Voting System Standards

This document is part of Agenda Document Number 01-62 on the agenda for consideration at the December 13, 2001, meeting of the Federal Election Commission.

Volume I, Section 9
Table of Contents

9   Overview of Qualification Tests

9.1   Introduction

This section provides an overview of the testing process for qualification testing of voting systems. Qualification testing is the process by which a voting system is shown to comply with the requirements of the Standards and the requirements of its own design and performance specifications. The testing also evaluates the completeness of the vendor's developmental test program, including the sufficiency of vendor tests conducted to demonstrate compliance with stated system design and performance specifications, and the vendor's documented quality assurance and configuration management practices.

Testing is performed by an Independent Test Authority (ITA) that is certified by NASED. The test process described in this section may be conducted by one or more ITAs for a given system, depending on the nature of tests to be conducted and the expertise of the certified ITAs.

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

- ♦ Qualification testing follows the vendor's developmental testing.

- ♦ Qualification testing provides an assurance to state election officials and local jurisdictions of the conformance of a voting system to the Standards as input to state certification of a voting system and acceptance testing by a purchasing jurisdiction.

- ♦ Qualification testing may precede state certification testing, or may be conducted in parallel as established by the certification program of individual states.

Generally a voting system remains qualified as long as no modifications are made to the system that have not been submitted to, and tested by, a certified ITA. The qualification test report remains valid for as long as the voting system remains unchanged. However, if a new threat to a particular voting system is discovered, it is the prerogative of NASED to determine which qualified voting systems are

vulnerable, whether those systems need to be retested, and the specific tests to be conducted.

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

9.2   Testing Scope

The qualification test process is intended to discover errors that, should they occur in actual election use, could result in failure to complete election operations in a satisfactory manner.

Five types of focuses guide the overall qualification testing process:

- ♦ Absolute logical correctness of all ballot processing software, for which no margin for error exists;

- ♦ Operational accuracy in the recording and processing of voting data, as measured by character error rate, for which the maximum acceptable error rate is one in one million characters; (while it would be desirable that there be an error rate of zero, if this had to be proven by a test, the test itself would take an infinity of time);

- ♦ Operational failures or the number of unrecoverable failures under conditions simulating the intended storage, operation, transportation, and maintenance environments for voting systems, using an actual time-based period of processing test ballots;

- ♦ System performance and function under normal and abnormal conditions; and

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

The ITA undertakes sample testing of the vendor's test modules and also designs independent system-level tests to supplement and check those designed by the vendor. The ITA may use automated software testing tools to assist in this process if they are available for the software under examination.

The procedure for disposition of system deficiencies discovered during qualification testing is described in Volume II of the Standards. This procedure recognizes that some but not necessarily all operational malfunctions (apart from software logic defects) may result in rejection. Basically, any defect that results in or may result in the loss or corruption of voting data, whether through failure of system hardware, software or communication, through procedural deficiency, or through deficiencies in security and audit provisions, shall be cause for rejection. Otherwise, malfunctions

that result from failure to comply fully with other requirements of this standard will not in every case warrant rejection. Specific failure definition and scoring criteria are also contained in Volume II.

9.2.1   Test Categories

The qualification test procedure is presented in several parts:

- ♦ Hardware qualification tests,

- ♦ Software qualification tests,

- ♦ Communication qualification tests,

- ♦ Security tests,

- ♦ Documentation tests,

- ♦ System-level tests, including audits,

- ♦ Reviews of documented vendor practices for quality assurance, and

- ♦ Reviews of documented vendor practices for configuration management

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

The qualification test procedures are presented in these categories because test authorities frequently focus separately on each. The following subsections provide information that test authorities need to conduct testing.

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

9.2.1.1   Focus of Hardware Tests

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

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

The operating tests involve running the system for an extended period of time under varying temperatures and voltages. This period of operation ensures with confidence that the hardware meets or exceeds the minimum requirements for reliability, data reading, and processing accuracy contained in Section 3. The procedure emphasizes equipment operability and data accuracy; it is not an exhaustive evaluation of all system functions. Moreover, the severity of the test conditions has, in most cases, been reduced from that specified in the Military Standards to reflect commercial and industrial, rather than military and aerospace, practice.

9.2.1.2   Focus of Software Evaluation

The software qualification tests encompass a number of interrelated examinations. The primary objective is to examine selectively in-depth all ballot processing source code for absolute logical correctness, for its modularity and overall construction, and for conformance with the documentation provided by the vendor. Part of this code examination will be focused on the assessment of potential hidden code. The code inspection will be followed by a series of functional tests to verify the proper performance of all system functions controlled by the software.

9.2.1.3   Focus of Telecommunications Tests

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

For voting systems that use telecommunications lines or networks that are not under the control of the vendor (e.g., public telephone networks), the ITA will test the interface of vendor-supplied components with these external components for effective interface, vote transmission, failure detection, and failure recovery.

9.2.1.4   Focus of Security Tests

The security qualification tests focus on the ability of the system to detect, prevent, log, and recover from a broad range of security risks as identified in Section 6. The range of risks tested is determined by the design of the system and potential exposure to risk. Regardless of system design and risk profile, all systems are tested for effective access control and physical data security.

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

9.2.1.5   Focus of Integration Tests

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

The PCA compares the voting system components submitted for qualification to the vendor's technical documentation and confirms that the documentation submitted meets the requirements of the Standards. As part of the PCA, the ITA also witnesses the building of the executable system to ensure that the qualified executable release is built from the tested components.

The FCA is an exhaustive verification of every system function and combination of functions cited in the vendors' documentation. Through use, the FCA verifies the accuracy and completeness of the system's Voter Manual, Operations Procedures, Maintenance Procedures, and Diagnostic Testing Procedures.

9.2.1.6   Focus of Useability/Accessibility Tests

The interface between the voting system and its users, both voters and election officials, is a key element of effective system operation and confidence in the system. At this time, general standards for the useability of voting systems by the average voter and election officials have not been defined, but are planned to be addressed in the next update of the Standards. However, standards for useability by individual voters with disabilities have been defined in Section 2 based on Section 508 of the Rehabilitation Act Amendments of 1998. Voting systems are tested to ensure that a voting device is included in the system and its design and operation conforms with these standards.

9.2.1.7   Tests of Ballot Counting Accuracy

The various options of software counting logic shall be tested during the system-level 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. For example, multiple test decks for variations in straight party and cross party endorsement will be created and processed by the ITA

9.2.1.8   Sequence of Tests and Audits

There is no required sequence for performing the system qualification tests and audits. For a new system, not previously qualified, a test using the generic test ballot decks might be performed before undertaking any of the more lengthy and expensive tests or documentation review. The test agency or vendor may, however, schedule the PCA, FCA, or other tests in any convenient order, provided that the prerequisite conditions for each test have been met before it is initiated.

9.2.2   Test System

Vendors shall submit for testing the specific system that is to be offered to jurisdictions, including:

a.   The hardware submitted for qualification testing shall be equivalent, in form and function, to the actual production versions of the hardware units.

b.   The software submitted for qualification testing shall be the exact software that will be used in production units.

c. Engineering or developmental prototypes are not acceptable, unless the vendor can show that the equipment to be tested is equivalent to standard production units in both performance and construction.

d. Benchmark directory listings shall be submitted for all software/firmware elements (and associated documentation) included in the vendor's release as they would normally be installed upon setup and installation.

9.3   Applicability

9.3.1   General Applicability

Voting system hardware, software, communications and documentation are examined and tested to determine suitability for elections use. Examination and testing addresses the broad range of system functionality and components, including system functionality for pre-voting, voting, and post-voting functions described in Section 2. All products custom designed for election use shall be tested in accordance with the applicable procedures contained in this section. COTS hardware, system software and communications components with proven performance in commercial applications other than elections, however, are exempted from certain portions of the test as long as such products are not modified for use in a voting system. Compatibility of these products all other components of the voting system shall be determined through functional tests integrating these products with the remainder of the system.

9.3.1.1   Exclusions

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

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

b. Production models of special purpose information technology equipment that have a documented history of successful performance under conditions equivalent to election use for relevant requirements of the standards and that

have demonstrated compatibility with the voting system components with which they interface; and

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

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

9.3.1.2 Software

Software qualification is applicable to the following:

    a.   Application programs that control and carry out ballot processing, commencing with the definition of a ballot and voting image, and including processing of the image (either from physical ballots or electronically activated images), and ending with the system's access to memory for the generation of output reports.

    b.   Specialized compilers and specialized operating systems associated with ballot processing.

    c.   Standard compilers and operating systems that have been modified for use in the vote counting process.

Ballot layout, vote recording, vote tabulation, and audit trail shall be subjected to selectively in-depth code inspection. If a DRE voting system incorporates independent processing paths, each path or module shall be examined. Functional testing of all these programs during software evaluation and system-level testing shall exercise any specially tailored software off-line from the ballot counting process (e.g.; software for preparing ballots and broadcasting results).

9.3.2 Modifications to Qualified Systems

9.3.2.1   General Requirements for Modifications

Changes introduced after the system has completed qualification will necessitate further review. The ITA will determine tests necessary for re-qualification based on a review of the nature and scope of changes, and other submitted information including the system documentation, vendor test documentation, configuration management records, and quality assurance information. Based on this review, the ITA may:

a. Determine that a review of all change documentation against the baseline materials is sufficient for recommendation for qualification, or

b. Determine that all changes must be retested against the previously qualified version (this will include review of changes to source code, review of all updates to the TDP, and a performance of functional tests), or

c. Determine that the scope of the changes is substantial and will require a complete retest of the hardware, software, and/or telecommunications.

9.3.2.2   Potential for Limited Testing of Modifications

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

a. The change does not affect demonstrated compliance with the Standards for:

   1) Performance of voting system functions;

   2) Voting system security and privacy;

   3) Overall flow of system control; and

   4) Manner in which ballots are defined and interpreted, or voting data are processed..

b. The change also falls into one or more of the following classifications:

   1) It is made for the purpose of correcting a defect, and test documentation and configuration management records are provided that verify that the installation of the altered hardware or corrected code results solely in the elimination of the defect;

   2) It is made solely for the purpose of providing additional audit or report generating capability, using existing audit and reporting subroutines;

   3) It is made for the purpose of enabling interaction with other equipment (general purpose or approved), or with other computer programs and databases. Procedural and test documentation and configuration management records must be provided to verify that such interaction does not involve or adversely affect vote counting and data storage; and

4) It is made for the purpose of permitting operation on a different processor or of using additional or different peripheral devices, and does not alter the software's structure and function in any manner.

These exceptions are intended to facilitate the correction of defects, the incorporation of improvements, the enhancement of portability and flexibility, and the integration of vote-counting software with other systems and elections software.

9.3.2.3   Utility Software and/Device Handlers

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

9.4   Documentation Submitted by Vendor

The vendor shall submit to the ITA documentation necessary for the identification of the full system configuration submitted for evaluation and for the development of an appropriate test plan by the ITA for system qualification testing.

One element of the documentation is the Technical Data Package (TDP). The TDP contains information that that defines the voting system design, method of operation, and related resources. It contains:

a. System overview;

b. System functionality description;

c. System hardware specification;

d. System design and software specifications;

e. System security specifications;

f. System test and verification specification

g. System operations procedures;

h. System maintenance procedures;

i. Personnel deployment and training requirements;

j. Configuration management plan; and

k. Quality assurance program; and

l. System Change Notes.

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

A second category of documentation is the vendor's documented practices for quality assurance and configuration management. This documentation is used by the ITA in constructing the qualification testing plan and is particularly important in constructing plans for the re-testing of systems that have been qualified previously. Re-testing of systems submitted by vendors that consistently adhere to particularly strong and well documented quality assurance and configuration management practices will generally be more efficient than for systems developed and maintained using less rigorous or less well documented practices. Volume II provides a detailed description of the documentation required for the vendor's quality assurance and configuration management practices used for the system submitted for qualification testing.

9.5   Qualification Test Process

The qualification test process may be performed by one or more ITAs that together perform the full scope of tests required by the Standards. Where multiple ITAs are involved, testing shall be conducted first for the voting system hardware, firmware, and related documentation; then for the system software and communications; and finally for the integrated system as a whole. Voting system hardware and firmware testing may be performed by one ITA independently of the other testing performed by other ITAs. Testing may be coordinated across ITAs so that hardware/firmware tested by one ITA can be used in the overall system tests performed by another ITA.

Whether one or more ITAs are used, the testing generally consists of three phases: Pre-test Activities, Qualification Testing, and Qualification Report Issuance and Post-test Activities.

9.5.1   Pre-test Activities

9.5.1.1   Initiation of Testing

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

    a. Request the performance of qualification testing from among the certified
        ITAs,

b. Enter into formal agreement with the ITAs for the performance of testing, and

c. Prepare and submit materials required for testing consistent with the requirements of the Standards.

Qualification testing shall be conducted for the initial version of a voting system as well as for all subsequent changes to the system prior to release for sale or for installation. As described in Section 9.3.2 the nature and scope of testing for system changes or new versions shall be determined by the ITA based on the nature and scope of the modifications to the system and on the quality of system documentation and configuration management records submitted by the vendor.

9.5.1.2   Pre-test Preparation

Pre-test preparation encompasses the following activities:

a. The vendor shall prepare and submit a complete TDP to the ITA. The TDP should consist of the items listed in Section 9.4 and specified in greater detail in Standards Volume II.

b. The ITA shall perform an initial review of the TDP for completeness and clarity and request additional information as required.

c. The vendor shall provide additional information, if requested by the ITA.

d. The vendor and ITA shall enter into an agreement for the testing to be performed by the ITAs in exchange for payment by the vendor.

e. The vendor shall deliver to the ITA all hardware and software needed to perform testing.

9.5.2   Qualification Testing

Qualification testing encompasses the activities described below:

9.5.2.1   Qualification Test Plan

The ITA shall prepare a Qualification Test Plan to define all tests and procedures required to demonstrate compliance with Standards, including:

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

b. Establishing the test environment or the special environment required to perform the test;

c. Initiating and completing operating modes or conditions necessary to evaluate the specific performance characteristic under test;

d. Measuring and recording the value or range of values for the characteristic to be tested, demonstrating expected performance levels;

e. Verifying, as above, that the equipment is still in normal condition and status after all required measurements have been obtained;

f. Confirming that documentation submitted by the vendor corresponds to the actual configuration and operation of the system; and

g. Confirming that documented vendor practices for quality assurance and configuration management comply with the Standards.

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

9.5.2.2   Qualification Test Practices

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

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

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

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

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

e. Any and all failures that occurred as a result of a deficiency shall be classified as purged, and test results shall be evaluated as though the failure or failures had not occurred, if:

1) the vendor submits a design, manufacturing, or packaging change notice to correct the deficiency, together with test data to verify the adequacy of the change,

2) the examiner of the equipment agrees that the proposed change will correct the deficiency, and

3) the vendor certifies that the change will be incorporated into all existing and future production units.

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

9.5.2.3   Qualification Test Conditions

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

a. Preparations for testing, arrangement of equipment, verification of equipment status, and the execution of procedures shall be witnessed by at least one independent, qualified observer, who shall certify that all test and data acquisition requirements have been satisfied.

b. When a test is to be performed at "standard" or "ambient" conditions, this requirement shall refer to a nominal laboratory or office environment, with a temperature in the range of 68 to 75 degrees Fahrenheit, and prevailing atmospheric pressure and relative humidity.

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

1) Temperature   +/- 4 degrees F

2) Electrical supply voltage   +/- 2 vac

9.5.2.4   Qualification Test Data Requirements

The following qualification test data practices shall be employed:

♦   A test log of the procedure shall be maintained. This log shall identify the system and equipment by model and serial number.

♦   Test environment conditions shall be noted.

♦   All operating steps, the identity and quantity of simulated ballots, annotations of output reports, the elapsed time for each procedure step, and observations of equipment performance and, in the case of non-operating hardware tests, the condition of the equipment shall be recorded.

9.5.2.5   Qualification Test Fixtures

ITAs may use test fixtures or ancillary devices to facilitate qualification testing. These fixtures and devices may include arrangements for automating the operation of voting devices and the acquisition of test data.

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

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

   c. If the vendor provides a means of simulating the casting of ballots, the simulation device is subject to the same performance, reliability, and quality requirements that apply to the voting device itself.

9.5.2.6   Witness of System Build and Installation

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

9.5.3   Qualification Report Issuance and Post-test Activities

Qualification report issuance and post-test activities encompass the activities described below:

   a. The ITA may issue interim reports to the vendor, informing the vendor of the testing status, findings to date, and other information. Such reports do not constitute official test reports for voting system qualification.

   b. The ITA shall prepare a Qualification Test Report that confirms the voting has passed the testing conducted by the ITA. The ITA shall include in the

Qualification Test Report the date testing was completed, the specific system version addressed by the report, the version numbers of all system elements separately identified with a version number by the vendor, and the scope of tests conducted. A recommended outline for the test report is contained in Volume II.

c. Where a system is tested by multiple ITAs, each ITA shall prepare a Qualification Test Report.

d. The ITA shall deliver the Qualification Test Report to the vendor and to NASED.

e. NASED shall issue a single Qualification Number for the system to the vendor and to the ITAs. The issuance of a Qualification Number indicates that the system has been tested by certified ITAs for compliance with the national test standards and qualifies for the certification process of states that have adopted the national standards.

f. This number applies to the system as a whole only for the versions of the system elements tested by the ITAs and identified in the Qualification Test Reports.

g. The Qualification Number is intended for use by the states and their jurisdictions to support state and jurisdiction processes concerning voting systems. States and their jurisdictions shall request ITA Qualification Test Reports based on the Qualification Number as part of their voting system certification and procurement processes systems that rely on the Standards.