# Volume II, Section 6
# Table of Contents


**6 System Level Integration Testing ..... 6-1**

6.1 Scope ..... 6-1

6.2 Basis of Integration Testing ..... 6-1

6.2.1 Testing Breadth ..... 6-2

6.2.2 System Baseline for Testing ..... 6-2

6.2.3 Testing Volume ..... 6-3

6.3 Testing Interfaces of System Components ..... 6-3

6.4 Security Testing ..... 6-3

6.4.1 Access Control ..... 6-4

6.4.2 Data Interception and Disruption ..... 6-5

6.5 Accessibility Testing ..... 6-6

6.6 Physical Configuration Audit ..... 6-6

6.7 Functional Configuration Audit ..... 6-7

# 6 System Level Integration Testing

## 6.1 Scope

This section contains a description of the testing to be performed by the ITAs to confirm the proper functioning of the fully integrated components of a voting system submitted for qualification 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 qualification tests address the integrated operation of both hardware and software, along with any telecommunications capabilities. The system-level qualification tests shall include the tests (functionality, volume, stress, usability, security, performance, and recovery) indicated in the ITAs' Qualification 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

ITAs 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, 5, 6 and 8.

These procedures shall also address the requirements for testing system functionality provided in Volume II, Section 3. Where practical, the ITA 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 vendor. The ITA 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; or

c. Both of the above.

The specific procedures to be used shall be identified in the Qualification Test Plan prepared by the ITA. These procedures may replicate testing performed by the vendor and documented in the vendor's TDP, but shall not rely on vendor testing as a substitute for testing performed by the ITA.

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

### 6.2.2 System Baseline for Testing

The system level qualification tests are conducted using the version of the system as it is intended to be sold by the vendor and delivered to jurisdictions. To ensure that the system version tested is the correct version, the ITA 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 qualification testing process, the ITA shall require the vendor conduct a new "build" of the system to ensure that the qualified 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 ITA shall design and perform test procedures that test the interfaces of all system modules and subsystems with each other against the vendor's specifications. These tests shall be documented in the ITA's Qualification Test Plan, and shall include the full range of system functionality provided by the vendor's specifications, including functionality that exceeds the specific requirements of the Standards.

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

a. Confirm that the version of previously approved components and subsystems are unchanged; and

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 vendor shall provide a public data specification of files or data objects used to exchange information.

Some systems use telecommunications capabilities as defined in Section 5. For those systems that do use such capabilities, components that are located at the poll site or separate vote counting site 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 vendor (e.g., public telephone networks), the ITA shall test the interface of vendor-supplied components with these external components for effective interface, vote transmission, failure detection, and failure recovery.

## 6.4 Security Testing

The ITA shall design and perform test procedures that test the security capabilities of the voting system against the requirements defined in Volume I, Section 6. These

procedures shall 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 and system capabilities and safeguards, claimed by the vendor in its TDP that go beyond the risks and threats identified in Volume I, 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 or official election results (such as ballots or tabulated results), the ITAs 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 qualification.

The ITA may meet these testing requirements by confirming proper implementation of proven commercial security software. In this case, the vendor must provide the published standards and methods used by the US 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 ITA may conduct or simulate attacks on the system to confirm the effectiveness of the system's security capabilities, employing test procedures approved by the NASED Voting Systems Board.

### 6.4.1 Access Control

The ITA shall conduct tests of system capabilities and review the access control policies and procedures and submitted by the vendor 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 ITA shall design tests to confirm that these security elements work as specified.

Specific activities to be conducted by the ITA shall include:

a. A review of the vendor’s access control policies, procedures and system capabilities to confirm that all requirements of Volume I, Section 6.2 have been addressed completely; and

b. Specific tests designed by the ITA to verify the correct operation of all documented access control procedures and capabilities, including tests

designed to circumvent controls provided by the vendor. These tests shall include:

1) Performing the activities that the jurisdiction will perform in specific accordance with the vendor's access control policy and procedures to create a secure system, including procedures for software (including firmware) installation (as described in Volume I, Section 6.4); and

2) 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 ITA shall review, and conduct tests of, the data interception and prevention safeguards specified by the vendor in its TDP. The ITA shall evaluate safeguards provided by the vendor 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 ITA shall also review the vendor'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; and

f. Confirmation of proper installation of new system releases.

## 6.5 Accessibility Testing

The ITA shall design and perform procedures that test the capability of the voting system to assist voters with disabilities. ITA test procedures shall confirm that:

a. Voting machines intended for use by voters with disabilities provide the capabilities required by Volume I, Section 2.2.7;

b. Voting machines intended for use by voters with disabilities operate consistent with vendor specifications and documentation; and

c. Voting machines intended for use by voters with disabilities meet all other functional requirements required by Volume I, Section2.

## 6.6 Physical Configuration Audit

The Physical Configuration Audit compares the voting system components submitted for qualification to the vendor'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 vendor'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 vendor's source code against the submitted documentation during the Physical Configuration Audit to verify that the software conforms to the vendor's specifications. This review shall include an inspection of all records of the vendor's release control system. If changes have been made to the baseline version, the test agency shall verify that the vendor's engineering and test data are for the software version submitted for qualification;

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, vendor documents containing this information shall be reviewed against the system's functional specifications. Any discrepancy or inadequacy in the vendor's plan or data shall be resolved prior to beginning the system-level functional and performance tests; and

e. All subsequent changes to the baseline software configuration made during the course of qualification testing shall be subject to reexamination. All changes to the system hardware that may produce a change in software operation shall also be subject to reexamination.

The vendor shall provide a list of all documentation and data to be audited, cross-referenced to the contents of the TDP. Vendor 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 vendor tests, and the conduct of additional tests, to verify that the system hardware and software perform all the functions described in the vendor'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 test agency shall review the vendor's test procedures and test results to determine if the vendor's specified functional requirements have been adequately tested. This examination shall include an assessment of the adequacy of the vendor's test cases and input data to exercise all system functions, and to detect program logic and data processing errors, if such be present; and

b. The test agency 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 vendor's test data reports. If vendor developmental test data is incomplete, the ITA shall design and conduct all appropriate module and integrated functional tests. The functional configuration audit may be performed in the facility either of the test agency or of the vendor, and shall use and verify the accuracy and completeness of the System Operations, Maintenance, and Diagnostic Testing Manuals.

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