, if possible, a copy of the source code provided to the accredited test lab with the generated source code replaced with an unexpanded macro call or its equivalent
k. Has no line of code exceeding 80 columns in width (including comments and tab expansions) without justification
l. Contains no more than one executable statement and no more than one flow control statement for each line of source code
m. In languages where embedded executable statements are permitted in conditional expressions, the single embedded statement may be considered a part of the conditional expression. Any additional executable statements should be split out to other lines
n. Avoids mixed-mode operations. If mixed mode usage is necessary, then all uses shall be identified and clearly explained by comments
o. Upon exit() at any point, presents a message to the user indicating the reason for the exit()
p. Uses separate and consistent formats to distinguish between normal status and error or exception messages. All messages shall be self-explanatory and shall not require the operator to perform any look-up to interpret them, except for error messages that require resolution by a trained technician
q. References variables by fewer than five levels of indirection (i.e., a.b.c.d or a[b].c->d)
r. Has functions with fewer than six levels of indented scope, counted as follows:

```
int function()
{
    if (a = true)
    {
        if ( b = true )
```

```
2 {
    if ( c = true )
3 {
        if ( d = true )
4 {
            while(e > 0 )
5 {
                code
            }
        }
    }
}
}
```

s. Initializes every variable upon declaration where permitted

t. t. Has all constants other than 0 and 1 defined or enumerated, or shall have a comment which clearly explains what each constant means in the context of its use. Where "0" and "1" have multiple meanings in the code unit, even they should be identified. Example: "0" may be used as FALSE, initializing a counter to zero, or as a special flag in a non-binary category

u. Only contains the minimum implementation of the "a = b ? c : d" syntax. Expansions such as "j=a?(b?c:d):e;" are prohibited

v. Has all assert() statements coded such that they are absent from a production compilation. Such coding may be implemented by ifdef()s that remove them from or include them in the compilation. If implemented, the initial program identification in setup should identify that assert() is enabled and active as a test version

6 System Integration Testing

Table of Contents

6 System Integration Testing

6.1 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.

6.2 Basis of Integration Testing

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

6.2.1 Testing Breadth

The 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 Section 3. Where practical, the VSTL will perform coverage reporting of the software branches executed in the functional testing. The selection of the baseline test cases will follow an operational profile of the common procedures, sequencing, and options among the shared state requirements and those that are specifically recognized and supported by the manufacturer. The VSTL will use the coverage report to identify any portions of the source code that were not covered and determine:

a. The additional functional tests that are needed
b. Where more detailed source code review is needed
c. Both of the above

The specific procedures to be used shall be identified in the National Certification Test Plan. These procedures may replicate testing performed by the 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.

6.2.2 System Baseline for Testing

The system level certification tests are conducted using the version of the system intended to be sold by the 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.

6.2.3 Testing Volume

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

6.3 Testing Interfaces of System Components

The 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.

6.4 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.

6.4.1 Access Control

The accredited testing laboratory shall conduct tests of system capabilities and review the access control policies and procedures submitted by the 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 VSTL 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.

6.4.2 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

6.5 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 3.1
b. Voting machines intended for use by voters with disabilities provide the capabilities required by Volume I, Subsection 3.2
c. Voting machines intended for use by voters with disabilities operate consistently with manufacturer specifications and documentation

6.6 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.

6.7 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.

7 Quality Assurance Testing

Table of Contents

7 Quality Assurance Testing

7.1 Scope

This section contains a description of the examination performed by the VSTL to verify conformance with the requirements for configuration management and quality assurance of voting systems. It describes the scope and basis for the examinations, the general sequence of the examinations within the overall test process, and provides guidance on the substantive focus of the examinations.

7.2 Basis of Examinations

The VSTL shall design and perform procedures that examine documented manufacturer practices for quality assurance and configuration management as addressed by Volume I, Sections 8 and 9 and Section 2.

Examination procedures shall be designed and performed to ensure:

a. Conformance with the requirements to provide information on manufacturer practices required by these *Guidelines*
b. Conformance of system documentation and other information provided by the manufacturer with the 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 can conduct 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. These include surveys, interviews with individuals at all levels of the development team, and examination of selected internal work products such as system change requests and problem tracking logs.

It is recognized that examinations of manufacturer practices, and determinations of conformance, entail a significant degree of professional judgment. These guidelines for manufacturer practices identify specific areas of focus but heavily rely on the expertise and professional judgment, of the VSTL.

The specific procedures used by the VSTL shall be identified in the Qualification Test Plan. Recognizing variations in manufacturers' quality assurance and configuration management practices and procedures, the VSTL shall design examination procedures that account for these variations.

7.3 General Examinations Sequence

There is no required sequence for performing the examinations of quality assurance and configuration management practices. No other testing is dependent on the performance and results of these examinations. However, examinations pertaining to configuration management, in particular those pertaining to configuration identification, will generally be useful in understanding the conventions used to define and document the components of the system and will assist with other elements of the certification test process.

7.3.1 Manufacturer Practices in Parallel with Other Certification Testing

While not required, the VSTL is encouraged to initiate the examinations of quality assurance and configuration management practices early in the overall testing sequence, and to conduct them in parallel with other testing of the voting system. Conducting these examinations in parallel is recommended to minimize the overall duration of the testing process.

7.3.2 Functional Configuration Audit and System Integration Testing

As described in Volume I, Section 9, the functional configuration audit verifies that the voting system performs all the functions described in the system documentation. To help ensure an efficient test process, this audit shall be conducted by the VSTL as an element of the system integration testing that confirms the proper functioning of the system as a whole.

7.4 Examination of Configuration Management Practices

The examination of configuration management practices shall address the full scope of requirements described in Volume I, Section 9, and the documentation requirements described in Section 2. In addition to confirming that all required information has been submitted, the VSTL shall determine the manufacturer's conformance with the documented configuration management practices.

7.4.1 Configuration Management Policy

The VSTL shall examine the manufacturer's documented configuration management policy to confirm that it:

a. Addresses the full scope of the system, including components provided by external suppliers

b. Addresses the full breadth of system documentation

7.4.2 Configuration Identification

The VSTL shall examine the manufacturer's documented configuration identification practices policy to confirm that it:

a. Describes clearly the basis for classifying configuration items into categories and subcategories, for numbering of configuration items; and for naming of configuration items
b. Describes clearly the conventions used to identify the version of the system as a whole and the versions of any lower level elements (e.g., subsystems, individual elements) if such lower level version designations are used

7.4.3 Baseline, Promotion, and Demotion Procedures

The VSTL shall examine the manufacturer's documented baseline, promotion, and demotion procedures to confirm that they:

a. Provide a clear, controlled process that promotes components to baseline status when specific criteria defined by the manufacturer are met; and
b. Provide a clear, controlled process for demoting a component from baseline status when specific criteria defined by the manufacturer are met.

7.4.4 Configuration Control Procedures

The VSTL shall examine the manufacturer's configuration control procedures to confirm that they:

a. Are capable of providing effective control of internally developed system components
b. Are capable of providing effective control of components developed or supplied by third parties

7.4.5 Release Process

The VSTL shall examine the manufacturer's release process to confirm that it:

a. Provides clear accountability for moving forward with the release of the initial system version and subsequent releases
b. Provides the means for clear identification of the system version being replaced

c. Confirms that all required internal manufacturer tests and audits prior to release have been completed successfully
d. Confirms that each system version released to customers has been certified
e. Confirms that each system release has been received by the customer
f. Confirms that each system release has been installed successfully by the customer

7.4.6 Configuration Audits

The VSTL shall examine the manufacturer's configuration audit procedures to confirm that they:

a. Are sufficiently broad in scope to address the entire system, including system documentation
b. Are conducted with appropriate timing to enable effective control of system versions
c. Are sufficiently rigorous to confirm that all system documentation prepared and maintained by the manufacturer matches the actual system functionality, design, operation, and maintenance requirements

7.4.7 Configuration Management Resources

The VSTL shall examine the configuration management resource information submitted by the manufacturer to determine whether sufficient information has been provided to enable another organization to clearly identify the resources used and acquire them for use. This examination is intended to ensure that in the event the manufacturer concludes business operations, sufficient information has been provided to enable an in-depth audit of the system should such an audit be required by election officials and/or a law enforcement organization.

7.5 Examination of Quality Assurance Practices

The examination of quality assurance practices shall address the full scope of requirements described in Volume I, Section 8, and the documentation requirements described in Volume II, Section 2. The VSTL shall confirm that all required information has been submitted, and assess whether the manufacturer's quality assurance program provides for:

a. Clearly measurable quality standards
b. An effective testing program throughout the system development life cycle
c. Application of the quality assurance program to external providers of system components and supplies
d. Comprehensive monitoring of system performance in the field and diagnosis of system failures

e. Effective record keeping of system failures to support analysis of failure patterns and potential causes
f. Effective processes for notifying customers of system failures and corrective measures that need to be taken, and for confirming that such measures are taken

In addition to the general examinations described above, the VSTL shall focus on the specific elements of the manufacturer's quality assurance program indicated below.

7.5.1 Quality Assurance Policy

The VSTL shall examine the manufacturer's quality assurance policy to confirm that it:

a. Addresses the full scope of the voting system
b. Clearly designates a senior level individual accountable for implementation and oversight of quality assurance activities
c. Clearly designates the individuals, by position within the manufacturer's organization, who are to conduct each quality assurance activity
d. Provides procedures that determine compliance with, and correct deviations from, the quality assurance program at a minimum annually

7.5.2 Parts and Materials Tests

The VSTL shall examine the manufacturer's parts and materials special tests and examinations to confirm that they:

a. Identify appropriate criteria that are used to determine the specific system components for which special tests are required to confirm their suitability for use in a voting system
b. Are designed in a manner appropriate to determine suitability
c. Have been conducted and documented for all applicable parts and materials

7.5.3 Quality Conformance Inspections

The VSTL shall examine the manufacturer's quality conformance plans, procedures and, inspection results to confirm that:

a. All components have been tested according to the test requirements defined by the manufacturer
b. All components have passed the requisite tests
c. For each test, the test documentation identifies:
    i. Test location
    ii. Test date
    iii. Individual who conducted the test
    iv. Test outcome

7.5.4 Documentation

The VSTL shall examine the manufacturer's voting system documentation to confirm that it meets the content requirements of Volume I, Subsection 8.7, and Section 2, and is written in a manner suitable for use by purchasing jurisdictions.

Appendix A: National Certification Test Plan

Table of Contents

Appendix A: National Certification Test Plan

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 ballot cards and control cards, standard and optional output data report formats, and any other materials used to simulate preparation for, and conduct of, elections.

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, Chapter 4. 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
Humidity test

Operating tests involving a series of procedures that test system reliability and accuracy under various temperatures and voltages relevant to election use

A.3.3 Software Module Test Case Design and Data

The VSTL shall review the manufacturer's program analysis, documentation, and, if available, 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.

If the manufacturer's module test case design does not provide conclusive coverage of all program paths, then the VSTL shall perform an independent analysis to assess the frequency and consequence of error of the untested paths. The VSTL shall design additional module test cases, as required, to provide coverage of all modules containing untested paths with potential for untrapped errors.

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 (3.4, 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.

Appendix A: National Certification Test Plan

A.1 Scope

This Appendix contains a recommended outline for the National Certification Test Plan, which is to be prepared by the test lab. The primary purpose of the test plan is to document the test lab's development of the complete or partial certification test. A sample outline is provided in Figure A-1 at the end of this Appendix.

It is intended that the test lab use this Appendix as a guide in preparing a detailed test plan, and that the scope and detail of the requirements for certification be tailored to the type of hardware, and the design and complexity of the software being tested. Required hardware tests are defined in Section 4, whereas software and system-level tests must be developed based on the vendor pre-certification tests and information available on the specific software's physical and functional configuration.

Prior to development of any test plan, the test lab must obtain the Technical Data Package (TDP) from the vendor submitting the voting system for certification. The TDP contains information necessary to the development of the test plan, such as the vendor's Hardware Specifications, Software Specifications, System Operating Manual and System Maintenance Manual.

It is specified by the Guidelines that voting systems incorporating the vendor's software and COTS hardware need only be submitted for software and system level tests. Recertification of systems with modified software or hardware is also anticipated. The test lab shall alter the test plan outline as required by these situations.

The following discussion describes the individual sections of the recommended National Certification Test Plan. The test lab shall include the identification, and a brief description of, the hardware and software to be tested, and any special considerations that affect the test design and procedure.

A.1.1References

The test lab shall list all documents that contain material used in preparing the test plan. This list shall include specific references to applicable portions of the guidelines, and to the vendor's TDP.

A.1.2Terms and Abbreviations

The test lab shall list and define all terms and phrases relevant to the hardware, the software, or the test plan.

A.2 Pre-certification Tests

The test lab shall evaluate vendor tests, or other lab tests in determining the scope of testing required for system certification. Pre-certification test activities may be particularly useful in designing software functional test cases and tests of system security. The test lab shall summarize pre-certification test results that support the discussion of the preceding section.

A.3 Materials Required for Testing

The following materials must be provided to the test lab to facilitate testing of the voting system:

a. Software
b. Equipment
c. Test materials
d. Deliverable materials
e. Proprietary data

A.3.1Software

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

A.3.2Equipment

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

A.3.3Test Materials

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

~~A.3.4Deliverable Materials~~

~~The test lab shall list all documents and materials to be delivered as a part of the system, such as:~~

~~a. Hardware specification~~
~~b. Software specification~~
~~c. Voter, operator, hardware, and software maintenance manuals~~
~~d. Program listings, facsimile ballots, tapes~~
~~e. Sample output report formats~~

~~A.3.5Proprietary Data~~

~~The test lab shall list and describe all documentation and data that are proprietary to the vendor, and hence are subject to restrictions with respect to test lab use, release, or disclosure.~~

~~A.4 Test Specifications~~

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

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

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

~~A.4.1Hardware Configuration and Design~~

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

A.4.2Software System Functions

The test lab shall describe the software functions in sufficient detail to provide a foundation for selecting the test case designs and conditions described in Section A.4.3. On the basis of this test case design, the test lab shall prepare a table delineating software functions and how each shall be tested.

A.4.3Test Case Design

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

a. Hardware qualitative examination design
b. Hardware environmental test case design
c. Software module test case design and data
d. Software functional test case design
e. System level test case design

A.4.3.1 Hardware Qualitative Examination Design

The test lab shall review the results, submitted by the vendor, of any previous examinations of the equipment to be tested. The results of these examinations shall be compared to the performance characteristics specified by Section 2 of the Guidelines concerning the requirements for:

a. Overall system capabilities
b. Pre-voting functions
c. Voting functions
d. Post-voting functions

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

A.4.3.2 Hardware Environmental Test Case Design

The test lab shall review the documentation, submitted by the vendor, of the results and design of any previous environmental tests of the equipment submitted for testing. The test design and results shall be compared to the tests described in Section 1. The test lab shall cite any additional tests required, based on this review and those tests requested by the vendor or the state. The test lab shall also cite any environmental tests that are not to be conducted, and note the reasons why.

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

a. Non-operating tests, including the:
    i. Bench handling test
    ii. Vibration test
    iii. Low temperature test
    iv. High temperature test
    v. Humidity test
b. Operating tests involving a series of procedures that test system reliability and accuracy under various temperatures and voltages relevant to election use

A.4.3.3 Software Module Test Case Design and Data

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

If the vendor's module test case design does not provide conclusive coverage of all program paths, then the test lab shall perform an independent analysis to assess the frequency and consequence of error of the untested paths. The test lab shall design additional module test cases, as required, to provide coverage of all modules containing untested paths with potential for untrapped errors.

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

A.4.3.4 Software Functional Test Case Design

The test lab shall review the vendor's test plans and data to verify that the individual performance requirements described in Subsection 2.5.3, are reflected in the software.

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

The vendor's test case design may be evaluated by any standard or special method appropriate; however, emphasis shall be placed on those functions where the vendor data

~~on module development reflects significant debugging problems, and on functional tests that resulted in disproportionately high error rates.~~

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

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

~~a. Ballot preparation subsystem~~
~~b. Test operations performed prior to, during, and after processing of ballots, including:~~
- ~~i. Logic tests to verify interpretation of ballot styles, and recognition of precincts to be processed~~
- ~~ii. Accuracy tests to verify ballot reading accuracy~~
- ~~iii. Status tests to verify equipment statement and memory contents~~
- ~~iv. Report generation to produce test output data~~
- ~~v. Report generation to produce audit data records~~

~~c. Procedures applicable to equipment used in the polling place for:~~
- ~~i. Opening the polling place and enabling the acceptance of ballots and maintaining a count of processed ballots~~
- ~~ii. Monitoring equipment status~~
- ~~iii. Verifying equipment response to operator input commands~~
- ~~iv. Generating real-time audit messages~~
- ~~v. Closing the polling place and disabling the acceptance of ballots~~
- ~~vi. Generating election data reports~~
- ~~vii. Transfer of ballot counting equipment, or a detachable memory module, to a central counting location~~
- ~~viii. Electronic transmission of election data to a central counting location~~

~~d. Procedures applicable to equipment used in a central counting place:~~
- ~~i. Initiating the processing of a ballot deck or programmable memory device for one or more precincts~~
- ~~ii. Monitoring equipment status~~
- ~~iii. Verifying equipment response to operator input commands~~
- ~~iv. Verifying interaction with peripheral equipment, or other data processing systems~~
- ~~v. Generating real-time audit messages~~
- ~~vi. Generating precinct-level election data reports~~
- ~~vii. Generating summary election data reports~~
- ~~viii. Transfer of a detachable memory module to other processing equipment~~
- ~~ix. Electronic transmission of data to other processing equipment~~
- ~~x. Producing output data for interrogation by external display devices~~

A.4.3.5 System-level Test Case Design

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

a. 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.
b. 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.
c. 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.
d. Accessibility tests: The test lab shall review the vendor's documentation of the usability and accessibility testing performed during system development.
e. 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.
f. Performance tests: These tests verify accuracy, processing rate, ballot format handling capability, and other performance attributes claimed by the vendor.
g. Recovery tests: These tests verify the ability of the system to recover from hardware and data errors.

A.5 Test Data

A.5.1Data Recording

The test lab shall identify all data recording requirements (e.g.; what is to be measured, how tests and results are to be recorded). The test lab shall also design or approve the design of forms or other recording media to be employed. The test lab shall supply any special instrumentation (e.g., pulse measuring device) needed to satisfy the data requirements.

A.5.2Test Data Criteria

The test lab shall describe the criteria against which test results will be evaluated, such as the following:

a. Tolerances: These criteria define the acceptable range for system performance. These tolerances shall be derived from the applicable hardware performance requirements contained in Volume I, Section 4
b. Samples: These criteria define the minimum number of combinations or alternatives of input and output conditions that can be exercised to constitute an acceptable test of the parameters involved
c. Events: These criteria define the maximum number of interrupts, halts or other system breaks that may occur due to nontest conditions. This count shall not include events from which recovery occurs automatically or where a relevant status message is displayed

A.5.3Test Data Reduction

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

A.6 Test Procedure and Conditions

The test lab shall describe the test conditions and procedures for performing the tests. If tests are not to be performed in random order, this section shall contain the rationale for the required sequence, and the criteria that must be met, before the sequence can be continued. This section shall also describe the procedure for setting up the equipment in which the software will be tested, for system initialization, and for performing the tests. Each of the following sections that contain a description of a test procedure shall also contain a statement of the criteria by which readiness and successful completion shall be indicated and measured.

A.6.1Facility Requirements

The test lab shall describe the space, equipment, instrumentation, utilities, manpower, and other resources required to support the test program.

A.6.2Test Set-up

The test lab shall describe the procedure for arranging and connecting the system hardware with the supporting hardware and telecommunications equipment, if applicable. It shall also describe the procedure required to initialize the system, and to verify that it is ready to be tested.

A.6.3Test Sequence

The test lab shall state any restrictions on the grouping or sequence of tests in this section.

A.6.4Test Operations Procedures

The test lab shall provide the step-by-step procedures for each test case to be conducted. Each step shall be assigned a test step number and this number, along with critical test data and test procedures information, shall be tabulated onto a test report form for test control and the recording of test results.

In this section, the test lab shall also identify all test operations personnel, and their respective duties. In the event that the operator procedure is not defined in the vendor's operations or user manual, the test lab shall also provide a description of the procedures to be followed by the test personnel.

Figure 7 - Test Plan Outline

1. Introduction
    - 1.1 References
    - 1.2 Terms and Abbreviations
2. Pre-certification Tests
    - 2.1 Pre-certification Test Activity
    - 2.2 Pre-certification Test Results
3. Materials Required for Testing
    - 3.1 Software
    - 3.2 Equipment
    - 3.3 Test Materials

Appendix B: National Certification Test Report

Table of Contents

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. Witness 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 failure rate and the failure rate that was demonstrated with 90 % confidence for each type of device, for each applicable failure type in the table of Volume I, Section 4.3.3;

- 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;
- 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.

Witness Build

The VSTL shall include as Appendix C of the Test Report a copy of the record of the final witness build and 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 form 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 B: National Certification Test Report~~

~~B.1 Scope~~

~~This Appendix contains a recommended outline for the National Certification Test Report to be prepared by the accredited test lab. The test report shall be organized so as to facilitate the presentation of conclusions and recommendations regarding system acceptability, a summary of the test operations, a summary of the test results, the test data records, and the analyses that support the conclusions and recommendations. The content of the report may vary based on the scope of review conducted.~~

~~B.1.1 New Certification Test Report~~

~~A full report is prepared for the initial certification testing of a voting system. This document consists of five main sections: Introduction, Certification Test Background, System Identification, System Overview, and Certification Test Results.~~

~~Detailed information about the test operations and findings, and test data, are included as appendices to the report.~~

~~Sections B.2 through B.7 describe the contents of the individual sections of this report.~~

~~B.1.2 Changes to Previously Certified Test Report~~

~~This report addresses a wide range of scenarios. After a preliminary review of the submitted changes, the accredited test lab may determine that:~~

~~a. A review of all change documentation against the baseline materials is sufficient for recommendation for certification~~
~~b. All changes must be retested against the previously certified baseline~~
~~c. The scope of the changes is substantial enough that a complete retest of the software is required~~

~~The format of this report will vary, based on the type of review that is performed. If only a review of change documentation against the baseline materials is performed the report is quite simple. It consists of an Introduction, a Version Description, the Testing Approach, and a Results Summary. A more extensive report is prepared, for changes that have extensive impact on the system design and/or operations.~~

B.2 Certification Test Background

This section contains the following information:

a. General information about the certification test process
b. A list and definition of all terms and nomenclature peculiar to the hardware, the software, or the test report

B.3 System Identification

This section gives information about the tested software and supporting hardware, including:

a. System name and major subsystems (or equivalent)
b. System version
c. Test support hardware
d. Specific documentation provided in the vendor's TDP used to support testing

B.4 System Overview

This section describes the voting system in terms of its overall design structure, technologies used, processing capacity claimed by the vendor for system components (such as ballot counters, voting machines, vote consolidation equipment), and mode of operation. It may also identify other products that interface with the voting system.

B.5 Certification Test Results and Recommendation

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

a. The acceptability of the system design and construction based on the performance of the system hardware, software and communications, and on the source code inspection
b. The degree to which the hardware and software meet the vendor's specifications and the guidelines, and the acceptability of the vendor's technical and user documentation
c. General findings on the maintainability of the system including, where applicable, notation of specific maintenance activities that are determined to be difficult to perform
d. Identification and description of any deficiencies that remain uncorrected after completion of the certification test and that have caused or are judged to be capable of causing, the loss or corruption of voting data, providing sufficient detail to support a recommendation to reject the system being tested. Similarly,

any deficiency in compliance with the security, accuracy, data retention, and audit requirements are fully described

e. A specific recommendation to the EAC for approval or rejection

Of note, any uncorrected deficiency that does not involve the loss or corruption of voting data shall not necessarily be cause for rejection. Deficiencies of this type may include failure to fully achieve the levels of performance specified in Volume I or failure to fully implement formal programs for quality assurance and configuration management described in Volume I, Sections 8 and 9. The nature of the deficiency is described in detail sufficient to support the recommendation either to accept or to reject the system. The recommendation is based on consideration of the probable effect the deficiency will have on safe and efficient system operation during all phases of election use.

B.6 Appendix - Test Operations and Findings

This appendix provides additional detail about the test results to enable the understanding of test results and recommendation. This information is organized in a manner that reflects the Certification Test Plan. Summaries of the results of hardware examinations, operating and non-operating hardware tests, software module tests, software function tests, and system-level tests (including security and telecommunications tests, and the results of the Physical and Functional Configuration Audits) are provided.

B.7 Appendix - Test Data Analysis

This appendix provides summary records of the test data and the details of the analysis. The analysis includes a comparison of the vendor's hardware and software specifications to the test data, together with any mathematical or statistical procedure used for data reduction and processing.

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

Table of Contents

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

C.1 General Method

Reliability, accuracy, and misfeed rate are measured using ratios, each of which is the number of some kind of event (failures, errors, or misfeeds, respectively) divided by some measure of voting volume. The test method discussed here is applicable generically to all three ratios; 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 events occur in a Poisson distribution, which means that the probability of an event occurring is assumed to be the same for each unit of volume processed. In reality, there are random events that satisfy this assumption but there are also nonrandom events that do not. For example, a logic error in tabulation software might be triggered every time a particular voting option is used. Consequently, a test suite that exercised that voting option often would be more likely to indicate rejection based on reliability or accuracy than a test suite that used different tests. However, since these Guidelines require absolute correctness of tabulation logic, the only undesirable outcome is the one in which the system containing the logic error is accepted. Other evaluations specified in these Guidelines, such as functional testing and logic verification, are better suited to detecting systems that produce nonrandom errors and failures. Thus, when all specified evaluations are used together, the different test methods complement each other and the limitation of this particular test method with respect to nonrandom events is not bothersome.

For simplicity, all three cases (failures, errors, and misfeeds) are modelled using a Poisson distribution rather than a binomial distribution. In this application, where the probability of an event occurring within a unit of volume is small, the difference in results from the two different models is negligible.

The problem is approached through classical hypothesis testing. The null hypothesis (H_0) 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_0: $r_t \leq r_b$

The alternative hypothesis (H_1) 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_1: $r_t > r_b$

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 more events occurring given a (marginally) conforming system is less than 0.1. H_0 is rejected if $1-P(n_o-1,r_bv_o)<0.1$, which is equivalent to $P(n_o-1,r_bv_o)>0.9$. This corresponds to the 90th 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 conformity has been demonstrated. It merely means that there is insufficient evidence to demonstrate non-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 $P(n_o,r_dv_o)=0.1$ 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 reliability, accuracy, or misfeed rate as this would bias the results. A Probability Ratio Sequential Test (PRST) as was specified in previous versions of these Guidelines 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 and p=0.9 for $0 \le n \le 750$.

Given n_o observed events after volume v_o, the demonstrated event rate r_d is found by solving $P(n_o,r_d v_o)=0.1$ for r_d. The pertinent factor is in the second column (p=0.1) in the row for $n=n_o$; dividing this factor by v_o yields r_d. For example, a volume of 600 with no events demonstrates an event rate of 2.302585/600, or 3.837642×10^{-3}.

Since the condition for rejecting H_0 is $P(n_o-1,r_b v_o)>0.9$, the critical value v_c, which is the minimum volume at which H_0 is not rejected for n_o observed events and event rate benchmark r_b, is found by solving $P(n_o-1,r_b v_c)=0.9$ for v_c. The pertinent factor is in the third column (p=0.9) in the row for $n=n_o-1$; dividing this factor by r_b yields v_c. For example, if a test with event rate benchmark $r_b=10^{-4}$ resulted in one observed event, then the system would be rejected unless the actual volume was at least $0.1053605/10^{-4}$, or 105.3605. Where the measurement of volume is discrete rather than continuous, one would round up to the next integer.

n	rv satisfying $P(n,rv)=0.1$	rv satisfying $P(n,rv)=0.9$	n	rv satisfying $P(n,rv)=0.1$	rv satisfying $P(n,rv)=0.9$	n	rv satisfying $P(n,rv)=0.1$	rv satisfying $P(n,rv)=0.9$
0	2.302585	0.1053605	250	271.5057	230.9226	500	529.8906	472.5376
1	3.889720	0.5318116	251	272.5461	231.8821	501	530.9192	473.5090
2	5.322320	1.102065	252	273.5864	232.8418	502	531.9478	474.4804
3	6.680783	1.744770	253	274.6267	233.8015	503	532.9764	475.4519
4	7.993590	2.432591	254	275.6669	234.7613	504	534.0049	476.4233
5	9.274674	3.151898	255	276.7070	235.7212	505	535.0334	477.3948
6	10.53207	3.894767	256	277.7470	236.6812	506	536.0619	478.3663
7	11.77091	4.656118	257	278.7870	237.6412	507	537.0904	479.3379
8	12.99471	5.432468	258	279.8269	238.6013	508	538.1188	480.3094
9	14.20599	6.221305	259	280.8667	239.5615	509	539.1472	481.2811
10	15.40664	7.020747	260	281.9064	240.5218	510	540.1755	482.2527
11	16.59812	7.829342	261	282.9460	241.4822	511	541.2039	483.2243
12	17.78159	8.645942	262	283.9856	242.4426	512	542.2322	484.1960
13	18.95796	9.469621	263	285.0251	243.4031	513	543.2605	485.1677
14	20.12801	10.29962	264	286.0645	244.3637	514	544.2887	486.1395
15	21.29237	11.13530	265	287.1039	245.3243	515	545.3170	487.1113
16	22.45158	11.97613	266	288.1432	246.2851	516	546.3452	488.0831
17	23.60609	12.82165	267	289.1824	247.2459	517	547.3734	489.0549
18	24.75629	13.67148	268	290.2215	248.2067	518	548.4015	490.0267
19	25.90253	14.52526	269	291.2605	249.1677	519	549.4296	490.9986
20	27.04510	15.38271	270	292.2995	250.1287	520	550.4577	491.9705
21	28.18427	16.24356	271	293.3384	251.0898	521	551.4858	492.9424
22	29.32027	17.10758	272	294.3773	252.0509	522	552.5138	493.9144
23	30.45330	17.97457	273	295.4160	253.0122	523	553.5418	494.8864
24	31.58356	18.84432	274	296.4547	253.9735	524	554.5698	495.8584
25	32.71121	19.71669	275	297.4934	254.9349	525	555.5978	496.8304

n	rv satisfying $P(n,rv) = 0.1$	rv satisfying $P(n,rv) = 0.9$	n	rv satisfying $P(n,rv) = 0.1$	rv satisfying $P(n,rv) = 0.9$	n	rv satisfying $P(n,rv) = 0.1$	rv satisfying $P(n,rv) = 0.9$
26	33.83639	20.59152	276	298.5319	255.8963	526	556.6257	497.8025
27	34.95926	21.46867	277	299.5704	256.8578	527	557.6536	498.7746
28	36.07992	22.34801	278	300.6088	257.8194	528	558.6815	499.7467
29	37.19850	23.22944	279	301.6472	258.7810	529	559.7094	500.7189
30	38.31510	24.11285	280	302.6855	259.7428	530	560.7372	501.6910
31	39.42982	24.99815	281	303.7237	260.7046	531	561.7650	502.6632
32	40.54274	25.88523	282	304.7618	261.6664	532	562.7928	503.6355
33	41.65395	26.77403	283	305.7999	262.6283	533	563.8205	504.6077
34	42.76352	27.66447	284	306.8379	263.5903	534	564.8482	505.5800
35	43.87152	28.55647	285	307.8758	264.5524	535	565.8759	506.5523
36	44.97802	29.44998	286	308.9137	265.5145	536	566.9036	507.5246
37	46.08308	30.34493	287	309.9515	266.4767	537	567.9313	508.4970
38	47.18676	31.24126	288	310.9893	267.4390	538	568.9589	509.4694
39	48.28910	32.13892	289	312.0269	268.4013	539	569.9865	510.4418
40	49.39016	33.03786	290	313.0646	269.3637	540	571.0140	511.4142
41	50.48999	33.93804	291	314.1021	270.3261	541	572.0416	512.3866
42	51.58863	34.83941	292	315.1396	271.2886	542	573.0691	513.3591
43	52.68612	35.74192	293	316.1770	272.2512	543	574.0966	514.3316
44	53.78250	36.64555	294	317.2144	273.2138	544	575.1241	515.3042
45	54.87781	37.55024	295	318.2517	274.1765	545	576.1515	516.2767
46	55.97209	38.45597	296	319.2889	275.1393	546	577.1789	517.2493
47	57.06535	39.36271	297	320.3261	276.1021	547	578.2063	518.2219
48	58.15765	40.27042	298	321.3632	277.0650	548	579.2337	519.1945
49	59.24900	41.17907	299	322.4002	278.0280	549	580.2610	520.1672
50	60.33944	42.08863	300	323.4372	278.9910	550	581.2884	521.1399
51	61.42899	42.99909	301	324.4741	279.9541	551	582.3156	522.1126
52	62.51768	43.91040	302	325.5110	280.9172	552	583.3429	523.0853
53	63.60553	44.82255	303	326.5478	281.8804	553	584.3702	524.0581
54	64.69257	45.73552	304	327.5845	282.8437	554	585.3974	525.0309
55	65.77881	46.64928	305	328.6212	283.8070	555	586.4246	526.0037
56	66.86429	47.56380	306	329.6578	284.7704	556	587.4517	526.9765
57	67.94901	48.47908	307	330.6944	285.7338	557	588.4789	527.9493
58	69.03300	49.39509	308	331.7309	286.6973	558	589.5060	528.9222
59	70.11628	50.31182	309	332.7673	287.6609	559	590.5331	529.8951
60	71.19887	51.22923	310	333.8037	288.6245	560	591.5602	530.8681
61	72.28078	52.14733	311	334.8400	289.5882	561	592.5872	531.8410
62	73.36203	53.06608	312	335.8763	290.5519	562	593.6142	532.8140
63	74.44263	53.98548	313	336.9125	291.5157	563	594.6412	533.7870
64	75.52260	54.90551	314	337.9486	292.4796	564	595.6682	534.7600
65	76.60196	55.82616	315	338.9847	293.4435	565	596.6952	535.7331
66	77.68071	56.74741	316	340.0208	294.4074	566	597.7221	536.7061
67	78.75888	57.66924	317	341.0568	295.3715	567	598.7490	537.6792
68	79.83647	58.59165	318	342.0927	296.3355	568	599.7759	538.6523
69	80.91350	59.51463	319	343.1285	297.2997	569	600.8028	539.6255

n	rv satisfying $P(n,rv) = 0.1$	rv satisfying $P(n,rv) = 0.9$	n	rv satisfying $P(n,rv) = 0.1$	rv satisfying $P(n,rv) = 0.9$	n	rv satisfying $P(n,rv) = 0.1$	rv satisfying $P(n,rv) = 0.9$
70	81.98997	60.43815	320	344.1643	298.2639	570	601.8296	540.5986
71	83.06591	61.36221	321	345.2001	299.2281	571	602.8564	541.5718
72	84.14132	62.28680	322	346.2358	300.1924	572	603.8832	542.5450
73	85.21622	63.21191	323	347.2714	301.1568	573	604.9099	543.5183
74	86.29061	64.13753	324	348.3070	302.1212	574	605.9367	544.4915
75	87.36450	65.06364	325	349.3426	303.0857	575	606.9634	545.4648
76	88.43790	65.99023	326	350.3780	304.0502	576	607.9901	546.4381
77	89.51083	66.91731	327	351.4135	305.0148	577	609.0168	547.4115
78	90.58329	67.84485	328	352.4488	305.9794	578	610.0434	548.3848
79	91.65529	68.77285	329	353.4842	306.9441	579	611.0700	549.3582
80	92.72684	69.70130	330	354.5194	307.9088	580	612.0966	550.3316
81	93.79795	70.63019	331	355.5546	308.8736	581	613.1232	551.3050
82	94.86863	71.55951	332	356.5898	309.8384	582	614.1498	552.2785
83	95.93888	72.48927	333	357.6249	310.8033	583	615.1763	553.2519
84	97.00871	73.41944	334	358.6599	311.7683	584	616.2028	554.2254
85	98.07813	74.35002	335	359.6949	312.7333	585	617.2293	555.1989
86	99.14714	75.28100	336	360.7299	313.6983	586	618.2558	556.1725
87	100.2158	76.21239	337	361.7648	314.6634	587	619.2822	557.1460
88	101.2840	77.14416	338	362.7996	315.6286	588	620.3086	558.1196
89	102.3518	78.07631	339	363.8344	316.5938	589	621.3350	559.0932
90	103.4193	79.00885	340	364.8692	317.5591	590	622.3614	560.0668
91	104.4864	79.94175	341	365.9038	318.5244	591	623.3878	561.0405
92	105.5531	80.87502	342	366.9385	319.4897	592	624.4141	562.0141
93	106.6195	81.80865	343	367.9731	320.4552	593	625.4404	562.9878
94	107.6855	82.74263	344	369.0076	321.4206	594	626.4667	563.9615
95	108.7512	83.67695	345	370.0421	322.3861	595	627.4930	564.9353
96	109.8165	84.61162	346	371.0765	323.3517	596	628.5192	565.9090
97	110.8815	85.54663	347	372.1109	324.3173	597	629.5454	566.8828
98	111.9462	86.48197	348	373.1453	325.2830	598	630.5716	567.8566
99	113.0105	87.41764	349	374.1796	326.2487	599	631.5978	568.8304
100	114.0745	88.35362	350	375.2138	327.2144	600	632.6240	569.8043
101	115.1382	89.28993	351	376.2480	328.1802	601	633.6501	570.7781
102	116.2016	90.22655	352	377.2821	329.1461	602	634.6762	571.7520
103	117.2647	91.16347	353	378.3162	330.1120	603	635.7023	572.7259
104	118.3275	92.10070	354	379.3503	331.0780	604	636.7284	573.6999
105	119.3899	93.03823	355	380.3843	332.0440	605	637.7544	574.6738
106	120.4521	93.97605	356	381.4182	333.0100	606	638.7804	575.6478
107	121.5140	94.91416	357	382.4521	333.9761	607	639.8064	576.6218
108	122.5756	95.85256	358	383.4860	334.9422	608	640.8324	577.5958
109	123.6369	96.79124	359	384.5198	335.9084	609	641.8584	578.5699
110	124.6980	97.73020	360	385.5536	336.8747	610	642.8843	579.5439
111	125.7587	98.66944	361	386.5873	337.8410	611	643.9102	580.5180
112	126.8192	99.60895	362	387.6209	338.8073	612	644.9361	581.4921
113	127.8794	100.5487	363	388.6546	339.7737	613	645.9620	582.4662

n	rv satisfying $P(n,rv) = 0.1$	rv satisfying $P(n,rv) = 0.9$	n	rv satisfying $P(n,rv) = 0.1$	rv satisfying $P(n,rv) = 0.9$	n	rv satisfying $P(n,rv) = 0.1$	rv satisfying $P(n,rv) = 0.9$
114	128.9394	101.4888	364	389.6881	340.7401	614	646.9879	583.4404
115	129.9991	102.4291	365	390.7217	341.7066	615	648.0137	584.4145
116	131.0586	103.3696	366	391.7552	342.6731	616	649.0395	585.3887
117	132.1177	104.3104	367	392.7886	343.6396	617	650.0653	586.3629
118	133.1767	105.2515	368	393.8220	344.6062	618	651.0911	587.3372
119	134.2354	106.1928	369	394.8553	345.5729	619	652.1168	588.3114
120	135.2938	107.1344	370	395.8886	346.5396	620	653.1426	589.2857
121	136.3520	108.0762	371	396.9219	347.5063	621	654.1683	590.2600
122	137.4100	109.0182	372	397.9551	348.4731	622	655.1940	591.2343
123	138.4677	109.9605	373	398.9883	349.4399	623	656.2196	592.2086
124	139.5252	110.9030	374	400.0214	350.4068	624	657.2453	593.1830
125	140.5825	111.8457	375	401.0545	351.3737	625	658.2709	594.1573
126	141.6395	112.7887	376	402.0875	352.3407	626	659.2965	595.1317
127	142.6963	113.7318	377	403.1205	353.3077	627	660.3221	596.1061
128	143.7529	114.6753	378	404.1535	354.2748	628	661.3477	597.0806
129	144.8093	115.6189	379	405.1864	355.2419	629	662.3732	598.0550
130	145.8655	116.5627	380	406.2192	356.2090	630	663.3987	599.0295
131	146.9214	117.5068	381	407.2520	357.1762	631	664.4242	600.0040
132	147.9771	118.4511	382	408.2848	358.1434	632	665.4497	600.9785
133	149.0326	119.3955	383	409.3176	359.1107	633	666.4752	601.9530
134	150.0880	120.3402	384	410.3503	360.0780	634	667.5006	602.9276
135	151.1431	121.2851	385	411.3829	361.0453	635	668.5261	603.9022
136	152.1980	122.2302	386	412.4155	362.0127	636	669.5515	604.8768
137	153.2527	123.1755	387	413.4481	362.9802	637	670.5768	605.8514
138	154.3072	124.1210	388	414.4806	363.9476	638	671.6022	606.8260
139	155.3615	125.0667	389	415.5131	364.9152	639	672.6276	607.8007
140	156.4156	126.0126	390	416.5455	365.8827	640	673.6529	608.7754
141	157.4695	126.9586	391	417.5779	366.8503	641	674.6782	609.7501
142	158.5233	127.9049	392	418.6103	367.8180	642	675.7035	610.7248
143	159.5768	128.8514	393	419.6426	368.7856	643	676.7287	611.6995
144	160.6302	129.7980	394	420.6749	369.7534	644	677.7540	612.6743
145	161.6834	130.7448	395	421.7071	370.7211	645	678.7792	613.6490
146	162.7364	131.6918	396	422.7393	371.6890	646	679.8044	614.6238
147	163.7892	132.6390	397	423.7714	372.6568	647	680.8296	615.5986
148	164.8418	133.5864	398	424.8035	373.6247	648	681.8548	616.5735
149	165.8943	134.5339	399	425.8356	374.5926	649	682.8799	617.5483
150	166.9465	135.4816	400	426.8676	375.5606	650	683.9050	618.5232
151	167.9987	136.4295	401	427.8996	376.5286	651	684.9302	619.4981
152	169.0506	137.3776	402	428.9316	377.4966	652	685.9552	620.4730
153	170.1024	138.3258	403	429.9635	378.4647	653	686.9803	621.4479
154	171.1540	139.2742	404	430.9954	379.4329	654	688.0054	622.4229
155	172.2054	140.2228	405	432.0272	380.4010	655	689.0304	623.3978
156	173.2567	141.1715	406	433.0590	381.3692	656	690.0554	624.3728
157	174.3078	142.1204	407	434.0907	382.3375	657	691.0804	625.3478

n	rv satisfying $P(n,rv) = 0.1$	rv satisfying $P(n,rv) = 0.9$	n	rv satisfying $P(n,rv) = 0.1$	rv satisfying $P(n,rv) = 0.9$	n	rv satisfying $P(n,rv) = 0.1$	rv satisfying $P(n,rv) = 0.9$
158	175.3587	143.0695	408	435.1225	383.3058	658	692.1054	626.3228
159	176.4095	144.0187	409	436.1541	384.2741	659	693.1304	627.2979
160	177.4601	144.9681	410	437.1858	385.2425	660	694.1553	628.2729
161	178.5106	145.9176	411	438.2174	386.2109	661	695.1802	629.2480
162	179.5609	146.8673	412	439.2489	387.1793	662	696.2051	630.2231
163	180.6111	147.8171	413	440.2805	388.1478	663	697.2300	631.1982
164	181.6611	148.7671	414	441.3119	389.1163	664	698.2549	632.1734
165	182.7109	149.7173	415	442.3434	390.0848	665	699.2797	633.1485
166	183.7606	150.6676	416	443.3748	391.0534	666	700.3045	634.1237
167	184.8102	151.6180	417	444.4062	392.0221	667	701.3293	635.0989
168	185.8596	152.5686	418	445.4375	392.9907	668	702.3541	636.0741
169	186.9089	153.5193	419	446.4688	393.9594	669	703.3789	637.0493
170	187.9580	154.4702	420	447.5001	394.9282	670	704.4036	638.0246
171	189.0069	155.4213	421	448.5313	395.8969	671	705.4284	638.9999
172	190.0558	156.3724	422	449.5625	396.8658	672	706.4531	639.9751
173	191.1045	157.3237	423	450.5936	397.8346	673	707.4778	640.9505
174	192.1530	158.2752	424	451.6247	398.8035	674	708.5025	641.9258
175	193.2014	159.2268	425	452.6558	399.7724	675	709.5271	642.9011
176	194.2497	160.1785	426	453.6868	400.7414	676	710.5518	643.8765
177	195.2978	161.1304	427	454.7178	401.7104	677	711.5764	644.8518
178	196.3458	162.0824	428	455.7488	402.6794	678	712.6010	645.8272
179	197.3937	163.0345	429	456.7797	403.6485	679	713.6256	646.8027
180	198.4414	163.9868	430	457.8106	404.6176	680	714.6501	647.7781
181	199.4890	164.9392	431	458.8415	405.5867	681	715.6747	648.7535
182	200.5365	165.8917	432	459.8723	406.5559	682	716.6992	649.7290
183	201.5839	166.8443	433	460.9031	407.5251	683	717.7237	650.7045
184	202.6311	167.7971	434	461.9338	408.4944	684	718.7482	651.6800
185	203.6781	168.7501	435	462.9646	409.4637	685	719.7727	652.6555
186	204.7251	169.7031	436	463.9952	410.4330	686	720.7972	653.6311
187	205.7719	170.6563	437	465.0259	411.4023	687	721.8216	654.6066
188	206.8186	171.6096	438	466.0565	412.3717	688	722.8461	655.5822
189	207.8652	172.5630	439	467.0871	413.3412	689	723.8705	656.5578
190	208.9117	173.5165	440	468.1176	414.3106	690	724.8949	657.5334
191	209.9580	174.4702	441	469.1481	415.2801	691	725.9192	658.5090
192	211.0043	175.4239	442	470.1786	416.2496	692	726.9436	659.4847
193	212.0504	176.3778	443	471.2090	417.2192	693	727.9679	660.4603
194	213.0963	177.3319	444	472.2394	418.1888	694	728.9922	661.4360
195	214.1422	178.2860	445	473.2698	419.1584	695	730.0165	662.4117
196	215.1879	179.2403	446	474.3001	420.1281	696	731.0408	663.3874
197	216.2336	180.1946	447	475.3304	421.0978	697	732.0651	664.3631
198	217.2791	181.1491	448	476.3607	422.0675	698	733.0893	665.3389
199	218.3245	182.1037	449	477.3909	423.0373	699	734.1136	666.3147
200	219.3698	183.0584	450	478.4211	424.0071	700	735.1378	667.2904
201	220.4150	184.0133	451	479.4513	424.9769	701	736.1620	668.2662

n	rv satisfying $P(n,rv) = 0.1$	rv satisfying $P(n,rv) = 0.9$	n	rv satisfying $P(n,rv) = 0.1$	rv satisfying $P(n,rv) = 0.9$	n	rv satisfying $P(n,rv) = 0.1$	rv satisfying $P(n,rv) = 0.9$
202	221.4600	184.9682	452	480.4814	425.9468	702	737.1862	669.2421
203	222.5050	185.9232	453	481.5115	426.9167	703	738.2103	670.2179
204	223.5498	186.8784	454	482.5416	427.8866	704	739.2345	671.1938
205	224.5945	187.8337	455	483.5716	428.8566	705	740.2586	672.1696
206	225.6392	188.7890	456	484.6016	429.8266	706	741.2827	673.1455
207	226.6837	189.7445	457	485.6316	430.7966	707	742.3068	674.1214
208	227.7281	190.7001	458	486.6615	431.7667	708	743.3309	675.0973
209	228.7724	191.6558	459	487.6914	432.7368	709	744.3550	676.0733
210	229.8166	192.6116	460	488.7213	433.7069	710	745.3790	677.0492
211	230.8607	193.5675	461	489.7511	434.6771	711	746.4030	678.0252
212	231.9047	194.5235	462	490.7810	435.6473	712	747.4270	679.0012
213	232.9485	195.4797	463	491.8107	436.6175	713	748.4510	679.9772
214	233.9923	196.4359	464	492.8405	437.5878	714	749.4750	680.9532
215	235.0360	197.3922	465	493.8702	438.5581	715	750.4990	681.9293
216	236.0796	198.3486	466	494.8999	439.5284	716	751.5229	682.9053
217	237.1231	199.3051	467	495.9295	440.4987	717	752.5468	683.8814
218	238.1664	200.2618	468	496.9591	441.4691	718	753.5708	684.8575
219	239.2097	201.2185	469	497.9887	442.4395	719	754.5946	685.8336
220	240.2529	202.1753	470	499.0182	443.4100	720	755.6185	686.8097
221	241.2960	203.1322	471	500.0478	444.3805	721	756.6424	687.7859
222	242.3390	204.0892	472	501.0773	445.3510	722	757.6662	688.7620
223	243.3819	205.0463	473	502.1067	446.3215	723	758.6901	689.7382
224	244.4247	206.0035	474	503.1361	447.2921	724	759.7139	690.7144
225	245.4674	206.9608	475	504.1655	448.2627	725	760.7377	691.6906
226	246.5100	207.9182	476	505.1949	449.2333	726	761.7614	692.6668
227	247.5525	208.8757	477	506.2242	450.2040	727	762.7852	693.6430
228	248.5949	209.8333	478	507.2535	451.1747	728	763.8089	694.6193
229	249.6372	210.7910	479	508.2828	452.1454	729	764.8327	695.5956
230	250.6795	211.7488	480	509.3120	453.1162	730	765.8564	696.5718
231	251.7216	212.7066	481	510.3413	454.0870	731	766.8801	697.5482
232	252.7636	213.6646	482	511.3704	455.0578	732	767.9038	698.5245
233	253.8056	214.6226	483	512.3996	456.0287	733	768.9274	699.5008
234	254.8475	215.5807	484	513.4287	456.9995	734	769.9511	700.4772
235	255.8893	216.5390	485	514.4578	457.9704	735	770.9747	701.4535
236	256.9310	217.4973	486	515.4869	458.9414	736	771.9983	702.4299
237	257.9726	218.4557	487	516.5159	459.9123	737	773.0219	703.4063
238	259.0141	219.4141	488	517.5449	460.8833	738	774.0455	704.3827
239	260.0555	220.3727	489	518.5739	461.8544	739	775.0691	705.3592
240	261.0969	221.3314	490	519.6028	462.8254	740	776.0926	706.3356
241	262.1381	222.2901	491	520.6317	463.7965	741	777.1162	707.3121
242	263.1793	223.2489	492	521.6606	464.7676	742	778.1397	708.2885
243	264.2204	224.2078	493	522.6894	465.7388	743	779.1632	709.2650
244	265.2614	225.1668	494	523.7183	466.7100	744	780.1867	710.2416
245	266.3023	226.1259	495	524.7471	467.6812	745	781.2102	711.2181

n	rv satisfying $P(n,rv) = 0.1$	rv satisfying $P(n,rv) = 0.9$	n	rv satisfying $P(n,rv) = 0.1$	rv satisfying $P(n,rv) = 0.9$	n	rv satisfying $P(n,rv) = 0.1$	rv satisfying $P(n,rv) = 0.9$
246	267.3431	227.0851	496	525.7758	468.6524	746	782.2336	712.1946
247	268.3839	228.0443	497	526.8046	469.6237	747	783.2571	713.1712
248	269.4246	229.0037	498	527.8333	470.5950	748	784.2805	714.1478
249	270.4652	229.9631	499	528.8620	471.5663	749	785.3039	715.1243
						750	786.3273	716.1010

C.3 Reliability

All tests executed during conformity assessment shall be considered "pertinent" for assessment of reliability, with the following exceptions:

a. Tests in which failures 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 number of failures and the applicable measure of volume for each pertinent test execution, for each type of device, for each applicable failure type addressed in Volume I, Section 4.3.3. "Type of device" refers to the different models produced by the manufacturer. These are not the same as device classes. The system may include several different models of the same class, and a given model may belong to more than one class.

When operational testing is complete, the VSTL shall calculate the failure total and total volume accumulated across all pertinent tests, for each type of device and failure type. If, using the test method in C.1, these values indicate rejection of the null hypothesis for any type of device and type of failure, the verdict on conformity to the requirements of Volume I, Section 4.3.3 shall be Fail. Otherwise, the verdict shall be Pass.

C.4 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 Fail. Otherwise, the verdict shall be Pass.

C.5 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 for any type of device, the verdict on conformity to the misfeed rate requirements of Volume I, Sections 4.1.5.1 shall be Fail. Otherwise, the verdict shall be Pass.

~~Appendix C: National Certification Test Design Criteria~~

~~C.1 Scope~~

~~This appendix describes the guiding principles used to design the voting system certification testing process conducted by the accredited test lab.~~

~~Certification tests are designed to demonstrate that the system meets or exceeds the requirements of the Guidelines. The tests are also used to demonstrate compliance with other levels of performance claimed by the manufacturer.~~

~~Certification tests must satisfy two separate and possibly conflicting sets of considerations. The first is the need to produce enough test data to provide confidence in the validity of the test and its apparent outcome. The second is the need to achieve a meaningful test at a reasonable cost, and cost varies with the difficulty of simulating expected real-world operating conditions and with test duration. It is the test designer's job to achieve an acceptable balance of these constraints.~~

~~The rationale for, and statistical methods of, the test designs required by the Guidelines are discussed below. Technical descriptions of these designs can be found in any of several books on testing and statistical analysis.~~

C.2 Approach to Test Design

The certification tests specified in the Guidelines are primarily concerned with assessing the magnitude of random errors. They are also, however, capable of detecting bias errors that would result in the rejection of the system.

Test data typically produce two results. The first is an estimate of the true value of some system attribute such as speed, error rate, etc. The second is the degree of certainty that the estimate is a correct one. The estimate of an attribute's value may or may not be greatly affected by the duration of the test. Test duration, however, is very important to the degree of certainty; as the length of the test increases, the level of uncertainty decreases. An efficient test design will produce enough data over a sufficient period of time to enable an estimate at the desired level of confidence.

There are several ways to design tests. One approach involves the pre-selection of some test parameter, such as the number of failures or other detectable factors. The essential element of this type of design is that the number of observations is independent of their results. The test may be designed to terminate after 1,000 hours or 10 days, or when 5 failures have been observed. The number of failures is important because the confidence interval (uncertainty band) decreases rapidly as the number of failures increases. However, if the system is highly reliable or very accurate, the length of time required to produce a predetermined number of failures or errors using this method may be unachievably long.

Another approach is to determine that the actual value of some attribute need not be learned by testing, provided that the value can be shown to be better than some level. The test would not be designed to produce an estimate of the true value of the attribute but instead to show, for example, that reliability is at least 123 hours or the error rate is no greater than one in ten million characters.

The latter design approach, which was chosen for the Guidelines, uses what is called Sequential Analysis. Instead of the test duration being fixed, it varies depending on the outcome of a series of observations. The test is terminated as soon as a statistically valid decision can be reached that the factor being tested is at least as good as, or no worse than, the predetermined target value. A sequential analysis test design called the "Wald Probability Ratio Test" is used for reliability and accuracy testing.

C.3 Probability Ratio Sequential Test (PRST)

The design of a Probability Ratio Sequential Test (PRST) requires that four parameters be specified:

H0, the null hypothesis
H1, the alternate hypothesis

a, the producer's risk
b, the consumer's risk

The Guidelines anticipate using the PRST for testing both time-based and event-based failures.

This test design provides decision criteria for accepting or rejecting one of two test hypotheses: the null hypothesis, which is the Nominal Specification Value (NSV), or the alternate hypothesis, which is the MAV. The MAV could be either the Minimum Acceptable Value, or the Maximum Acceptable Value, depending upon what is being tested. Performance may be specified by means of a single value or by two values. When a single value is specified, it shall be interpreted as an upper or lower single-sided 90 percent confidence limit. If two values, these shall be interpreted as a two-sided 90 percent confidence interval, consisting of the NSV and MAV.

In the case of Mean Time Between Failure (MTBF), for example, the null hypothesis is that the true MTBF is at least as great as the desired value (NSV), while the alternate hypothesis is that the true value of the MTBF is less than some lower value (Minimum Acceptable Value). In the case of error rate, the null hypothesis is that the true error rate is less than some very small desired value (NSV), while the alternate hypothesis is that the true error rate is greater than some larger value that is the upper limit for acceptable error (Maximum Acceptable Value).

C.4 Time-based Failure Testing Criteria

The equivalence between a number of events and a time period can be established when the operating scenarios of a system can be determined with precision. Some of the performance test criteria of Volume II, Section 4, use this equivalence.

System acceptance or rejection can be determined by observing the number of relevant failures that occur during equipment operation. The probability ratio for this test is derived from the exponential probability distribution. This distribution implies a constant hazard rate for equipment failure that is not dependent on the time of testing or the previous failures. In that case, two or more systems may be tested simultaneously to accumulate the required number of test hours, and the validity of the data is not affected by the number of operating hours on a particular unit of equipment. However, for environmental operating hardware tests, no unit shall be subjected to less than two complete 24-hour test cycles in a test chamber as required by Volume II, Subsection 4.7.1.

In this case, the null hypothesis is that the Mean Time Between Failure (MTBF), as defined in Volume I, Subsection 4.3.3 is at least as great as some value, here the Nominal Specification Value. The alternate hypothesis is that the MTBF is no better than some value, here the Minimum Acceptable Value.

For example, a typical system operations scenario for environmental operating hardware tests will consist of approximately 45 hours of equipment operation. Broken down, this time allotment involves 30 hours of equipment setup and readiness testing and 15 hours of elections operations. If the Minimum Acceptable Value is defined as 45 hours, and a

~~test discrimination ratio of 3 is used (in order to produce an acceptably short expected time of decision), then the Nominal Specification Value equals 135 hours.~~

~~With a value of decision risk equal to 10 percent, there is no more than a 10 percent chance that a system would be rejected when, in fact, with a true MTBF of at least 135 hours, the system would be acceptable. It also means that there is no more than a 10 percent chance that a system would be accepted with a true MTBF lower than 45 hours when it should have been rejected.~~

~~Therefore,~~

~~H0: MTBF = 135 hours~~
~~H1: MTBF = 45 hours~~

~~a = 0.10~~
~~b = 0.10.~~

~~Under this PRST design, the test is terminated and an ACCEPT decision is reached when the cumulative number of equipment hours in the second column of the following table has been reached, and the number of failures is equal to or less than the number shown in the first column. The test is terminated and a REJECT decision is reached when the number of failures occurs in less than the number of hours specified in the third column. Here, the minimum time to accept (on zero failures) is 169 hours. In the event that no decision has been reached by the times shown in the last table entries, the test is terminated, and the decision is declared as indicated. Any time that 7 or more failures occur, the test is terminated and the equipment rejected. If, after 466 hours of operation, the cumulative failure score is less than 7.0, then the equipment is accepted.~~

~~Number of Failures~~	~~Accept if Time Greater Than~~	~~Reject if Time Less Than~~
~~0~~	~~169~~	~~Continue test~~
~~1~~	~~243~~	~~Continue test~~
~~2~~	~~317~~	~~26~~
~~3~~	~~392~~	~~100~~
~~4~~	~~466~~	~~175~~
~~5~~	~~466~~	~~249~~
~~6~~	~~466~~	~~323~~
~~7~~	~~N/A~~	~~(1)~~

~~(1) Terminate and REJECT~~

~~This test is based on the table of test times of the truncated PRST design V-D in the Military Handbook MIL-HDBK-781A that is designated for discrimination ratio 3 and a nominal value of 0.10 for both a and b. The Handbook states that the true producer risk~~

is 0.111 and the true consumer risk is 0.109. Using the theoretical formulas for either the untruncated or truncated tests will lead to different numbers.

The test design will change if given a different set of parameters. Some jurisdictions may find the Minimum Acceptable Value of 45 hours unacceptable for their needs. In addition, it may be appropriate to use a different discrimination ratio, or different, Consumer's and Producer's risk. Also, before using tests based on the MTBF, it should be determined whether time-based testing is appropriate rather than event-based or another form of testing. If MTBF-based procedures are chosen, then the appropriateness of the assumption of a constant hazard rate with exponential failures should in turn be assessed.

C.5 Accuracy Testing Criteria

Some voting system performance attributes are tested by inducing an event or series of events, and the relative or absolute time intervals between repetitions of the event has no significance. Although equivalence between a number of events and a time period can be established when the operating scenarios of a system can be determined with precision, another type of test is required when such equivalence cannot be established. It uses event-based failure frequencies to arrive at ACCEPT/REJECT criteria. This test may be performed simultaneously with time-based tests.

For example, the failure of a device is usually dependent on the processing volume that it is required to perform. The elapsed time over which a certain number of actuation cycles occur is, under most circumstances, not important. Another example of such an attribute is the frequency of errors in reading, recording, and processing vote data.

The error frequency, called "ballot position error rate," applies to such functions as process of detecting the presence or absence of a voting punch or mark, or to the closure of a switch corresponding to the selection of a candidate.

Certification and acceptance test procedures that accommodate event-based failures are, therefore, based on a discrete, rather than a continuous probability distribution. A Probability Ratio Sequential Test using the binomial distribution is recommended. In the case of ballot position error rate, the calculation for a specific device (and the processing function that relies on that device) is based on:

HO: Desired error rate = 1 in 10,000,000
H1: Maximum acceptable error rate = 1 in 500,000

a = 0.05
b = 0.05

and the minimum error-free sample size to accept for qualification tests is 1,549,703 votes.

~~The nature of the problem may be illustrated by the following example, using the criteria contained in the Guidelines for system error rate. A target for the desired accuracy is established at a very low error rate. A threshold for the worst error rate that can be accepted is then fixed at a somewhat higher error rate. Next, the decision risk is chosen, that is, the risk that the test results may not be a true indicator of either the system's acceptability or unacceptability. The process is as follows:~~

a. ~~The desired accuracy of the voting system, whatever its true error rate (which may be far better), is established as no more than one error in every ten million characters (including the null character)~~
b. ~~If it can be shown that the system's true error rate does not exceed one in every five hundred thousand votes counted, it will be considered acceptable. This is more than accurate enough to declare the winner correctly in almost every election~~
c. ~~A decision risk of 5 percent is chosen, to be 95 percent sure that the test data will not indicate that the system is bad when it is good or good when it is bad~~

~~This results in the following decision criteria:~~

d. ~~If the system makes one error before counting 26,997 consecutive ballot positions correctly, it will be rejected. The vendor is then required to improve the system~~
e. ~~If the system reads at least 1,549,703 consecutive ballot positions correctly, it will be accepted~~
f. ~~If the system correctly reads more than 26,997 ballot positions but less than 1,549,703 when the first error occurs, the testing will have to be continued until another 1,576,701 consecutive ballot positions are counted without error (a total of 3,126,404 with one error)~~