# 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 II, Section 2
# Table of Contents

# 2 Technical Data Package

## 2.1 Introduction

This section contains a description of vendor documentation relating to the voting system that shall be submitted with the system as a precondition of qualification testing. These items are necessary to define the product and its method of operation; to provide vendor technical and test data supporting the vendor's claims of the system's functional capabilities and performance levels; and to document instructions and procedures governing system operation and field maintenance. Other items relevant to the system evaluation shall be submitted along with this documentation (such as disks, tapes, source code, object code, and sample output report formats).

Both formal documentation and notes of the vendor's system development process shall be submitted for qualification tests. Documentation outlining system development permits assessment of the vendor's systematic efforts to test the system and correct defects. Inspection of this process also enables the design of a more precise qualification test plan. If the vendor's developmental test data is incomplete, the test agency shall design and conduct the appropriate tests.

### 2.1.1 Content and Format

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

- Overall system design, including subsystems, modules and the interfaces among them;
- Specific functional capabilities provided;

- Performance and design specifications;
- Design constraints, applicable standards, and compatibility requirements;
- Personnel, equipment, and facility requirements for system operation, maintenance, and logistical support;
- Vendor practices for assuring system quality during the system's development and subsequent maintenance; and
- Vendor practices for managing the configuration of the system during development and for modifications to the system throughout its life cycle.

The vendor shall list all documents 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 Qualification

At a 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; and
k. Quality assurance program; and
l. System change notes.

Systems in existence at the time the revised standards are promulgated may not have all required developmental documentation. When they are subject to evaluation as a result of system modification, vendors shall provide what information they can.

Vendors may also submit other information relevant to the evaluation of the system, such as documentation of tests performed by other independent test authorities and records of the system's performance history, if any.

#### 2.1.1.2 Required Content for System Changes and Re-qualification

For systems seeking re-qualification, vendors shall submit System Change Notes as described in Section 2.11, as well as current versions of all documents that have been updated to reflect system changes.

#### 2.1.1.3 Format

The formats presented are general in nature; specific format details are of the vendor's choosing. Other items submitted by the vendor, such as documentation of tests conducted by other test authorities, performance history, failure analysis, and corrective action may be provided in a format of the vendor's choosing.

The TDP shall include a detailed table of contents for the required documents, an abstract of each document and listing each of the informational sections and appendices presented within each. A cross-index shall be provided indicating the portions of the documents that are responsive to documentation requirements for any item presented using the vendor's format.

### 2.1.2 Other Uses for Documentation

Although all of this documentation is required for qualification testing, some of these same items shall also be required during the state certification process and, possibly, local level acceptance testing. 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 vendor shall identify all documents, or portions of documents, containing proprietary information not approved for public release. Any person or test agency receiving these documents shall agree to use the information contained therein solely for the purpose of analyzing and testing the system, and shall refrain from otherwise using the proprietary information or disclosing it to any other person or agency without the prior written consent of the vendor.

## 2.2 System Overview

In the system overview, the vendor shall provide information that enables the test authority identify the functional and physical components of the system, how they are structured, and the interfaces between them.

### 2.2.1 System Description

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

a. A description of the functional components (or subsystems) as defined by the vendor (e.g., environment, election management and control, vote recording, vote conversion, reporting, and their interconnection);

b. A description of the operational environment of the system that provides an overview of the hardware, software and communications structure;

c. A theory of operation 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, vendor and version used for each such component, including:

    1) Operating systems;

2) Database software;

3) Communications routers;

4) Modem drivers; and

5) 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 identification of:

1) file specifications, data objects, or other means used for information exchange; and

2) 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 vendor's release as they would normally be installed upon setup and installation.

## 2.2.2 System Performance

The vendor shall provide system performance information that includes:

the expected values and acceptable ranges of performance attributes for each.

The vendor shall provide descriptions of the following:

a. For all operating modes and functions, their performance characteristics in terms of expected and maximum speed, throughput capacity, maximum volume, and processing frequency;

b. Quality attributes such as reliability, maintainability, availability, usability, and portability;

c. Provisions for safety, security, privacy, and continuity of operation; and

d. Design constraints, applicable standards, and compatibility requirements.

## 2.3 System Functionality Description

The vendor shall declare the scope of the system's functional capabilities, thereby establishing the performance, design, test, manufacture, and acceptance context for the system

The vendor shall provide a listing of the system's functional processing capabilities, encompassing capabilities required by the Standards and any additional capabilities provided by the system. This listing shall provide a simple description of each capability. Detailed specifications shall be provided in other documentation required for the TDP as indicated by the standards for that documentation.

a. The vendor 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 of the Standards. The contents of Volume I Section 2 may be used as the basis for a checklist whereby the vendor indicates 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 vendor'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 vendor shall expand on the system osverview by providing detailed specifications of the hardware components of the system,

including hardware used to support the telecommunications capabilities of the system, if applicable.

### 2.4.1 System Hardware Characteristics

The vendor shall provide a detailed discussion of the characteristics of the system, indicating how the hardware meets individual requirements defined in Volume I, Sections 3, 4, 5 and 6 of the Standards including:

a. **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;

b. **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;

c. **Reliability:** This discussion addresses system and component reliability stated in terms of the systems operating functions, and identification of items that require special handling or operation to sustain system reliability;

d. **Maintainability:** This discussion addresses maintainability attributes of the system, including the Mean Time to Repair, the Maximum Time to Repair at the 95the Percentile (the maximum time required for replacement or repair of 95 percent of the failures expected to occur in a given operating period), and any maintenance task requiring special training, tools, or equipment; and

e. **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 of system.

### 2.4.2 Design and Construction

The vendor shall provide sufficient data (or references to data) to identify unequivocally the details of the system configuration submitted for qualification testing. The vendor shall provide a list of materials and components used in the system, standards used for their selection, 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. The system's susceptibility to threats that may be present in its operating environment, including:

   1) Temperature variation;

   2) Electrical power disturbance;

   3) Electromagnetic radiation;

   4) Electrostatic disruption;

   5) Electrical fast transient

   6) Lightening surge;

   7) Conducted RF; and

   8) Magnetic fields.

d. Operator and voter safety considerations, and any constraints on system operations or the use environment;

e. Human engineering considerations, including provisions for access by handicapped voters.

## 2.5 Software Design and Specification

The vendor 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 vendor 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 vendor 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 vendor 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:

   1) Written in-house;

   2) Procured and not modified;

   3) Procured and modified including descriptions of the modifications;

d. Additional information for each item that includes:

   1) Item identification;

   2) General description;

   3) Software requirements performed by the item;

   4) Identification of interfaces with other items provide data to, or receive data from, the item; and

5) Concept of execution for the item;

The vendor shall also include a certification that procured software items were obtained directly from the manufacturer.

## 2.5.4 Software Standards and Conventions

The vendor shall provide information that can be used an ITA or state certification board to support software analysis and test design. The information shall address standards and conventions developed internally by the vendor as well as published industry standards that have been applied by the vendor. The vendor shall provide information that addresses the following standards and conventions:

a. System development methodology;

b. Software design standards, including internal vendor procedures;

c. Software specification standards, including internal vendor procedures;

d. Software coding standards, including internal vendor procedures;

e. Software testing and verification standards, including internal vendor 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 by the ITA to examine and test the software. These documents include standards for program flow and control charts, program documentation, test planning, and for 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 vendor 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; and

f. Operator controls, indicators, and displays.

#### 2.5.5.2 Software Environment

The vendor shall identify the compilers or assemblers used in the generation of executable code, and describe the operating system or system monitor. The vendor shall also provide an overview of the compile-time interaction of the voting system software with library calls and linking.

### 2.5.6 Software Functional Specification

The vendor 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 vendor 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 vendor 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; and

c. A definition of the outputs produced (again, with characteristics, tolerances, or acceptable ranges as applicable).

#### 2.5.6.2 Software Functions

The vendor 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; and

g. Security monitoring and control.

### 2.5.7 Programming Specifications

The vendor 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, HIPOs, 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. All modules or module interfaces that are potentially vulnerable to degradation in data quality or security penetration shall be identified

### 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 vendor 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 to be 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 (DBMS) for defining forms and reports, on-line DBMS queries for database access and manipulation, input to a graphical user interface (GUI) 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. (Section 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:

    1) Conditions in effect within the software module or unit when its execution is initiated

    2) Conditions under which control is passed to other software modules or units

    3) Response and response time to each input, including data conversion, renaming, and data transfer operations

    4) Sequence of operations and dynamically controlled sequencing during the software module's or unit's operation, including:

i) The method for sequence control

ii) The logic and input conditions of that method, such as timing variations, priority assignments

iii) Data transfer in and out of memory

iv) The sensing of discrete input signals, and timing relationships between interrupt operations within the software module or unit

5) Exception and error handling.

g. If the software module is a database, provide the information described in Volume II, Section 2.5.10.

## 2.5.8 System Database

The vendor 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 data base 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 references) needed to understand the design:

c. Identification and description of all database entities and how they are implemented physically (e.g., tables, files, etc.);

d. Entity relationship diagram and description of relationships; and

e. Details of table, record or file contents (as applicable) to include individual data elements and their specifications, including:

1) Names/identifiers;

2) Data type (alphanumeric, integer, etc.);

3) Size and format (such as length and punctuation of a character string);

4) Units of measurement (such as meters, dollars, nanoseconds);

5) Range or enumeration of possible values (such as 0-99);

6) Accuracy (how correct) and precision (number of significant digits);

7) Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether business rules apply;

8) Security and privacy constraints; and

9) 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 vendor 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 vendor shall provide:

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; and

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 vendor shall provide information that describes:

a. Type of interface (such as real-time data transfer, storage-and-retrieval of data, etc.) to be implemented

b. Characteristics of individual data elements that the interfacing entity(ies) will provide, store, send, access, receive, etc., such as:

1) Names/identifiers;

2) Data type (alphanumeric, integer, etc.);

3) Size and format (such as length and punctuation of a character string);

4) Units of measurement (such as meters, dollars, nanoseconds);

5) Range or enumeration of possible values (such as 0-99);

6) Accuracy (how correct) and precision (number of significant digits);

7) Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether business rules apply;

8) Security and privacy constraints; and

9) 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:

1) Communication links/bands/frequencies/media and their characteristics;

2) Message formatting;

3) Flow control (such as sequence numbering and buffer allocation);

4) Data transfer rate, whether periodic/aperiodic, and interval between transfers;

5) Routing, addressing, and naming conventions;

6) Transmission services, including priority and grade; and

7) 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:

1) Priority/layer of the protocol;

2) Packeting, including fragmentation and reassembly, routing, and addressing;

3) Packeting, including fragmentation and reassembly, routing, and addressing;

4) Legality checks, error control, and recovery procedures;

5) Synchronization, including connection establishment, maintenance, termination; and

6) Status, identification, and any other reporting features;

e. Other characteristics, such as physical compatibility of the interfacing entity(ies) (dimensions, tolerances, loads, voltages, plug compatibility, etc.)

## 2.5.10 Appendices

The vendor 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 vendor. Topics recommended for amplification or treatment in appendix form include:

a. **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;

b. **References:** A list of references to all related vendor documents, data, standards, and technical sources used in software development and testing; and

c. **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 6 of the Standards. 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 5, the means used to keep the security capabilities of the system current to respond to the evolving threats against these systems.

Information provided by the vendor in this section of the TDP may be duplicative of information required by other sections. Vendors may cross reference to information provided in other sections provided that the means used provides a clear mapping to the requirements of this section.

Information submitted by the vendor shall be used by the test authority to assist in developing and executing the system qualification test plan. The Security Specification shall contain the sections identified below

### 2.6.1 Penetration Analysis

The vendor shall provide a detailed description of the penetration analysis undertaken to preclude intrusion by unauthorized persons and fraudulent manipulation of elections data to meet the specific requirements of Volume I, Section 6.2.1 of the Standards.

Such penetration analysis will be subject to strict confidentiality and non-disclosure by the test authority. For security reasons, the penetration analysis shall not be routinely distributed to the jurisdictions that program elections.

### 2.6.2 Access Control Policy

The vendor shall specify the features and capabilities of the access control policy recommended to purchasing jurisdictions to provide effective voting system security to meet the specific requirements of

Volume I, Section 6.2.2 of the Standards. The access control policy shall address the general features and capabilities and individual access privileges indicated in Volume I, Section 6.2.2.

### 2.6.3 Access Control Measures

The vendor 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, Section 6.2.3 of the Standards.

The vendor also shall define and provide a detailed description of the methods used to preclude unauthorized access to the access control capabilities of the system itself.

### 2.6.4 Equipment and Data Security

The vendor 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, Section 6.3 of the Standards. This information shall address measures for polling place security and central count location security.

### 2.6.5 Software Installation

The vendor 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, Section 6.4 of the Standards. This information shall address software installation for all system components.

## 2.6.6 Telecommunications and Data Transmission Security

The vendor 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, Section 6.5 of the Standards.

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 5, this information shall also include:

   1) Capabilities used to provide protection against threats to third party products and services;

   2) Policies and processes used by the vendor to ensure that such protection is updated to remain effective over time;

   3) Policies and procedures used by the vendor to ensure that current versions of such capabilities are distributed to user jurisdictions and are installed effectively by the jurisdiction;

   4) 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;

   5) 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; and

   6) 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.

## 2.6.7 Other Elements of an Effective Security Program

The vendor 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; and

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 vendor shall provide two types of test and verification specifications:

a. Development test specifications; and

b. Qualification test specifications.

### 2.7.1 Development Test Specifications

The vendor 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:

   1) Test structure

   2) Test sequence or progression

   3) Test conditions

a. Standard test procedures, including any assumptions or constraints;

b. Special purpose test procedures including any assumptions or constraints;

c. Test data; including the data source, whether it is real or simulated, and how test data is controlled; and

d. Expected test results.

e. Criteria for evaluating test results;

Additional details for these requirements are provided by MIL-STD-498, Software Test Plan (STP) and Software Test Description (STD).

In the event that test data is not available, the ITA shall design test cases and procedures equivalent to those ordinarily used during product verification.

### 2.7.2 Qualification Test Specifications

The vendor 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; and

h. Production of audit trails and statistical data.

The specifications shall identify procedures for assessing and demonstrating the suitability of the software for elections 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 Section 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, including the sections listed below:

## 2.8.1 Introduction

The vendor 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 vendor shall also list all reference and supporting documents pertaining to the use of the system during elections operations.

## 2.8.2 Operational Environment

The vendor shall describe the system environment, and the interface between the user or operator and the system. The vendor 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; and

c. Other locations.

## 2.8.3 System Installation and Test Specification

The vendor 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 Section 2.3 above, including:

a. Pre-voting functions;

b. Voting functions;

c. Post-voting functions; and

d. General capabilities.

These specifications also serve to provide guidance to the procuring agency in developing its acceptance test plan and procedure according to the agency's contract provisions, and the election laws of the state.

### 2.8.4 Operational Features

The vendor shall provide documentation of system operating features that meets the following requirements:

a. Provides a detailed description of all input, output, control, and display features accessible to the operator or voter;

b. Provide examples of simulated interactions in order to facilitate understanding of the system and its capabilities;

c. Provide sample data formats and output reports; and

d. Illustrate and describe all status indicators and information messages.

### 2.8.5 Operating Procedures

The vendor 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 the 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. Define and illustrate procedures to enable and control the external interface to the system operating environment if supporting hardware and software are involved (such information shall be provided for the interaction of the system with other data processing systems or data interchange protocols as well);

f. Provide 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. To support successful ballot and program installation and control by election officials, provide 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 and

h. To support diagnostic testing, specify diagnostic tests that may be employed to identify problems in the system, verify the correction of maintenance problems; and isolate and diagnose faults from various systems states.

### 2.8.6 Operations Support

The vendor 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 vendor documentation provided to the ITA and to system users); and

b. Describe 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 vendor 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 vendor. Topics recommended for discussion include:

a. **Glossary:** A listing and brief definition of all terms that may be unfamiliar to persons not trained in either voting systems or computer operations;

b. **References:** A list of references to all vendor documents and to other sources related to operation of the system; and

c. **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.

d. **Manufacturer's Recommended Security Procedures:** This appendix shall contain all security procedures that are to be executed by the system operator.

## 2.9 System Maintenance Procedures

The system maintenance procedures shall provide information in sufficient detail to support election workers, data 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 vendor 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 theory of operation 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 are 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; and

h. How test and diagnostic information is acquired and used.

## 2.9.2 Maintenance Procedures

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

### 2.9.2.1 Preventive Maintenance Procedures

The vendor 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; and

d. Any maintenance tasks that must be coordinated with the vendor 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 vendor shall provide fault detection, fault isolation, correction procedures, and logic diagrams for all operational abnormalities identified by design analysis and operating experience.

The vendor 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; and

f. Any coordination required with the vendor, or other party for off the shelf items.

### 2.9.3 Maintenance Equipment

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

### 2.9.4 Parts and Materials

Vendors 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 vendor 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; and

f. Sources from which they may be obtained.

### 2.9.4.2 Paper-Based Systems

For marking devices manufactured by multiple external sources, the vendor shall provide a listing of sources and model numbers that are compatible with the system.

For paper-based voting systems that process ballots using general purpose readers, the vendor shall specify the card or paper stock, punch or mark configurations, and punch or mark field locations complying with industry standards cited by the vendor for information technology supplies and equipment

## 2.9.5 Maintenance Facilities and Support

The vendor shall identify all facilities, furnishings, fixtures, and utilities that will be required for equipment maintenance.

In addition, vendors 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; and

c. Organizational affiliation (i.e., jurisdiction, vendor) of qualified maintenance personnel.

### 2.9.6 Appendices

The vendor 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 vendor. Topics recommended for amplification or treatment in appendix form include:

a. **Glossary:** A listing and brief definition of all terms that may be unfamiliar to persons not trained in either voting systems or computer maintenance;

b. **References:** A list of references to all vendor documents and other sources related to maintenance of the system; and

c. **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.

d. **Maintenance and Security Procedures:** This appendix shall contain technical illustrations and schematic representations of electronic circuits, with indications of all test and adjustment points, and the nominal value and tolerance or waveform to be measured.

## 2.10 Personnel Deployment and Training Requirements

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

## 2.10.1 Personnel

The vendor shall specify the number of personnel and skill level required to perform each of the following functions:

a. Pre-election or election preparation functions (e.g., entering an election, race 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; and

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 vendor personnel.

## 2.10.2 Training

The vendor 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. Data personnel; and

f. Vendor personnel.

## 2.11 Configuration Management Plan

Vendors shall submit a Configuration Management Plan that addresses the configuration management requirements of Volume I, Section 8 of the Standards. This plan shall describe all policies, processes and procedures employed by the vendor to carry out these requirements. Information submitted by the vendor shall be used by the test authority to assist in developing and executing the system qualification 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 test authority 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 vendor shall provide a description of its organizational policies for configuration management, addressing the specific requirements of Volume I, Section 8.3 of the Standards. These requirements pertain to:

a. Scope and nature of configuration management program activities; and

b. Breadth of application of vendor's policy and practices to the voting system.

### 2.11.2 Configuration Identification

The vendor shall provide a description of the procedures and naming conventions used to address the specific requirements of Volume I, Section 8.4 of the Standards. These requirements pertain to:

a. Classifying configuration items into categories and subcategories;

b. Uniquely numbering or otherwise identifying configuration items; and

c. Naming configuration items.

### 2.11.3 Baseline, Promotion, and Demotion Procedures

The vendor shall provide a description of the procedures and naming conventions used to address the specific requirements of Volume I, Section 8.5 of the Standards. 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 qualification testing; and

c. Promoting subsequent instances of a component to baseline status as the component is maintained throughout its life cycle.

### 2.11.4 Configuration Control Procedures

The vendor shall provide a description of the procedures used by the vendor to approve and implement changes to a configuration item to prevent unauthorized additions, changes, or deletions to address the specific requirements of Volume I, Section 8.6 of the Standards. These requirements pertain to:

a. Developing and maintaining internally developed items;

b. Developing and maintaining third-party items;

c. Resolve internally identified defects; and

d. Resolve externally identified and reported defects.

## 2.11.5 Release Process

The vendor shall provide a description of the contents of a system release, and the procedures and related conventions by which the vendor installs, transfers, or migrates the system to ITAs and customers to address the specific requirements of Volume I, Section 8.7 of the Standards. These requirements pertain to:

a. A first release of the system to an ITA;

b. A subsequent maintenance or upgrade release of a system, or particular components, to an ITA;

c. The initial delivery and installation of the system to a customer; and

d. A subsequent maintenance or upgrade release of a system, or particular components, to a customer.

## 2.11.6 Configuration Audits

The vendor shall provide a description of the procedures and related conventions for the two audits required by Volume I, Section 8.8 of the Standards. These requirements pertain to:

a. Physical configuration audit that verifies the voting system components submitted for qualification to the vendor's technical documentation; and

b. Functional configuration audit that verifies the system performs all the functions described in the system documentation.

## 2.11.7 Configuration Management Resources

The vendor shall provide a description of the procedures and related conventions for the maintaining information about configuration management tools required by Volume I, Section 8.9 of the Standards. These requirements pertain to information about:

a. Specific tools used, current version, and operating environment;

b. Physical location of the tools, including designation of computer directories and files; and

c. Procedures and training materials for using the tools.

## 2.12 Quality Assurance Program

Vendors shall submit a Quality Assurance Program that addresses the quality assurance requirements of Volume I, Section 7 of these the vendor's Standards. This plan shall describe all policies, processes and procedures employed by the vendor 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 test authority. A well-organized, robust and detailed Quality Assurance Program will enable the test authority 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 indicate below:

### 2.12.1 Quality Assurance Policy

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

a. Scope and nature of QA activities; and

b. Breadth of application of vendor's policy and practices to the voting system.

### 2.12.2 Parts & Materials Special Tests and Examinations

The vendor shall provide a description of its practices for parts and materials tests and examinations that meet the requirements of Volume I, Section 7.3 of the Standards.

### 2.12.3 Quality Conformance Inspections

The vendor shall provide a description of its practices for quality conformance inspections that meet the requirements of Volume I, Section 7.4 of the Standards.

The record of tests provided shall include for each test performed:

a. test location;

b. test date;

c. individual who conducted the test; and

d. test outcome

### 2.12.4 Documentation

The vendor shall provide a description of its practices for documentation of the system and system development process that meet the requirements of Volume I, Section 7.5 of the Standards.

## 2.13 System Change Notes

Vendors submitting a system for testing that has been tested previously by the test authority and issued a qualification number shall submit system change notes. These will be used by the test authority 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 changes;

b. A listing of the specific changes made, citing the specific system configuration items changed and providing detailed references to the sections of documentation changed;

c. The specific sections of the documentation that are changed (or complete revised documents, if more suitable to address a large number of changes) ;

d. Documentation of the test plan and procedures executed by the vendor for testing the individual changes and the system as a whole, and records of test results.