

**New York State Voting System Qualification
Master Test Plan (Draft)**

8/31/2006
Version: 0.1

DRAFT

NEW YORK STATE VOTING SYSTEM QUALIFICATION	1
MASTER TEST PLAN (DRAFT)	1
1. SCOPE	5
1.1. Qualification Test Approach	5
1.2. Qualification Test Evaluation Criteria.....	6
1.3. Proprietary Data	7
1.4. Reference.....	7
1.5. Terms and Abbreviations	7
2. PRODUCT SUBMITTAL AND INITIAL INSPECTION	8
2.1. Materials Required for Qualification Testing	8
2.1.1. Documentation	8
2.1.2. Software	9
2.1.3. Equipment	9
2.1.4. Test Materials	10
2.1.5. Deliverable Materials	10
2.2. Initial TDP Review and Functional Audit.....	11
3. TDP REVIEW	12
4. SOURCE CODE REVIEW	12
5. PRE-CERTIFICATION TESTS	13
6. VOTING SYSTEM TEST PLAN PREPARATION	13
6.1. Requirements Specification.....	13
6.2. Hardware Configuration	14
6.3. Test Case Design.....	14
6.3.1. Component Test Case Design	15
6.3.2. Hardware Testing	16
6.3.3. System Integration Test Case Design	16
6.4. Test Data	17
7. MASTER TEST SPECIFICATIONS	18

7.1. Component Tests.....	18
7.1.1. Ballot Preparation Component	18
7.1.2. DRE Component Test	20
7.1.3. Paper Ballot Processing Component	23
7.1.4. Central Tally Component	24
7.1.5. Witness Compile Test	26
7.2. Hardware Component Tests	28
7.2.1. Hardware Qualitative Examination Design	28
7.3. System Integration Test.....	29
7.3.1. General Election System Integration Test	29
DOES STRAIGHT PARTY VOTE NEED TO BE REMOVED – VERIFY WITH NYBOE	29
7.3.2. Primary Election System Integration Test.....	30
8. TEST PROCEDURE AND CONDITIONS.....	31
8.1. Facility Requirements.....	31
8.1.1. Ciber Facility	31
8.1.2. Wyle Facility	31
8.1.3. NYBOE System Integration Test Facility	32
8.2. Test Set-up	32
8.3. Test Sequence	32
8.4. Test Operations Procedures	32
8.4.1. Anomaly Processing.....	33
APPENDIX A: REQUIREMENTS	34
A.1 Functional Requirements	34
A.2 TDP Requirements.....	58
A.3 Source Code Standards.....	88
APPENDIX B: TEST SCENARIOS.....	97
B.1 Ballot Preparation.....	97
1. Jurisdiction Specification	97
2. (Geographical Breakdown) (specify precincts, split precincts, districts, polling places).....	97
3. Election Specific Definition	97
4. Candidate Definition.....	97
5. Create Ballot Styles.....	97

6.	Election backup and restore.....	97
7.	Multiple languages.....	97
8.	HAVA – Audio/ disabilities.....	98
9.	Test ballot generation.....	98
10.	Voting (DRE).....	98
11.	Machine startup and test.....	98
12.	Poll closing.....	98
13.	Voter receipt.....	99
B.2	Voting (Paper ballot).....	99
B.3	Central Tally.....	99
APPENDIX C: TDP INITIAL MATRIX CHECKLIST.....		100
APPENDIX D: REQUIRED FUNCTIONS CHECKLIST.....		103
APPENDIX E: SYSTEM INTEGRATION TEST BALLOTS.....		104

DRAFT

1. Scope

This document defines the procedures that will be used to qualify voting systems for use within the State of New York. The State of New York Board of Elections (NYBOE) has specified requirements and standards for voting systems that qualify for State Certification. This Master Test Plan describes the reviews, inspections, audits and tests used to assess the degree of compliance of voting systems to those certification standards. While all voting systems must conform to the standards specified by the NYBOE, they may differ in the operations and methods used, and may provide additional features that are not required. The procedures and test specifications defined in this test plan may be tailored as appropriate to match the unique characteristics of each system. The development of these individual voting system test plans implementing the procedures identified in this document will ensure that all voting systems are accurately assessed to the same standards.

The following subsections provide an overview to the qualification test process. Sections 2 through 5 describe the document review and code inspection procedures. Section 6 describes the preparation of the individual voting system test plan that defines the component, hardware and system integration testing for a voting system. Section 7 provides basic test cases that are intended to provide a template for the designing of test cases for each voting system. Section 8 discusses the procedures that each tester should follow when setting up and conducting the component and system integration tests. The Appendices provide detailed information that augments the main text.

(In this document, when the term NYBOE refers to an organization that is performing some qualification test activity, the term includes both the NYBOE and the organizations that it authorizes to assist with the testing.)

1.1. Qualification Test Approach

The qualification test for each voting system consists of the following:

- Product Submittal and Initial Inspection – Ciber conducts an Initial TDP Review and Functional Audit to verify that the voting system includes all documentation and critical functions necessary to be accepted for qualification test. The Ciber team sets up a database to track and coordinate Qualification Test activities as part of this effort.
- TDP Review – Ciber reviews the entire technical data package (TDP) for technical completeness, consistency and accuracy.
- Source Code Review – Ciber verifies that the source code complies with state (see 1.4 Reference 2), federal (see 1.4 Reference 1), and vendor coding standards.

- Pre-certification Tests – Ciber reviews the vendors’ test specifications and pre-certification test results to assess the effectiveness of the vendors’ testing activities.
- Voting System Test Plan Preparation - the test specifications provided in this Master Test Plan are tailored based on the unique characteristics of each voting system to fully validate all NYBOE required and/or vendor specified functions and standards.
- Component Testing – All options and functions of each software and hardware components are validated for correct operation. Environmental tests are conducted on all hardware components.
- Internal Audit Report – Upon completion of Component Testing, Ciber creates a report describing the results of all review and test activities conducted to that point.
- System Integration Testing, - The NYBOE and Ciber validate the integrated operation of the voting system by simulating one or more elections under public observation.
- Prepare Final Report – Ciber documents the results of the qualification test with the recommendation “For” or “Against” State certification.

If anomalies are encountered in any of the review or test activities, Ciber provides a report of the anomaly to the vendor. At the discretion of the NYBOE and Ciber, the test may continue or be suspended until the anomaly is resolved with the vendor.

The NYBOE and Ciber have divided the approach into two phases. Phase one consists of all activities listed above up to and including the Component Testing and resulting Internal Audit Report. Ciber and Wyle Laboratories will perform Phase I activities in Huntsville, AL. Phase II will consist of System Integration Testing and Final Report preparation. System Integration Testing will be conducted in New York at a location specified by the NYBOE.

1.2. Qualification Test Evaluation Criteria

The voting system must conform to the standards and requirements presented in the following documents:

1. EAC 2005 Voluntary Voting System Guidelines
2. New York State Voting System Standards
3. Voting System TDP submitted by the vendor

Appendix A presents the requirements extracted from the first two sources for qualification test evaluation. Functional requirements are validated by component or system integration tests. Vendor-specific requirements are validated by document review or code inspection. Those vendor-specific requirements flagged as “optional” are not required for certification but they must operate correctly if the voting system provides them.

The TDP must accurately describe the voting system. All functions and standards described in the TDP must be implemented in the voting system as described. The failure of the system to operate as described in the TDP is noted as an anomaly.

Appendix A contains many similar requirements. The qualification test procedures described in this test plan associates similar requirements so that they can all be addressed with a minimum number of reviews and/or tests.

1.3. Proprietary Data

All proprietary data that is so marked will be distributed only to those persons that the NYBOE identifies as needing the information for the conduct of qualification testing. The vendor is required to mark all proprietary documents as such. All organizations and individuals receiving proprietary documents will ensure those documents are not available to non-authorized persons.

1.4. Reference

1. Election Assistance Commission 2005 Voluntary Voting System Guidelines
2. Subtitle V of Title 9, Part 6209 (Voting System Standards) of the Official Compilation of Codes, Rules and Regulations of the State of New York
3. Cyber ITA Qualification Test Process for Voting System Software, Document Number ITA 2002 QTP, Release 1.0, 4/15/05
4. NASED Voting System Standards Board, Technical Guide #3, Witness Compile Clarification, (no date), (No version)

1.5. Terms and Abbreviations

- COTS – Commercial off the Shelf
- CP – Component
- DRE – Direct Recording Electronic voting system
- EAC – Election Assistance Committee
- FEC – Federal Election Commission
- ITA – Independent Test Authority (NASED certified)
- NASED – National Association of State Election Directors
- NYBOE – New York State Board of Elections (includes their authorized testing agents when referring to the conduct of a qualification test activity.)
- N of M Contest
- PPO – Preprinted Oval
- QTP – Qualification Test Process
- TDP – Technical Data Package, the documentation provided by the vendor.

2. Product Submittal and Initial Inspection

The vendor will submit all materials and equipment to the NYBOE prior to the start of qualification testing. The NYBOE will distribute the materials and equipment to the appropriate locations for review, audit and test. The materials and equipment submitted by the vendor are specified in the following Subsection. The procedure for the initial review and audit of the submittal is described in Subsection 2.2.

2.1. Materials Required for Qualification Testing

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

- Software
- Equipment
- Test materials
- Deliverable materials
- Proprietary data

All materials will be delivered to the NYBOE. The NYBOE will ship the test materials and equipment to the location(s) specified by Ciber. Test materials will be provided in an electronic format, Microsoft Word, Adobe Acrobat or a compatible format. The vendor may provide source code in the internal format of a development tool with the stipulation that tool and its user documentation is furnished for the duration of the qualification test.

2.1.1. Documentation

The vendor will supply a Technical Data Package (TDP) that conforms to the requirements listed in Appendix A.2. The minimum documentation to be provided in the TDP must include the following documents as specified by the federal guidelines:

- A list of the documents submitted with a mapping of each document to the TDP requirement(s) that it satisfies. (i.e. a mapping of the TDP to the state and federal requirements.)
- System Overview
- System Functionality Description
- System Hardware Specification
- Software Design And Specification
- System Security Specification
- System Test And Verification Specification
- System Operational Procedures
- System Maintenance Procedures
- System Deployment and Training Requirements
- Configuration Management Plan
- Quality Assurance Program
- System Change Notes

If the vendor's documentation is organized differently than indicated in the requirements (i.e. different documents or different organization of the sections within a document), the vendor must supply a cross-reference mapping that directs the reviewer to the document and paragraph in which each item in the requirement list is addressed by his TDP. The vendor must include a functional matrix with the submitted TDP. The matrix is provided by the NYBOE. The vendor must complete the matrix by identifying each function that the software provides, as well as, the document that describes the operation of the identified function.

2.1.2. Software

The vendor shall provide the voting system software and all software necessary to support testing of the voting system. The software shall be delivered on the media in the format that would be provided to the jurisdiction that purchased the system. All required COTS software, (operating system, utilities, report generators, database managers, etc) that is not delivered with the above media, must be provided on separate, installable, licensed media.

The software is also initially installed with the hardware components when they are delivered as described in the following section.

2.1.3. Equipment

The vendor shall provide equipment required for performance testing of the hardware, software, telecommunications, security and system integration tests. The vendor will submit the following equipment in quantities sufficient for testing as specified by the New York State:

- Custom hardware devices to include DRE voting devices, paper vote scanning, marking and tabulating devices, recording devices, voter identification devices, and any other devices that support the maintenance and operation of the voting system. The vendor will supply the devices in the specified counts as follows:
 - 6 of each item for component test
 - 3 of each item for environmental and volume tests (component test)
 - 5 of each item for system integration test
- General purpose data processing and communications equipment and quantities required for the operation of the system including COTS computers used in the operation and maintenance of the voting system, such as ballot preparation, vote tally, equipment maintenance are listed as follows:
 - 1 of each item normally located at the central site for election management and tabulation for component test
 - 5 of each item when the item is located at the polling place (precinct level).

- Test instrumentation, as required, such as devices used to emulate large volumes of voters, polling places, communication lines are listed as follows:
 - Devices to emulate large volumes of voters for component testing on each hardware machine provided
 - Device to simulate multiple communication lines simultaneously accessing the voting system during system integration testing

The vendor must submit all voting system equipment configured as it would be delivered to a purchasing jurisdiction including the installed software that is normally resident on that equipment when it is delivered to the jurisdiction.

Unless Ciber specifies otherwise, the NYBOE will ship equipment to Wyle Laboratories in Huntsville for the conducting of component testing.

2.1.4. Test Materials

The vendor will provide the materials necessary to create ballots, vote ballots, tally and prepare reports. The test materials include the following:

- Paper as necessary to print paper ballots. Paper must be provided that conforms to the paper stock specified in the TDP. If the specification provides multiple weights, the minimum and maximum weights must be provided in each sheet size that is supported.
- Blank ballots (PPO Stock), if the system uses paper ballots but does not print them.
- Write/Read media used by the system for transferring data or controlling access. Such items as magnetic cards for controlling voter access, flash memory devices or any other media that is required to conduct an election or maintain the system. (CDs are provided by Ciber if needed.)
- Spare printer ribbons (2) or toner cartridges (2) for each printer submitted

The NYBOE will provide ballot styles to be used for System Integration Testing. For systems that do not print ballots, the vendor will provide sufficient number of ballots to perform the System Integration Test. If the vendor requires the ballots to be printed by another source, the vendor must coordinate with the NYBOE to get the election definition.

2.1.5. Deliverable Materials

The vendor will provide two matrixes with its TDP. The first will indicate that the required TDP content has been provided and will identify the document and paragraph where it is found. The second will consist of a checklist of basic functions required by the system. This checklist will be provided to the vendor organization, which will then confirm those functions are provided by indicating which document and paragraph describes the operation of the listed function.

The vendor will deliver all equipment and materials, including the TDP in a single delivery to the NYBOE. The specified quantities of equipment devices will be sufficient to allow component and system integration testing as stated in this Master Test Plan.

The NYBOE will forward the equipment and materials required for Phase 1 to the location(s) specified by Ciber. Upon completion of Phase 1, Ciber will return the equipment and any unused materials to the NYBOE.

2.2. Initial TDP Review and Functional Audit

Ciber will conduct an initial review and audit to verify that the voting system contains the minimal required capabilities, equipment and materials necessary to be accepted for qualification testing. The TDP initial review will verify that the vendor has responded positively to each line item in the “required documents” matrix. The review will consist of verifying the vendor has “checked” that item as being provided and that the physical document in which it is to appear has been submitted. The objective of this initial review is to identify any documents that may be missing from the TDP. The full TDP review which follows in Section 3 will determine if the documentation is adequate.

Ciber will review the Functional Qualification Matrix with the vendor to verify the basic functionality required by the NYBOE. The objective of this review is to ensure the vendor has been made aware of the minimal functions that must be provided and to eliminate those systems that do not provide them.

Ciber and Wyle Laboratories will physically audit the materials provided. The model numbers and serial numbers of all equipment will be recorded in an inventory file for this system. The audit will verify that the models provided are consistent with the equipment identified in the TDP and other documentation submittals. All software will be inventoried to include the version number of each item. The reviewer will verify that the version numbers are consistent with the documented versions specified in the TDP and in other documents required with this submittal.

If the review and audit process determines that any items are missing or that the version numbers are not as documented, the reviewer will notify the NYBOE and will suspend the qualification test until directed by the NYBOE to continue.

The inventory information is maintained throughout the qualification test process and is updated with status information as the equipment is relocated, serviced or returned.

3. TDP Review

The objective of the TDP review is to verify that the TDP conforms to the New York State Voting System Standards and the EAC 2005 Voluntary Voting System Guidelines. Ciber utilizes a checklist of TDP requirements derived from the fore mentioned standards and guidelines (see Appendix A.2) to verify that the submitted TDP contains the required content. The TDP checklist will become part of the Phase I Interim Report. Ciber will also use the vendor-supplied cross reference matrix to verify the information with the specifications.

Any omissions or inaccuracies detected by the review will generate an anomaly list that is sent to the NYBOE for resolution. The NYBOE may coordinate with the vendor to resolve the anomalies and will direct Ciber to continue or suspend the qualification test. Ciber will track the status of each anomaly and will include that information in the Phase 1 Interim report.

The reviewer will review the TDP submitted with the voting system according to the TDP review process described in Section 4.0 of the Ciber ITA Qualification Test Process for Voting System Software.

Test specifications provided with the TDP are examined by the Ciber tester(s) to assess the quality of the vendor's quality assurance program. The review of the vendor's test specifications is described in Section 5 of this document.

4. Source Code Review

The objective of the source code review is to verify that the code meets the requirements of the New York State Voting System Standards, the EAC 2005 Voluntary Voting System Guidelines, and the vendor's internal coding standards. The source code review is performed using a checklist, which is derived from the fore mentioned standards and guidelines, and a database form which is tailored for each vendor based upon the language used by that vendor. If the vendor has also specified internal coding standards that are to be adhered to, the reviewer will include those standards in the review.

The tester will review every line of source code using the source code review template as described in Section 5 of the Ciber ITA Qualification Test Process for Voting System Software (Reference 3). The vendor may provide additional or alternate coding standards that at the discretion of the NYBOE may be merged into the standards listed in Appendix A.3. All anomalies will be recorded in the source code review database and reported to the NYBOE. The NYBOE will direct Ciber to continue or suspend testing. Ciber will track all anomalies to resolution or until the qualification test is complete. A report of source code anomalies will be included in the Phase 1 Interim report.

5. Pre-certification Tests

Ciber will review the vendor's test specifications and test data that is submitted with the TDP. Ciber may utilize the vendor's test plans and data for component testing and will assess the coverage of the vendor's test cases against those that are contained within this test plan (see Appendix B). Ciber may utilize the vendor's test cases that it has determined equivalent, and will modify the vendor's test cases as necessary to ensure all functional requirements are validated for each component.

The vendor may include the documented results of its internal testing that (1) are signed by the tester, (2) identifies the date of the test, and (3) indicates the version of the software/hardware used in the test. When these items are provided, they may be used at the discretion of Ciber as validation of selected characteristics of the component.

When vendor's test results are used, Ciber will confirm the integrity of those results by independent test of selected portions of the vendor's test.

6. Voting System Test Plan Preparation

A detailed test plan will be prepared by the test team for each voting system submitted for qualification test. The test team will prepare a voting system test plan that defines the component and system integration testing as required by this Master Test Plan. The Voting System Test Plan defines the component and system integration tests necessary to validate the functional operation of both the software and hardware. The test plan will include:

- A listing of requirements / standards applicable to that voting system
- A list the equipment / software to be tested
- Identification of test facilities and test equipment required
- Definition of the test cases to be executed
- A traceability matrix linking every requirement to the test(s) that validate it (if necessary, the tester must expand existing test cases or create new ones)

A second, separate test plan will be prepared defining the hardware environmental testing to be conducted. That test plan will identify the environmental tests to be performed, the test facility required and the equipment to be tested.

6.1. Requirements Specification

The NYBOE declared that all voting systems shall be tested for conformance to the state's standards (see 1.4 Reference 2) and the 2005 federal guidelines (see 1.4 Reference 1). Ciber has extracted those requirements into a master database, flagging those functional requirements that must be validated by component and/or system integration testing (see Appendix A.1). However, each voting system may provide additional features, alternate features or may omit some capabilities that are not critical to the NYBOE. The test team must edit the requirements listed in the master database to match

the specific characteristics of that voting system. This edit consists of adding functions described in the voting system's TDP but not required by New York or federal standards, flagging requirements listed in the database but not provided according to the TDP, and editing some requirements to be more specific to a particular voting system.

Requirements are added to the database with an identifier that consists of a code identifying the source document and the paragraph number from which the requirement was extracted. Requirements that appear in the master list, but are edited or deleted by the test team will be flagged. And comments will be attached to the requirement describing the action taken, the justification for the action, and the impact to the qualification potential of that voting system. The requirement must be edited to reflect the specific capacities, limits, or choices that are not specified by the master requirements list.

Ciber has linked each requirement in the master database to the test case(s) that validates that requirement. When the test team adds or edits requirements the linkages to test cases must be examined and deleted if the test case is not applicable. Prior to the completion of testing, each requirement must be linked to a test case that validates it.

The testing must validate all requirements in the resulting voting system's specific requirements. Those requirements that are added and represent additional functions provided by the voting system that are not required by state or federal standards must be validated as if they were required by the standards and their failure to operate as specified in the TDP must be reported as an anomaly.

6.2. Hardware Configuration

The test plan must identify each hardware component of the voting system that is included in the test by documenting the following:

- component type
- manufacturer
- model number
- serial number

Any alternations or replacements to the equipment will be recorded in the inventory file for this voting system qualification test.

Component and hardware tests will be conducted in Huntsville at the Wyle Laboratory Facility. System integration tests will be conducted at a location in New York to be specified by the NYBOE. System integration tests will be open to public viewing.

6.3. Test Case Design

Component and system integration tests are defined by creating a number of test cases that operates the voting system sufficiently to ensure that all functional requirements

listed for this voting system are exercised. Each test case consists of a series of actions that exercise the selected voting system's functions and the expected results produced by those functions. The test team will then execute the test cases, record their observations, and analyze the output of the voting system to assess the pass/fail status for each requirement.

Ciber has defined a set of generic test cases and has linked those test cases to the requirements that they validate. These test cases and the tracing to the requirements are provided in the master database that the test team copied for their testing of the assigned voting system. The test team must review these master test cases and modify them if necessary to test the voting system assigned. The design will include maintaining the test-requirements cross reference that links each requirement to the test that validates it.

Test case design occurs at two levels of detail. The first level is the summary level in which the test team identifies test cases to exercise all functions provided by the voting system and to validate every functional requirement that is listed in the database. The test cases provided in this master test plan are at this summary level of detail. The second level is the detail level which consists of adding information to each test case that directs the tester on how that test case is to be executed on that specific voting system. Ciber requires the test team to complete test cases to the summary level. The need for the detail level may vary depending upon the specific voting system. The implementation of the detail level is at the discretion of the test team.

The test team must address the following types of tests:

- Component test case design
 - COTS Component Testing
 - Custom Component Testing
- Hardware environmental test case design

6.3.1. Component Test Case Design

Component test cases are designed to exercise every option and feature of the component. These tests utilize test elections as necessary to operate the component. The tests are conducted to verify:

- All installation options
- Every user action that can occur through the user interface
- Security of the component against unauthorized access
- Accuracy of tabulation features
- Completeness and accuracy of the audit log
- Recovery from errors
- Operation at the capacity limits specified in the TDP
- Provision for persons with visual or motor impairments
- Privacy

The design of component test cases varies based on whether they consist entirely of COTS hardware or if they utilize custom built hardware. In both cases the test team begins the design by selecting from this master test plan those test cases that apply to the voting system being tested. The team may modify the test cases as appropriate to address additional functions or alternate functions as provided by that voting system. As the test team completes each test case, they will update the mapping of tests cases to requirements. When all requirements have been traced, the design is complete for the summary level. If this is a COTS product, the test team may continue design to the level of detail desired. However, if this component is based on custom hardware, the test team will review the test cases with the hardware team that is to perform the hardware environmental tests. The test team and the hardware team will coordinate the detail test case design to ensure that all requirements are validated with minimal overlap of effort. The design will include team assignment of the requirement to be tested at the detail level.

The test team will evaluate the success / failure of the test case by verifying that each requirement assigned to that test case was successfully validated and flagging the requirement as such in the master database.

The component will have been successfully tested when all requirements assigned to all test cases for that component have been flagged as successfully validated.

6.3.2. Hardware Testing

6.3.3. System Integration Test Case Design

System integration test cases are designed to exercise all components of the voting system by conducting a simulated election. The simulation includes the following:

- preparing the electronic ballot
- distributing the ballot to multiple voting devices (DRE and paper)
- voting the election using all voting devices
- tabulating the results
- conducting a recount

System integration test cases are defined to execute elections using the sample ballot layouts provided by the NYBOE. These test cases derived by the sample ballot layouts are defined in this Master Test Plan. The test team must ensure that any requirements not fully tested during component testing are covered by the system integration test cases. The sample ballot layouts provided by the NYBOE are provided in Appendix E. The system integration tests derived from the sample ballots will consist of a primary election and a general election. The general election will include the following:

- 13 Contests

- 10 Parties
- 2 Person Slate
- N of M Contest
- 10 Proposals
- Write-in Votes

The primary election will include the followings:

- 11 Contests
- 3 Parties
- N of M Contest
- Write-in Votes

The test team will conduct both elections utilizing the provided ballot styles and at least 3 precincts, with one precinct having three voting machines. The elections will include absentee, early, provisional, and normal voting.

6.4. Test Data

The testing process will include creation of the ballots, voting and tallying votes. The same ballot layouts will be used for all vendors. However Ciber will tailor the ballots as necessary to test specific features or requirements of a voting system where the requirement or its method of implementation is unique to that voting system.

Component test data will be defined to exercise all functions of the component being tested. The component test cases will include elections that exercise the capacities and limits documented in the voting system TDP. Where those values are not specified, the test team will develop test data assuming that the component must support the following:

- XX candidates in one contest **NEED TO DISCUSS w/NY**
- XX contests **NEED TO DISCUSS w/NY**
- 3 precincts with 3 machines in one precinct
- N of M election
- Ranked election **NEED TO DISCUSS w/NY**
- Cumulative Election **NEED TO DISCUSS w/NY**
- Judicial election
- 2 fonts sizes for DRE devices
- All states of all options that are available for the component
- Invalid ballots and voter selections
- All user interface selections
- All installation options

System integration tests will use sample ballot layouts specified by the State of New York (see Appendix E).

BALLOT SPEC PROVIDED BY NYBOE

7. Master Test Specifications

Test specifications must verify each required capability in Appendix A.

7.1. Component Tests

Component testing exercises every option and feature of each component of the voting system. Component testing verifies the operation of each function, exercises error recovery logic, and tests the limits of operation as specified in the TDP.

In this set of component tests, the input data for one component may be provided by the output of another component test. That is, the ballots generated by the Ballot Preparation component test will provide the input data for the DRE component test. The results of the DRE component test will provide the input data for the Central Tally component test.

Components containing hardware that is custom built must complete environmental testing and if applicable, reliability and accuracy testing. The hardware test team describes the environmental, reliability and accuracy testing in a separate test plan. For these devices, the hardware test team may perform additional functional testing where the function requires little or no software implementation. In all cases, the Cyber team will track the testing of each requirement to ensure the tests provide full coverage of all requirements.

- **EXACTLY WHICH LANGUAGES ARE TO USED IN THE COMPONENT TESTS – VERIFY WITH NYBOE**
- **WILL NY UTILIZE A STRAIGHT BALLOT - VERIFY WITH NYBOE**
- **WHAT TYPE OF CONTESTS WILL NY CONDUCT: NoM, RANKED,CUMULATIVE, JUDICIAL, RECALL ... VERIFY WITH NYBOE**

7.1.1. Ballot Preparation Component

The Ballot Preparation component test includes all devices required to prepare the election for loading at the voting stations and to provide any electronic or hardcopy materials required for the voting process. Those items may include poll worker identification cards and voter identification cards. This test considers those devices to be one component of the voting system and the test must exercise each option of each device.

Test Case: CP-BPS-01	Configuration
<p>Ballot Preparation Component Test Plan - General Election</p> <p>This test must exercise all options that can be specified when building the ballots. These options may be utilized here to generate inputs for DRE, PB and CT. All values of each option must be exercised. Additional test cases may be generated as necessary.</p> <p>This test should follow the procedures exactly as described in the BPS Operators manual.</p> <p>Additional devices required for creating poll worker cards and voter identification cards are included with this component.</p>	<ol style="list-style-type: none"> 1. BPS computer is use to create ballots with following properties: General Election, 3 precincts, 5 machines, multiple ballot styles with XX Contests, 10 Parties, 2 Person Slate, N of M contest, Ranked, Recall, Cumulative, Judicial, 10 proposals, XX candidates in one contest 2. English, Spanish, Chinese 3. Multi-line Write-in 4. Straight party 5. Specify DRE / PB / other options 6. Include rotation, all contest options defined
Voting Devices Utilized: Ballot Preparation Computer	
Procedures:	
<ol style="list-style-type: none"> 1. Log into system as administrator and open menu option to Create New General Election 2. Verify password processing by attempting to use invalid password, change the password, and log in as a member as each "role" defined by the component. 3. Define jurisdiction organization as defined in above "configuration", include a split precinct 4. Add parties and contests to database as specified in above "configuration". Exercise all options provided and attempt entry of invalid data and out of order actions. 5. Add candidates with candidate rotation specified. Exercise options to order candidates and other options provided 6. Add proposals, insert alternate text if provided and exercise all options 7. Set all other database options (DRE Settings, poll start / stop times, etc) 8. Generate and view ballots, make changes to ballot formats and contents at all levels. 9. View sample ballot if that feature is provided 10. Add additional languages – exercise the logic to create the language phrases as required by the jurisdiction preparing the ballot. 11. Make final edits as necessary to get correct ballots. 12. Perform backup of ballot database (do backup of jurisdiction and contests separately if that capability is provided). 13. Prepare authorization media for poll workers and voters as required by the voting system 14. Attempt to make a change so that it is not logged in the audit log 15. Export the election as if it was to be loaded in the machines and precincts above. 16. Print required reports 17. Print each paper ballot style 18. Inspect and save audit log file 19. Attempt to modify election on exported media. 	

NUMBER OF CANDIDATES TO BE USED IN TEST CASE– VERIFY WITH NYBOE
NUMBER OF CONTESTS TO BE USED IN TEST CASE– – VERIFY WITH NYBOE

<p>Test Case: CP-BPS-02</p> <p>Ballot Preparation Component Test Plan – Primary Election</p> <p>This test must exercise all options that can be specified when building the ballots. These options may be set here for use in the DRE, PB or CT. All values of each option must be exercised. Additional test cases may be generated as necessary. This test should follow the procedures exactly as described in the BPS Operators manual.</p>	<p>Configuration</p> <ol style="list-style-type: none"> 1. BPS computer is use to create ballots with following properties: Primary election, 3 precincts, 5 machines, multiple ballot styles with XX Contests,8 Parties, 2 Person Slate, N of M contest, Ranked, Recall, Cumulative, Judicial, 10 Proposals, 2. English, Spanish, Chinese 3. Specify DRE / PB / other options 4. Include rotation, all contest options defined
<p>Voting Devices Utilized: Ballot Preparation Computer</p>	
<p>Procedures:</p> <ol style="list-style-type: none"> 1. Log into system as administrator and open menu option to Create New Primary Election 2. Verify password processing by attempting to use invalid password, change the password, and log in as a member as each “role” defined by the component 3. Import jurisdiction and contest information from previous election 4. Select or Add parties and contests to database as specified in above “configuration”. Exercise all options not exercised in previous test. 5. Add candidates with no candidate rotation. 6. Add proposals, insert alternate text if provided and exercise all options 7. Set all other database options (DRE Settings, poll start / stop times, etc using variables different than previous test). 8. Generate and view ballots, make changes to ballot formats and contents at all levels. 9. View sample ballot if that feature is provided 10. Make final edits as necessary to get correct ballots. 11. Perform backup of ballot database 12. Prepare authorization media for poll workers and voters as required by the voting system 13. Attempt to make a change so that it is not logged in the audit log 14. Export the election as if it was to be loaded in the machines and precincts above. 15. Print required reports 16. Print each paper ballot style 17. Inspect and save audit log file 18. Attempt to modify election on exported media. 	

NUMBER OF CANDIDATES TO BE USED IN TEST CASE– VERIFY WITH NYBOE
NUMBER OF CONTESTS TO BE USED IN TEST CASE– – VERIFY WITH NYBOE

7.1.2. DRE Component Test

The Ciber test team will create a large election that contains the maximum number of contests, parties and candidates required by the State of New York. The Component and hardware test cases defined for the DRE must exercise all possible choices for all features provided by the DRE.

Test Case: CP- DRE -01	Configuration
<p>DRE Component Test Plan - General Election</p> <p>Component test must exercise all states of every installation option and operational feature of the component. Additional tests cases may be generated if necessary. Five machines may be used to execute this test. The following procedure can be executed across the 5 machines, not intended to duplicate steps by executing the same step on multiple machines.</p>	<ol style="list-style-type: none"> 1. 3 precincts, multiple ballot styles, five voting machinist 2. General election with XX Contests,10 Parties,2 Person Slate, 10 proposals, XX candidates in one contest 3. Partisan Contest Types: Vote for one, Vote N of M, Cumulative, Presidential/Vice-Presidential Slate 4. Non-partisan Contest Types: Recall, Ranked, Proposal. 5. English, Spanish, Chinese
Voting Devices Utilized: DRE, VVPAT	
Procedures:	
<ol style="list-style-type: none"> 1. Inspect the voting station to insure privacy, lighting and aides for disabled, paraplegic, deaf, and blind voters 2. Power up voting station and verify diagnostics report and load database. 3. Vote election in test mode 4. Open polls (sign-in, print/review zero totals report) 5. Verify the ballot displays on single surface (may be scrollable) 6. Vote multiple ballots till all options possible options have been exhausted including the use of aides for disabled, paraplegic, deaf, and blind voters. <ol style="list-style-type: none"> a. Candidate write-in (both qualified and non-qualified) b. Under vote, over vote, other invalid voter actions c. Review and change ballot selections before casting d. Review paper record summary display and change max. number of times e. Exercise each font, color and contrast option f. Exercise each time-out situation (including Fleeing Voter) 7. Attempt to output ballot results prior to closing poll 8. Close poll 9. Export ballot results from primary and alternate memory sources 10. Export results for alternate media 11. Reconcile paper records to electronic record and reconcile rejected ballots to rejected voter receipts 12. Print/export and review audit log 13. Import and verify results formatted correctly for central tabulator 	

NUMBER OF CANDIDATES TO BE USED IN TEST CASE– VERIFY WITH NYBOE
NUMBER OF CONTESTS TO BE USED IN TEST CASE– – VERIFY WITH NYBOE

Test Case: CP- DRE -02	Configuration
<p>DRE Component Test Plan - Primary Election Component test must exercise all states of every installation option and operational feature of the component. Additional tests cases may be generated if necessary.</p> <p>Five machines may be used to execute this test. The following procedure can be executed across the 5 machines, not intended to duplicate steps by executing the same step on multiple machines.</p>	<ol style="list-style-type: none"> 1. 3 precincts, 5 machines, multiple ballot styles 2. Primary election with XX Contests, 10 Parties, 2 Person Slates, 10 proposals 3. Partisan Contest Types: Vote for one, Vote N of M, Cumulative, Presidential/Vice-Presidential slate 4. Non-partisan Contest Types: Recall, Ranked, Proposal. 5. English
Voting Devices Utilized: DRE, VVPAT	
Procedures:	
<ol style="list-style-type: none"> 1. Power up voting station and verify diagnostics report and load database. Vote election in test mode 2. Open polls (sign-in, print/review zero totals report) 3. Verify the ballot displays on single surface (may be scrollable) 4. Vote early and suspend early vote 5. Vote multiple ballots till all options possible options have been exhausted including the use of aides for disabled, paraplegic, deaf, and blind voters. <ol style="list-style-type: none"> a. Candidate write-in (both qualified and non-qualified) b. Under vote, over vote, other invalid voter actions c. Review and change ballot selections before casting d. Review and paper record summary display and change max. number of times e. Exercise each font, color and contrast option f. Exercise each time-out situation (including Fleeing Voter) 6. Resolve early votes 7. Disable electrical service and verify battery power source 8. Close poll 9. Export ballot results from primary memory source 10. Reconcile paper records to electronic record and reconcile rejected ballots to rejected voter receipts 11. Print/export and review audit log 12. Import and verify results formatted correctly for central tabulator 	

NUMBER OF CANDIDATES TO BE USED IN TEST CASE– VERIFY WITH NYBOE
NUMBER OF CONTESTS TO BE USED IN TEST CASE– – VERIFY WITH NYBOE

7.1.3. Paper Ballot Processing Component

Test Case: CP- PB -01	Configuration
Paper Ballot Component Test Plan - Primary Election	<ol style="list-style-type: none"> 1. Three precincts with at least one split (multiple ballot styles) 2. Primary election with XX Contests, 10 Parties, 2 Person Slate, 10 proposals, XX candidates in one contest 3. Partisan Contest Types: N of M 4. Non-partisan Contest Types: Recall, Ranked, Proposal 5. English, Spanish, Chinese 6. Multi-line Write-in
Voting Devices Utilized: Paper Ballot Scanner and Tabulator	
Procedures:	
<ol style="list-style-type: none"> 1. Power up voting station and verify the startup procedure by printing the diagnostics report. The database can then be loaded. 2. Vote election in test mode 3. Open polls (sign-in, print/review zero totals report) 4. Ballot displayed on single surface of paper and may appear on the reverse side. 5. Vote multiple ballots till all options possible options have been exhausted: <ol style="list-style-type: none"> a. Candidate write-in (both qualified and non-qualified) b. Under vote, over vote, other invalid voter actions c. Utilize blank ballots d. Shuffle the ballots / insert incorrect ballots / skew ballots on input e. Force double feed or feed jam if possible f. Paper ballot will be used for manual audits g. Max and min paper stock weights, including all paper sizes specified 6. Attempt to output ballot results prior to closing poll 7. Resolve write-ins, overvotes and undervotes if those features are provided 8. Close poll 9. Export ballot results 10. Reconcile paper records to electronic record and reconcile rejected ballots to rejected voter receipts 11. Print/export and review audit log 12. Import and verify votes into central tabulator 	

NUMBER OF CANDIDATES TO BE USED IN TEST CASE– VERIFY WITH NYBOE
NUMBER OF CONTESTS TO BE USED IN TEST CASE– – VERIFY WITH NYBOE

Test Case: CP- PB -02	Configuration
Paper Ballot Component Test Plan - General Election (This test will use the ballot files output by the BPS component test.)	1. Three precincts with at least one split (multiple ballot styles) 2. General election with XX Contests, 10 Parties, 2 Person Slate, 10 proposals, XX candidates in one contest 3. Partisan Contest Types: N of M 4. Non-partisan Contest Types: Recall, Ranked, Proposal. 5. English, Spanish, Chinese 6. Multi-line Write-in
Voting Devices Utilized: Paper Ballot Scanner and Tabulator	
Procedures:	
<ol style="list-style-type: none"> 1. Power up voting station and load database. 2. Open polls (sign-in, print/review zero totals report) 3. Vote early and suspend early voting. 4. Ballot displayed on single surface of paper and may appear on the reverse side. 5. Vote multiple ballots till all possible options have been exhausted including the use of aides for disabled, paraplegic, deaf, and blind voters. <ol style="list-style-type: none"> a. Candidate write-in (both qualified and non-qualified) b. Under vote, over vote, other invalid voter actions c. Utilize blank ballots d. Shuffle the ballots / insert incorrect ballots / skew ballots on input e. Force double feed or feed jam if possible f. Paper ballot will be used for manual audits g. Max and min paper stock weights, including all paper sizes specified 6. Resolve write-ins, overvotes and undervotes if those features are provided 7. Resolve early votes 8. Close poll 9. Export ballot results 10. Reconcile paper records to electronic record and reconcile rejected ballots to rejected voter receipts 11. Print/export and review audit log 12. Import and verify votes into central tabulator 	

NUMBER OF CANDIDATES TO BE USED IN TEST CASE– VERIFY WITH NYBOE
NUMBER OF CONTESTS TO BE USED IN TEST CASE– – VERIFY WITH NYBOE

7.1.4. Central Tally Component

The Central Tally component test is defined in this section to include all devices necessary to receive the vote tallies from the polling places, compute the consolidated totals at various jurisdictional levels, and broadcast or distribute the election results. Voting systems will vary depending upon the equipment they use to receive and tally the votes at the central site. The broadcasting of unofficial results is not required, but must be tested if the voting system provides it. If multiple hardware devices are used for these central tally functions, this component test may treat them as one component provided that all features and options that can be exercised in an election are exercised in this test.

Test Case: CP-CT-01	Configuration
<p>Central Tally Component Test Plan – Primary Election</p> <p>This test includes all devices necessary to receive the vote tallies from the polling places, compute the consolidated totals at various jurisdictional levels, and broadcast or distribute the election results. If multiple hardware devices are used for these functions, this component test may treat them as one component provided that all features and options that can be exercised in an election are exercised in this test.</p>	<ol style="list-style-type: none"> 1. 3 Precincts including one split , multiple ballot styles 2. Primary election, 8 political parties, XX contests, Presidential slate, XX candidates in one contest, 10 Proposals 3. 2 Person slate 4. Contest Types: N of M, Ranked, Cumulative, Judicial, Recall 5. Regular and Provisional ballots 6. Straight Party voting 7. English, Spanish, Chinese
Voting Devices Utilized: Central Tally Device, Telecommunication devices	
Procedures:	
<ol style="list-style-type: none"> 1. Start Central Tally and verify counter values are set to zero 2. Import vote totals (electronically) from precincts and initiate broadcast of unofficial tally (aggregated only, marked “unofficial”) 3. Attempt to modify official results on transport media using unauthorized methods 4. Import official vote tallies (hand carried from poll) from precincts, including absentee ballots, to the Central Talley location. 5. Tally votes at Central Site 6. Perform resolution of irregular ballots such as provisional, write-ins (qualified and unqualified) 7. attempt to modify / alter votes or ballot information in database using unauthorized methods 8. Tally votes cast for each proposition 9. Finalize results 10. Execute all Reports 11. Retrieve report of number of overvotes and undervotes by tabulator, precinct and additional jurisdictional levels 12. Report totals by election districts such as legislative districts or wards 13. Export data in a standard, commercial format for reading by external program(s) 14. Reinitialize Central Site tabulator to clear all counters and perform recount / audit utilizing paper records 15. Conduct recount using paper receipts and paper ballots 16. Inspect audit log, including any audit logs imported with vote tallies from precincts 17. Use a standard commercial text edition to read exported files and verify digital signature 	

NUMBER OF CANDIDATES TO BE USED IN TEST CASE– VERIFY WITH NYBOE
NUMBER OF CONTESTS TO BE USED IN TEST CASE– – VERIFY WITH NYBOE

7.1.5. Witness Compile Test

Witness Compile tests are performed to ensure that each voting system component contains only the software specified in the voting system TDP. Also the Witness Compile tests are performed to ensure that the installation media that is distributed to purchasing jurisdictions contains all software required to install the system except for those items explicitly specified by the vendor as prerequisites. The test case requires a report utilizing the Ciber format.

Test Case: Witness Build	Configuration
The witness compile must be performed all software/firmware that is part of the Voting System.	The vendor's development system is used to generate the installable modules and create the installation media. One of each device in the voting system must be purged of all software to sufficiently ensure the only software resident is that which has been declared by the vendor as a prerequisite for installation of the voting system.
Voting System Component Utilized: Development Environment, One of each voting system device that utilizes software/firmware.	
Procedures:	
<ol style="list-style-type: none"> 1. Reviewer of the technical data package must extract a description of the compilation environment including the operating system, service packs, compilers, libraries and utilities that the system developer will use to build the system installation media. 2. Auditor of the compilation environment will examine the compilation environment to determine that it complies with the description in deliverable number 1 and will create a report stating the finding of compliance. 3. Test team will observe the source being copied to the specified directory on the development computer and will ensure that the directory is the source used by the compiler. 4. Test team witness shall observe, in person, on site, the developer's employees compiling the programs and assembling the contents and formatting of the installation media, using the source code that has been independently reviewed by the test agency and not previously provided to developers prior to this witness build test. 5. Test team will collect each installation media and will maintain it with no distribution to any external agency. 6. Test team will generate hash numbers for each installation module and for the source modules that were used to create it. 7. At each device, the test team will examine the machine and perform actions necessary to ensure: <ol style="list-style-type: none"> a. Directories to be used are cleared of prior source code and compiled output files. b. Objects and executables are then copied into the directories for the install creation. c. The test team will exercise the component to verify the installation and the application in the test environment. 8. Test team will prepare a report documenting the witness build and will provide directory information using the Ciber format. 	

Witness Compile

A witnessed compile in an audited compilation environment was created for the “*Vendor and System Name and Version*”. This work was performed in compliance with the Technical Guide #3 adopted by the National Association of State Election Directors (NASED). The Auditing and Witnessing was performed by “*Auditor*”.

The technical data package documents defining the compilation environment, including the operating system, service packs, compilers, libraries and utilities, were audited and documented below. The source code used for the compile was reviewed by Ciber. The source code review was completed. The anomalies and basis for recommending the source code for compliance are documented in TBD.

To prepare the machine for the witnessed compile:

- Directories to be used were cleared of prior source code and compiled output files.
- The source was copied to “*Directory*” from the Auditors possession.
- The presence of all files was verified.

The compile was executed.

The object and executables were then copied into the directories for the install creation. Installed and verified functionality of both the install and the application in the test environment. “*Test PC*”.

System Name:	
Date:	
System Developer:	
PC/Laptop Make, Model, and Serial Number:	
Operating System and Service Pack:	
Compiler Name, Version and Serial Number:	
Libraries:	
Utilities	

Anomalies and Observations

Prepared two media devices

“Source and Build Documents” and “MD5 hash numbers”

“Trusted Build” and “MD5 hash numbers”

As a part of this process, the tester shall review the vendor's functional test case designs. The detailed list of functions provided in Appendix A will be used in conjunction with the standard test scenarios. A subset of tests will be developed to verify each requirement provided by this system as specified in the TDP.

The tests shall be tailored for a specific system by the following actions:

- Utilizing the Qualification Matrix and the TDP review results to identify the requirements / features to be tested
- Selecting the test scenarios that verify those features
- Modifying those test scenarios to conform to the procedures specified by the system operator / user manuals
- Expanding the test scenarios for optional features provided by the vendor that are not listed in the federal or New York standards (see 1.4 Reference).

7.2. Hardware Component Tests

7.2.1. Hardware Qualitative Examination Design

Wyle will conform to the State of New York's 6902.2 Voting Specifications and also the Federal Specification in Volume 1, Section 4 and Volume 2, Section 4. Ciber will provide Wyle with the test cases to verify these specifications.

7.3. System Integration Test

7.3.1. General Election System Integration Test

Test Case: SY-GE-01	Configuration
System Integration General Election Test Case	<ol style="list-style-type: none"> 1. 3 Precincts plus split precinct 2. 5 voting; machines, 3 in one precinct 3. 10 political parties 4. 10 Proposals 5. 2 person slate 6. Multiple ballot styles 7. Contest types: N of M, 8. Regular and provisional ballots 9. Straight Party voting 10. English, Spanish, Chinese 11. Voter Registration Files as inputs
Voting Devices Utilized: DRE, VVPAT, Paper Ballots	
Procedures:	
<ol style="list-style-type: none"> 1. Prepare electronic ballot and export to media for transfer to voting systems and print paper ballots 2. Power up voting station and load database. 3. Prepare voter access media for applicable voting device for each voter that will vote in the election 4. Vote election in test mode 5. Open polls (sign-in, print/review zero totals report) 6. Verify that ballot displayed on single surface 7. Vote early and suspend early voting 8. Cast provisional votes 9. Vote multiple ballots on 5 voting stations <ol style="list-style-type: none"> a. Candidate write-in (both qualified and non-qualified) b. Touch screen and voice assisted voting c. Under vote, over vote, other invalid voter actions d. Review and change ballot selections before casting e. Review paper record summary display and change max. number of times f. Exercise time-out situation for Fleeing Voter 10. Resolve early votes where applicable 11. Close poll, perform precinct level tabulations, and export ballot results 12. Print/export and review audit log 13. At Central Tabulation Site <ol style="list-style-type: none"> a. Tally test voting where applicable b. Verify zero totals c. Initiate unofficial Tally Broadcasting d. Import totals, including absentee ballots e. Consolidate vote from precinct levels f. Perform resolution of irregular ballots (provisional, write-ins, etc) g. Finalize results h. Print all reports i. Print and review audit log j. Simulate a recount 	

DOES STRAIGHT PARTY VOTE NEED TO BE REMOVED – VERIFY WITH NYBOE

7.3.2. Primary Election System Integration Test

Test Case: SY-PE-01	Configuration
System Integration Primary Election Test Case	<ol style="list-style-type: none"> 1. 3 Precincts 5 voting machines 2. 3 political parties 3. Contest types: N of M, 4. Regular and provisional ballots 5. English, Spanish, Chinese Languages 6. Voter Registration Files as inputs
Voting Devices Utilized: DRE, VVPAT, Paper Ballots	
Procedures:	
<ol style="list-style-type: none"> 1. Prepare electronic ballot according to export to media for transfer to voting systems and print paper ballots 2. Power up voting station and verify the startup by printing the diagnostics report. The database can then be loaded. 3. Prepare voter access media for applicable voting device for each voter that will vote in the election 4. Open polls (sign-in, print/review zero totals report) 5. Cast provisional votes 6. Verify that multiple ballots of each ballot type both DRE and Paper Ballots <ol style="list-style-type: none"> a. Candidate write-in (both qualified and non-qualified) b. Touch screen and voice assisted voting c. Under vote, over vote, other invalid voter actions d. Review and change ballot selections before casting e. Review and paper record summary display and change max. number of times f. Possibly – cross party voting, endorsed candidate (candidate in multiple parties?) 7. Close poll, perform precinct level tabulations, and export ballot results 8. Print/export and review audit log 9. At Central Tabulation Site <ol style="list-style-type: none"> a. Verify zero totals b. Import totals, including absentee ballots c. Tally Central Site results d. Perform resolution of irregular ballots (provisional, write-ins, etc) e. Finalize results f. Print all required reports g. Print and review audit log 	

8. Test Procedure and Conditions

This section addresses only the component and system integration testing activities of the qualification testing.

8.1. Facility Requirements

The tests will be performed at the following facilities:

- Ciber facility
- Wyle Facility
- NYBOE System Test Facility

The following paragraphs provide a brief statement of the testing that will occur at each facility.

8.1.1. Ciber Facility

Ciber will manage and coordinate all testing from its facility. All documentation and source code will be shipped to the Ciber office. The Ciber Test Team will conduct the TDP and source code reviews, perform test planning. Ciber administrators will provide configuration management and will oversee project schedules.

The Ciber facility provides office space for the test teams with separate tools for each team to prepare test plans, record test results and prepare test reports. Each voting system will be supported by a dedicated test team, their required office space that includes a computer for each person and access to a central server. Each test team will be provided an automated tool for planning and tracking their test activities.

The configuration manager will utilize a central server for archival of electronic documents. File cabinets are available for hardcopy documents, optical and magnetic media.

The facility will be used for reliability and accuracy testing of COTS hardware that has not been previously certified for voting system use. The hardware will be maintained in test rooms that ensure it is protected from observation by unauthorized personnel.

8.1.2. Wyle Facility

Wyle Laboratories will perform environmental and accuracy testing of all custom hardware. The facility provides chambers for environmental, vibration and electrostatic testing of the hardware. The facility provides office space and computers for the Hardware test team.

All voting system hardware will be shipped to the Wyle facility. Following environmental testing, the hardware team will setup the equipment for Component Testing.

8.1.3. NYBOE System Integration Test Facility

The NYBOE will provide a facility for conducting system test. The facility will provided sufficient room to allow each voting system to be setup with necessary testing gear. The facility will provide work space for the Ciber test team while conducting the system tests.

The facility will provide for public viewing of the test from an area that is separated by the equipment being tested and the work area used by the Ciber Test Team. The facility will allow for all voting systems to be tested simultaneously.

8.2. Test Set-up

The Wyle Laboratory Hardware Test Team will receive all equipment and setup the equipment for environmental testing. When equipment becomes available, the hardware team will move it to an area reserved for component testing. The hardware team will set up the equipment for component testing and will support the Ciber team if they encounter any equipment failures during the testing.

The Vendors will set up the equipment for system integration testing. Ciber will notify the NYBOE of any equipment problems during the system integration test.

8.3. Test Sequence

The sequence of testing is as follows:

- Hardware component testing, including environmental and functional tests are performed by Wyle and ballot generation and tally component is conducted by Ciber
- System Integration testing will be conducted in New York for those systems that successfully complete component testing.

8.4. Test Operations Procedures

The test cases in Section 7 provide the steps performed for each test. Each test team will prepare and conduct tests by executing the following procedure:

1. Create a copy of the Master Test Database for dedicated use in planning and tracking the testing of the assigned voting system.
2. Review and tailor the requirements list to include requirements unique to this voting system and eliminate requirements that do not apply based on the results of the TDP review.
3. Create test cases necessary to fully test this voting system by copying and modifying the master test scenarios provided in the test database.
4. Update test to requirements cross reference so that each requirement is traced to the test case that validates it.
5. Conduct component test of each component, notifying the NYBOE of any anomalies and recording test results for each component test case.
6. Following successful completion of component test, prepare a test report of results.

7. Edit and revise system test scripts as appropriate based on component test results.
8. Conduct system test at the location specified by NYBOE, recording results and reporting anomalies.
9. Prepare final report.

8.4.1. Anomaly Processing

Ciber will utilize the following methods for reporting anomalies.

During TDP reviews, anomalies will be recording in electronic media and transmitted to the NYBOE. If an anomaly is resolved, the record will be updated to note that it is not a current anomaly.

During source code reviews, the reviewer will record the unit (subroutine, procedure) that contained the error, the line number of the error and a definition of the error. This information is accumulated for the entire review and then transmitted to the NYBOE at the completion of the review. If any anomalies are resolved, they will be so indicated it the original report.

During component and system test, an exception report will be created for each anomaly and the exceptions for each test will be provided to the NYBOE following each test. If the exception is resolved, the exception report will be closed, indicating the exception was resolved.

The interim and final reports will contain logs of all anomalies and exceptions that were detected during the test, including those that have been resolved.

The TDP and Source Code reviews continue even when anomalies are discovered unless the NYBOE directs Ciber to suspend. During Component test, Ciber will terminate testing if it is not possible to complete some of the remaining test steps. Ciber will notify the NYBOE that it is suspending the testing. Testing may resume when there is a resolution that allows the test proceed with the approval and direction of the NYBOE. During system test, an anomaly other than a cosmetic failure will cause testing to suspend and allow the vendor 2 days to correct the problem.

Appendix A: Requirements

The NYBOE has specified that voting systems submitted for this qualification testing are to be evaluated against the requirements and standards specified in the following documents:

1. Election Assistance Commission 2005 Voluntary Voting System Guidelines
2. Subtitle V of Title 9, Part 6209 (Voting System Standards) of the Official Compilation of Codes, Rules and Regulations of the State of New York

Ciber extracted the requirements from those documents and classified flagged each requirement as requiring validation by test (functional requirements), validation by document review (TDP requirement) or validation by source code review (source code requirement). This appendix presents the requirements that were classified in one of the above three categories, grouped by category.

A.1 Functional Requirements

The following requirements will be validated by component and or system integration tests.

Functional Requirements List

Requirement ID	Description
6209.2.A.01	Polling Place Voting System Requirements: A. In order for a polling place voting system to be considered by the State Board for certification, it must comply with the mandates of New York State Election Law, and meet the Election Assistance Commission's 2005 Voluntary Voting System Guidelines to the extent that they are consistent with state law and these regulations. Such polling place voting systems shall meet the following requirements: (1) Provide a full ballot display on a single surface, except that proposals may appear on the reverse side of any paper ballot, and that such ballot display is easily visible under typical lighting found in a poll site.
6209.2.A.02	Polling Place Voting System Requirements: (2) For jurisdictions within the State of New York that have been identified by the U.S. Department of Justice, as requiring that ballots be provided in alternate languages, pursuant to Section 203 of the Voting Rights Act, 42 USC 1973aa-1a. Voting systems must be able to recognize and interpret alternate language ballots.
6209.2.A.03	Polling Place Voting System Requirements: (3) Provide a device that produces and retains a voter-verifiable permanent paper record, pursuant to statute, which the voter can review and/or correct prior to the casting of their vote. In the case of a paper-based voting system, the ballot marked by the voter shall constitute the paper record referred to in Section F. The paper record shall allow a manual audit and allow for preservation in accordance with the provisions of Election Law, Section 3-222.
6209.2.A.04	Polling Place Voting System Requirements: (4) Provide a device or means by which the record of the votes cast on the machine can be printed and visually reviewed after the polls are closed.
6209.2.A.07	Polling Place Voting System Requirements: (7) The system shall incorporate multiple memories, including resident vote tabulation, storage of results and ballot images in resident memory, serving as a redundant means of verifying or auditing election results and ballot images, and further, the system shall be required to alert the election day worker that memory capacity is about to be reached.
6209.2.A.08	Polling Place Voting System Requirements: (8) In a DRE voting system, the system must prevent voters from overvoting and indicate to the voter specific contests or ballot issues for which no selection or an insufficient number of selections has been made. In a paper-based voting system, the system must indicate to the voter specific contests or ballot issues for which an overvote or undervote is detected.
6209.2.A.10	Polling Place Voting System Requirements: (10) The voting system shall be capable of accumulating and reporting a count of the number of ballots tallied for an election district and votes cast for each candidate, and the total vote for or against each ballot proposal, and shall be capable of separating and tabulating those election district totals to produce a report of the total of ballots tallied by groups of election districts such as legislative districts or wards.
6209.2.B.2	Polling Place Voting System Requirements: (2) The voting system or equipment shall be equipped with an audio voting feature, pursuant to Election Law Section 7-202. The audio feature shall be able to be used either independently or simultaneously with the on-screen display.
6209.2.F.1	Polling Place Voting System Requirements: F. Voter Verified Paper Audit Trails (VVPAT) (1) The voting system shall print and display a paper record of the voter's ballot choices prior to the voter making the ballot choices final. In the case of a paper-based voting system, the ballot marked by the voter shall constitute the paper record referred to in this Section F.
6209.2.F.1.a	Polling Place Voting System Requirements: a) The paper record shall constitute a complete record of ballot choices that can be used in audits of the accuracy of the voting systems electronic records, in audits of the election results, and in full recounts.
6209.2.F.1.b	Polling Place Voting System Requirements: (b) In the case of a DRE voting system, the paper record shall contain all information stored in the electronic record.
6209.2.F.1.c	Polling Place Voting System Requirements: (c) The voting system shall be capable of showing the information on both the display screen and the paper in a font size of 3.0mm, and should be capable of showing the information in at least two font ranges, a) 3.0-4.0 mm and b) 6.3-9.0 mm, under control of the voter.
6209.2.F.1.d	Polling Place Voting System Requirements: d) In the case of a DRE voting system, the paper and electronic display of the voter's selections shall be presented and positioned so as to allow the voter to easily read and compare the two.
6209.2.F.1.e	Polling Place Voting System Requirements: (e) If the paper record cannot be displayed in its entirety, a means for moving the paper to show all paper record contents shall be provided.
6209.2.F.10	Polling Place Voting System Requirements: (10) The voting system's ballot records shall be structured and contain information so as to support highly precise audits of their accuracy.
6209.2.F.10.b	Polling Place Voting System Requirements: (b) This information shall contain, but not be limited to, the voting site/election district, type of election, ballot style, and whether the system is operating in a "test" mode.

Functional Requirements List

Requirement ID	Description
6209.2.F.11	Polling Place Voting System Requirements: (11) In the case of a DRE voting system, the electronic and paper records shall be linked by including a unique identifier within each record that can be used to identify each record uniquely and correspond the two accordingly.
6209.2.F.12	Polling Place Voting System Requirements: (12) The voting system shall generate and store a digital signature for each electronic record.
6209.2.F.13	Polling Place Voting System Requirements: (13) The electronic records shall be able to be exported for auditing or analysis on standards-based and/or information technology computing platforms.
6209.2.F.13.a	Polling Place Voting System Requirements: (a) The exported electronic records shall be in an open, non-proprietary format.
6209.2.F.13.b	Polling Place Voting System Requirements: (b) The voting system shall export the records accompanied by a digital signature of the collection of records, which shall be calculated on the entire set of electronic records and their associated digital signatures.
6209.2.F.13.c	Polling Place Voting System Requirements: (c) The voting system vendor shall provide documentation as to the structure of the exported records and how they shall be read and processed by software.
6209.2.F.13.d	Polling Place Voting System Requirements: (d) The vendor shall provide a software program that will display the exported records and such software may include other capabilities, such as providing vote tallies and indications of undervotes.
6209.2.F.14.a	Polling Place Voting System Requirements: (a) The voting system shall communicate with its printers over a standard, publicly documented printer port using a standard communication protocol.
6209.2.F.14.f	Polling Place Voting System Requirements: (f) Prior to the opening of polls on election day, poll workers shall demonstrate that the ballot storage devices are empty. The storage devices shall then be sealed and no further access shall be provided to polling place workers.
6209.2.F.15.d	Polling Place Voting System Requirements: (d) There shall be adequate supplies of consumable items such as paper and printer ink on hand to operate from opening to closing of polls.
6209.2.F.15.d.i	Polling Place Voting System Requirements: (i) Printing devices should contain paper and ink of sufficient capacity so as not to require reloading or opening equipment covers or enclosures and circumvention of security features, or reloading shall be able to be accomplished with minimal disruption to voting and without circumvention of security features such as seals.
6209.2.F.16	Polling Place Voting System Requirements: (16) Vendor documentation shall include procedures for investigating and resolving malfunctions including but not limited to misreporting of votes, unreadable paper records, paper jams, low ink, mis-feeds and power failures.
6209.2.F.2	Polling Place Voting System Requirements: (2) There shall be instructions for performing the verification process made available to the voter in a location on the voting system.
6209.2.F.3	Polling Place Voting System Requirements: (3) The voting system shall display, print, and store a paper record in any of the alternative languages chosen for making ballot selections. Candidate names and other markings not related to the ballot selection on the paper record shall appear in English.
6209.2.F.4	Polling Place Voting System Requirements: (4) The voting system shall allow the voter to approve or reject the paper record, in the case of DRE systems, marking the ballot as such in the presence of the voter.
6209.2.F.4.a	Polling Place Voting System Requirements: (a) Any DRE voting system shall provide a means to reconcile the number of rejected paper records with the number of occurrences of rejected electronic selections, and procedures shall be in place to address any discrepancies.
6209.2.F.4.b	Polling Place Voting System Requirements: (b) Prior to reaching the maximum number of ballots allowed pursuant to statute, any DRE voting system shall display a warning message to the voter indicating the voter may reject only one more ballot, and that the third ballot shall become the ballot of record.
6209.2.F.5	Polling Place Voting System Requirements: (5) In case of conditions that prevent voter review of the paper record, there shall be a means for the voter to notify an election official, and in the case of a DRE voting system, shall cause an error message to be displayed and shall prevent the recording of the electronic record.
6209.2.F.7	Polling Place Voting System Requirements: (7) The voting system shall not record the electronic record as being approved by the voter until the paper record has been stored.
6209.2.F.9	Polling Place Voting System Requirements: (9) The voter's privacy and anonymity shall be preserved during the process of recording, verifying, and auditing ballot choices.

Functional Requirements List

Requirement ID	Description
6209.2.F.9.a	Polling Place Voting System Requirements: (a) The privacy and anonymity of the voter's verification of ballot choices and the creation and storage of these choices, both electronically and on paper record, shall be maintained.
6209.2.F.9.b	Polling Place Voting System Requirements: (b) The privacy and anonymity of voters whose paper records contain any of the alternative languages chosen for making ballots selections shall be maintained.
6209.2.F.9.c	Polling Place Voting System Requirements: (c) Information for the purposes of auditing the electronic or paper records that may permit a voter to reveal his or her ballot choices shall be displayed so as not to be memorable to the voter.
6209.3.A	Additional Requirements for Voting Systems: A. In addition to voting system requirements provided for elsewhere in these rules and regulations, paper-based systems shall:
6209.3.B.1	Additional Requirements for Voting Systems: B. Ballot specifications:(1) As to the printing and arrangement of ballots, all ballots shall meet the requirements as to form and content provided in section 7-121 of the Election Law, and:
6209.3.B.2	Additional Requirements for Voting Systems: (2) ballots shall be printed in black print on a white background or on backgrounds of different colors to identify different types of ballots (i.e., emergency, affidavit, etc) or in the case of a primary, to identify ballots for each political party according to the color assigned to such party pursuant to law, and
6209.3.B.3	Additional Requirements for Voting Systems: (3) coding which is both machine readable and manually readable shall be used to identify different ballot styles, and
6209.3.B.4	Additional Requirements for Voting Systems: (4) ballots used in the paper-based voting system shall be able to be counted by hand as well as be counted by machine, and
6209.3.B.5	Additional Requirements for Voting Systems: (5) The types of ballots used and their form, type size and arrangement must be approved by the State Board of Elections.
6209.3.C.1	Additional Requirements for Voting Systems: C. For all paper-based voting systems, the system shall count a mark on a ballot that is in a:(1) Sensitive Area for a candidate whose name is on the ballot;
6209.3.C.2	Additional Requirements for Voting Systems: (2) Sensitive Area for a candidate whose name is on the ballot;
6209.3.C.3	Additional Requirements for Voting Systems: (3) Sensitive Area for a ballot proposal.
6209.3.D	Additional Requirements for Voting Systems: D. With regard to the central counting of absentee, affidavit, emergency and special ballots, the requirements of 6209.2 (F)(1)(c-e),and (F)(2) not consistent with this section shall not apply.
6209.3.I.A.1	Additional Requirements for Voting Systems: (1) Allow the voter, at their choice, to vote a new ballot or submit the ballot 'as is'.
6209.3.I.A.2	Additional Requirements for Voting Systems: (2) An over-vote in one or more office or ballot proposals shall not prevent the counting of all other offices or ballot proposals contained on the ballot.
6209.3.I.A.3	Additional Requirements for Voting Systems: (3) In the case of candidates who appear on one or more party lines, the system shall be capable of correctly counting the vote according to provisions of Election Law §9-112.
6209.6.A	Examination Criteria: A.Each tested system shall, at a minimum, conform to the EAC's 2005 Voluntary Voting System Guidelines, to the extent that they are consistent with State Law and these Regulations.
6209.6.E.5.b	Examination Criteria: (b) Production models of special purpose data processing equipment (scanners, bar code readers, etc.) having successfully performed in elections use and having been shown to be compatible with the voting system.
Vol I Sec.2.1.1 a	Overall System Capabilities, Security To ensure security, all systems shall: a. Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability.
Vol I Sec.2.1.1 b	Overall System Capabilities, Security b. Provide system functions that are executable only in the intended manner and order, and only under the intended conditions.
Vol I Sec.2.1.1 c	Overall System Capabilities, Security c. Use the system's control logic to prevent a system function from executing if any preconditions to the function have not been met.

Functional Requirements List

Requirement ID	Description
Vol I Sec.2.1.1 d	Overall System Capabilities, Security d. Provide safeguards in response to system failure to protect against tampering during system repair or interventions in system operations.
Vol I Sec.2.1.1 e	Overall System Capabilities, Security e. Provide security provisions that are compatible with the procedures and administrative tasks involved in equipment preparation, testing, and operation.
Vol I Sec.2.1.1 f	Overall System Capabilities, Security f. Incorporate a means of implementing a capability if access to a system function is to be restricted or controlled
Vol I Sec.2.1.10	Overall System Capabilities, Data Retention United States Code Title 42, Sections 1974 through 1974e states that election administrators shall preserve for 22 months "all records and paper that came into (their) possession relating to an application, registration, payment of poll tax, or other act requisite to voting". This retention requirement pertains to systems that will be used at anytime for voting of candidates for Federal offices. Therefore, all systems shall provide for maintaining the integrity of voting and audit data during an election and for a period of at least 22 months afterward. For 22-month document retention, the general rule is that all printed copy records produced by the election database and ballot processing systems shall be so labeled and archived. Regardless of system type, all audit trail information spelled out in Subsection 5.5 shall be retained in its original format, whether that be real-time logs generated by the system, or manual logs maintained by election personnel. The election audit trail includes not only in process logs of election-night and subsequent processing of absentee or provisional ballots, but also time logs of baseline ballot definition formats, and system readiness and testing results
Vol I Sec.2.1.2 a	Accuracy, Common Standards To ensure vote accuracy, all systems shall: a. Record the election contests, candidates, and issues exactly as defined by election officials;
Vol I Sec.2.1.2 b	Accuracy, Common Standards . Record the appropriate options for casting and recording votes;
Vol I Sec.2.1.2 c	Accuracy, Common Standards c. Record each vote precisely as indicated by the voter and produce an accurate report of all votes cast;
Vol I Sec.2.1.2 d	Accuracy, Common Standards d. Include control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) to demonstrate that the system has been designed for accuracy
Vol I Sec.2.1.2 e	Accuracy, Common Standards e. Provide software that monitors the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected.
Vol I Sec.2.1.2 f	Accuracy, DRE System Standards As an additional means of ensuring accuracy in DRE systems, voting devices shall record and retain redundant copies of the original ballot image. A ballot image is an electronic record of all votes cast by the voter, including undervotes.
Vol I Sec.2.1.3 a	Overall System Capabilities, Error Recovery To recover from a non-catastrophic failure of a device, or from any error or malfunction that is within the operator's ability to correct, the system shall provide the following capabilities: a. Restoration of the device to the operating condition existing immediately prior to the error or failure, without the loss or corruption of voting data previously stored in the device;
Vol I Sec.2.1.3 b	Overall System Capabilities, Error Recovery b. Resumption of normal operation following the correction of a failure in a memory component, or in a data processing component, including the central processing unit
Vol I Sec.2.1.3 c	Overall System Capabilities, Error Recovery c. Recovery from any other external condition that causes equipment to become inoperable, provided that catastrophic electrical or mechanical damage due to external phenomena has not occurred.
Vol I Sec.2.1.4 a	Error Recovery, Common Standards To ensure system integrity, all systems shall: a. Protect against a single point of failure that would prevent further voting at the polling place;
Vol I Sec.2.1.4 b	b. Protect against the interruption of electrical power;
Vol I Sec.2.1.4 c	c. Protect against generated or induced electromagnetic radiation;

Functional Requirements List

Requirement ID	Description
Vol I Sec.2.1.4 d	d. Protect against ambient temperature and humidity fluctuations;
Vol I Sec.2.1.4 e	e. Protect against the failure of any data input or storage device;
Vol I Sec.2.1.4 f	f. Protect against any attempt at improper data entry or retrieval;
Vol I Sec.2.1.4 g	g. Record and report the date and time of normal and abnormal events;
Vol I Sec.2.1.4 h	h. Maintain a permanent record of original audit data that cannot be modified or overridden, but may be augmented by designated authorized officials in order to adjust for errors or omissions (e.g. during the canvassing process);
Vol I Sec.2.1.4 I	i. Detect and record every event, including the occurrence of an error condition that the system cannot overcome and time-dependent or programmed events that occur without the intervention of the voter or a polling place operator
Vol I Sec.2.1.4 j	j. Include built-in measurement, self-test, and diagnostic software and hardware for detecting and reporting the system's status and degree of operability.
Vol I Sec.2.1.4 k	Integrity, DRE System Standards In addition to the common standards, DRE systems shall: k. Maintain a record of each ballot cast using a process and storage location that differs from the main vote detection, interpretation, processing, and reporting path
Vol I Sec.2.1.4 l	l. Provide a capability to retrieve ballot images in a form readable by humans.
Vol I Sec.2.1.5.1 (1)	System Audit, Operational Requirements Audit records shall be prepared for all phases of election operations performed using devices controlled by the jurisdiction or its contractors.
Vol I Sec.2.1.5.1 (2)	System Audit, Operational Requirements These records shall address the ballot preparation and election definition phase, system readiness tests, and ballot-counting operations.
Vol I Sec.2.1.5.1 (3)	System Audit, Operational Requirements The software shall activate the logging and reporting of audit data as described in the following sections. [2.1.5.1 a - c)
Vol I Sec.2.1.5.1 a i	Operational Requirements, Time, Sequence, and Preservation of Audit Records a All voting systems shall meet the requirements for time, sequence and preservation of audit records outlined below. i. Except where noted, systems shall provide the capability to create and maintain a real-time audit record.
Vol I Sec.2.1.5.1 a ii 1	
Vol I Sec.2.1.5.1 a ii 2	a ii. All systems shall include a real-time clock as part of the system's hardware. The system shall maintain an absolute record of the time and date or a record relative to some event whose time and data are known and recorded.
Vol I Sec.2.1.5.1 a iii	c. All audit record entries shall include the time-and-date stamp.
Vol I Sec.2.1.5.1 a iv	iv. The audit record shall be active whenever the system is in an operating mode. This record shall be available at all times, though it need not be continually visible.
Vol I Sec.2.1.5.1 a v	v. The generation of audit entries shall not be terminated or altered by program control, or by the intervention of any person. The physical security and integrity of the record shall be maintained at all times.
Vol I Sec.2.1.5.1 a vi	vi. Once the system has been activated for any function, the system shall preserve the contents of the audit record during any interruption of power to the system until processing and data reporting have been completed.
Vol I Sec.2.1.5.1 a vii	vii. The system shall be capable of printing a copy of the audit record. A separate printer is not required for the audit record, and the record may be produced on the standard system printer if all the following conditions are met: 1) The generation of audit trail records does not interfere with the production of output reports; 2) The entries can be identified so as to facilitate their recognition, segregation, and retention; and 3) The audit record entries are kept physically secure.
Vol I Sec.2.1.5.1 b i	b. All voting systems shall meet the following requirements for error messages: i. The system shall generate, store, and report to the user all error messages as they occur;
Vol I Sec.2.1.5.1 b ii	ii. All error messages requiring intervention by an operator or precinct official shall be displayed or printed unambiguously in easily understood language text, or by means of other suitable visual indicators;

Functional Requirements List

Requirement ID	Description
Vol I Sec.2.1.5.1 b iii	iii. When the voting system uses numerical error codes for trained technician maintenance or repair, the text corresponding to the code shall be self-contained, or affixed inside the unit device;
Vol I Sec.2.1.5.1 b iv	iv All error messages for which correction impacts vote recording or vote processing shall be written in a manner that is understandable to an election official who possesses training on system use and operation, but does not possess technical training on system servicing and repair;
Vol I Sec.2.1.5.1 b v	v. The message cue for all systems shall clearly state the action to be performed in the event that voter or operator response is required;
Vol I Sec.2.1.5.1 b vi	f. Voting System design shall ensure that erroneous responses will not lead to irreversible error; and
Vol I Sec.2.1.5.1 b vii	vii. Nested error conditions shall be corrected in a controlled sequence such that system status shall be restored to the initial state existing before the first error occurred.
Vol I Sec.2.1.5.1 c (1)	The voting system shall display and report critical status messages using clear indicators or English language text. The voting system need not display non-critical status messages at the time of occurrence. Voting systems may display non-critical status messages (i.e., those that do not require operator intervention) by means of numerical codes for subsequent interpretation and reporting as unambiguous text.
Vol I Sec.2.1.5.1 c (2)	Operational Requirements, Status Messages Voting Systems shall provide a capability for the status messages to become part of the real-time audit record.
Vol I Sec.2.1.5.1 c (3)	Operational Requirements, Status Messages The system shall provide a capability for a jurisdiction to designate critical status messages.
Vol I Sec.2.1.5.2 (2)	System Audit, COTS General Purpose Computer System Requirements First, authentication shall be configured on the local terminal (display screen and keyboard) and all external connection devices ("network cards" and "ports"). This ensures that only authorized and identified users affect the system while election software is running.
Vol I Sec.2.1.5.2 (3)	System Audit, COTS General Purpose Computer System Requirements Second, operating system audit shall be enabled for all session openings and closings, for all connection openings and closings, for all process executions and terminations, and for the alteration or deletion of any memory or file object. This ensures the accuracy and completeness of election data stored on the system. It also ensures the existence of an audit record of any person or process altering or deleting system data or election data.
Vol I Sec.2.1.5.2 (4)	System Audit, COTS General Purpose Computer System Requirements Third, the system shall be configured to execute only intended and necessary processes during the execution of election software. The system shall also be configured to halt election software processes upon the termination of any critical system process (such as system audit) during the execution of election software.
Vol I Sec.2.1.6 (1)	Overall System Capabilities, Election Management System An EMS [Election Management System] shall generate and maintain a database, or one or more interactive databases, that enables election officials or their designees to perform the following functions: a. Define political subdivision boundaries and multiple election districts as indicated in the system documentation;
Vol I Sec.2.1.6 (2)	b. Identify contests, candidates, and issues;
Vol I Sec.2.1.6 (3)	c. Define ballot formats and appropriate voting actions;
Vol I Sec.2.1.6 (4)	d. Generate ballots and election-specific programs for voting equipment;
Vol I Sec.2.1.6 (5)	e. Install ballots and election-specific programs;
Vol I Sec.2.1.6 (6)	f. Test that ballots and programs have been properly prepared and installed;
Vol I Sec.2.1.6 (7)	g. Accumulate vote totals at multiple reporting levels as indicated in the system documentation;
Vol I Sec.2.1.6 (8)	h. Generate the post-voting reports required by Subsection 2.4
Vol I Sec.2.1.6 (9)	i. Process and produce audit reports of the date indicated in Subsection 5.5
Vol I Sec.2.1.7.1 (1)	Vote Tabulating Program The vote tabulating program software resident in each voting machine, vote count server, or other devices shall include all software modules required to: a. Monitor system status and generate machine-level audit reports;
Vol I Sec.2.1.7.1 (2)	b. Accommodate device control functions performed by polling place officials and maintenance personnel;

Functional Requirements List

Requirement ID	Description
Vol I Sec.2.1.7.1 (3)	c. Register and accumulate votes; and
Vol I Sec.2.1.7.1 (4)	d. Accommodate variations in ballot counting logic.
Vol I Sec.2.1.8 (1)	Overall System Capabilities, Ballot Counter For all voting systems, each device that tabulates ballots shall provide a counter that: a. Can be set to zero before any ballots are submitted for tally;
Vol I Sec.2.1.8 (2)	b. Records the number of ballots cast during a particular test cycle or election;
Vol I Sec.2.1.8 (3)	c. Increases the count only by the input of a ballot;
Vol I Sec.2.1.8 (4)	d. Prevents or disables the resetting of the counter by any person other than authorized persons at authorized points
Vol I Sec.2.1.8 (5)	e. Is visible to designated election officials.
Vol I Sec.2.1.9	Overall System Capabilities, Telecommunications For all voting systems that use telecommunications for the transmission of data during pre-voting, voting, and post-voting activities, capabilities shall be provided that ensure data are transmitted with no alteration or unauthorized disclosure during transmission. Such transmissions shall not violate the privacy, secrecy, and integrity demands of the Guidelines. Section 6 describes telecommunications standards that apply to, at a minimum, the following types of data transmissions: Voter Authentication: Coded information that confirms the identity of a voter for security purposes for a system that transmit votes individually over a public network Ballot Definition: Information that describes to voting equipment the content and appearance of the ballots to be used in an election Vote Transmission to Central Site: For voting systems that transmit votes individually over a public network, the transmission of a single vote to the county (or contractor) for consolidation with other county vote data Vote Count: Information representing the tabulation of votes at any one of several levels: polling place, precinct, or central count List of Voters: A listing of the individual voters who have cast ballots in a specific election
Vol I Sec.2.2	2.2 Pre-voting Capabilities This subsection defines capabilities required to support functions performed prior to the opening of polls. All voting systems shall provide capabilities to support: <ul style="list-style-type: none"> • Ballot preparation • Election programming • Ballot and program installation and control • Readiness testing • Verification at the polling place • Verification at the central counting place The standards also include requirements to ensure compatible interfaces with the ballot definition process and the reporting of election results.
Vol I Sec.2.2.1.1 a	Ballot Preparation, General Capabilities All systems shall be capable of: a. Enabling the automatic formatting of ballots in accordance with the requirements for offices, candidates, and measures qualified to be placed on the ballot for each political subdivision and election district;
Vol I Sec.2.2.1.1 b	b. Collecting and maintaining the following data: i) Offices and their associated labels and instructions; ii) Candidate names and their associated labels; and iii) Issues or measures and their associated text;
Vol I Sec.2.2.1.1 c	c. Supporting the maximum number of potentially active voting positions as indicated in the system documentation;
Vol I Sec.2.2.1.1 d	d. For a primary election, generate ballots that segregate the active voting positions by party affiliation;
Vol I Sec.2.2.1.1 e	e. Generating ballots that contain identifying codes or marks uniquely associated with each format; and
Vol I Sec.2.2.1.1 f	f. Ensuring that vote response fields, selection buttons, or switches properly align with the specific candidate names and/or issues printed on the ballot display, ballot card or sheet, or separate ballot pages.
Vol I Sec.2.2.1.1 g	paper-based systems shall also meet the following requirements applicable to the technology used: g Enable voters to make selections by making a mark in areas designated for this purpose upon each ballot sheet;
Vol I Sec.2.2.1.1 h	c. For marksense systems, ensure that the timing marks align properly with the vote response fields.

Functional Requirements List

Requirement ID	Description
Vol I Sec.2.2.1.2 a	<p>Ballot Preparation, Ballot Formatting All systems shall provide a capability for:</p> <p>a. Creation of newly defined elections;</p>
Vol I Sec.2.2.1.2 b	b. Rapid and error-free definition of elections and their associated ballot layouts;
Vol I Sec.2.2.1.2 c	c. Uniform allocation of space and fonts used for each office, candidate, and contest such that the voter perceives no active voting position be preferred to any other;
Vol I Sec.2.2.1.2 d	d. Simultaneous display of the maximum number of choices for a single contest as indicated by the vendor in the system documentation;
Vol I Sec.2.2.1.2 e	e. Retention of previously defined formats for an election;
Vol I Sec.2.2.1.2 f	f. Prevention of unauthorized modification of any ballot formats
Vol I Sec.2.2.1.2 g	g. Modification by authorized persons of a previously defined ballot format for use in a subsequent election.
Vol I Sec.2.2.1.3	<p>Ballot Preparation, Common Standards The voting system shall provide a means of printing or otherwise generating a ballot display that can be installed in all system voting devices for which it is intended.</p>
Vol I Sec.2.2.1.3 a	<p>Ballot Preparation, Common Standards All voting systems shall provide the capabilities below</p> <p>a. The electronic display or printed document on which the user views the ballot is capable of rendering an image of the ballot in any of the languages required by The Voting Rights Act of 1965, as amended;</p>
Vol I Sec.2.2.1.3 b	b. The electronic display or printed document on which the user views the ballot does not show any advertising or commercial logos of any kind, whether public service, commercial, or political, unless specifically provided for in State law. Electronic displays shall not provide connection to such material through hyperlink; and
Vol I Sec.2.2.1.3 c	c. The ballot conforms to vendor specifications for type of paper stock, weight, size, shape, size and location of punch or mark field used to record votes, folding, bleed through, and ink for printing if paper ballot documents or paper displays are part of the system.
Vol I Sec.2.2.1.3 d	<p>Ballot Preparation, Paper-Based System Standards Vendor documentation for marksense systems shall include specifications for ballot materials to ensure that vote selections are read from only a single ballot at a time, without detection of marks from multiple ballots concurrently (e.g. reading of bleed-through from other ballots).</p>
Vol I Sec.2.2.2 a	<p>Pre-Voting Functions, Election Programming All systems shall provide for the:</p> <p>a. Logical definition of the ballot, including the definition of the number of allowable choices for each office and contest;</p>
Vol I Sec.2.2.2 b	b. Logical definition of political and administrative subdivisions, where the list of candidates or contests varies between polling places;
Vol I Sec.2.2.2 c	c. Exclusion of any contest on the ballot in which the voter is prohibited from casting a ballot because of place of residence, or other such administrative or geographical criteria;
Vol I Sec.2.2.2 d	d. Ability to select from a range of voting options to conform to the laws of the jurisdiction in which the system will be used;
Vol I Sec.2.2.2 e	e. Generation of all required master and distributed copies of the voting program, in conformance with the definition of the ballots for each voting device and polling place, and for each tabulating device.
Vol I Sec.2.2.3	<p>Pre-Voting Functions, Ballot and Program Installation and Control All systems shall provide a means of installing ballots and programs on each piece of polling place or central count equipment in accordance with the ballot requirements of the election and the requirements of the jurisdiction in which the equipment will be used.</p>
Vol I Sec.2.2.3 b	b. A capability for automatically verifying that the software has been properly selected and installed in the equipment or in a programmable memory device and for indicating errors
Vol I Sec.2.2.3 c	c. A capability for automatically validating that software correctly matches the ballot formats that it is intended to process, for detecting errors, and for immediately notifying an election official of detected errors.

Functional Requirements List

Requirement ID	Description
Vol I Sec.2.2.4 a	<p>Readiness Testing, Common Standards</p> <p>All voting systems shall provide the capabilities to:</p> <p>a. Verify that voting machines or vote recording and data processing equipment, precinct count equipment, and central count equipment are properly prepared for an election, and collect data that verifies equipment readiness;</p>
Vol I Sec.2.2.4 b	b. Obtain status and data reports from each set of equipment;
Vol I Sec.2.2.4 c	c. Verify the correct installation and interface of all system equipment;
Vol I Sec.2.2.4 d	d. Verify that hardware and software function correctly;
Vol I Sec.2.2.4 e	e. Generate consolidated data reports at the polling place and higher jurisdictional level
Vol I Sec.2.2.4 f	f. Segregating test data from actual voting data, either procedurally or by hardware/software features.
Vol I Sec.2.2.4 g	<p>Resident test software, external devices, and special purpose test software connected to or installed in voting equipment to simulate operator and voter functions may be used for these tests provided that the following standards are met:</p> <p>g. These elements shall be capable of being tested separately, and shall be proven to be reliable verification tools prior to their use;</p>
Vol I Sec.2.2.4 i	<p>Paper based systems shall:</p> <p>i. Support conversion testing that uses all potential ballot positions as active positions</p>
Vol I Sec.2.2.4 j	j. Support conversion testing of ballots with active position density for systems without pre-designated ballot positions.
Vol I Sec.2.3.1.1.2 b	
Vol I Sec.2.4 (1)	<p>Functional Capabilities, Post Voting Functions</p> <p>All systems shall provide capabilities to accumulate and report results for the jurisdiction and to generate audit trails.</p>
Vol I Sec.2.4 (2)	<p>Functional Capabilities, Post Voting Functions</p> <p>In addition, precinct count systems must provide a means to close the polling place including generating appropriate reports.</p>
Vol I Sec.2.4.1 a	<p>Post-Voting Functions, Closing the Polling Place (Precinct Count)</p> <p>The voting system shall provide the means for:</p> <p>a. Preventing the further casting of ballots once the polling place has closed;</p>
Vol I Sec.2.4.1 b	b. Providing an internal test that verifies that the prescribed closing procedure has been followed, and that the device status is normal
Vol I Sec.2.4.1 c	c. Incorporating a visible indication of system status;
Vol I Sec.2.4.1 d	d. Producing a diagnostic test record that verifies the sequence of events, and indicates that the extraction of voting data has been activated;
Vol I Sec.2.4.1 e	e. Precluding the unauthorized reopening of the polls once the poll closing has been completed for that election
Vol I Sec.2.4.2	<p>Post-Voting Functions, Consolidating Vote Data</p> <p>All systems shall provide a means to consolidate vote data from all polling places, and optionally from all other sources such as absentee ballots, provisional ballots, and voted ballots requiring human review (e.g. write-in votes).</p>
Vol I Sec.2.4.3	<p>Post-Voting Systems, Producing Reports</p> <p>All systems shall be able to create reports summarizing the data on multiple levels.</p>
Vol I Sec.2.4.3 a	<p>Producing Reports, Common Standards</p> <p>All systems shall provide capabilities to:</p> <p>a. Support geographic reporting, which requires the reporting of all results for each contest at the precinct level and additional jurisdictional levels;</p>
Vol I Sec.2.4.3 b	b. Produce a printed report of the number of ballots counted by each tabulator;
Vol I Sec.2.4.3 c	c. Produce a printed report for each tabulator of the results of each contest that includes the votes cast for each selection, the count of undervotes and the count of overvotes;
Vol I Sec.2.4.3 d	d. Produce a consolidated printed report of the results for each contest of all votes cast (including count of ballots from other sources supported by the system as specified by the vendor) that includes the votes cast for each selection, the count of undervotes, and the count of overvotes;

Functional Requirements List

Requirement ID	Description
Vol I Sec.2.4.3 e	e. Be capable of producing a consolidated printed report of the combination of overvotes for any contest that is selected by an authorized official (e.g. the number of overvotes in a given contest by combining Candidate A and Candidate B, combining Candidate A and Candidate C, etc.);
Vol I Sec.2.4.3 f	f. Produce all system audit information required in Section 5.4 in the form of printed reports, or in electronic memory for printing centrally;
Vol I Sec.2.4.3 g	g. Prevent data from being altered or destroyed by report generation, or by the transmission of results over telecommunications lines.
Vol I Sec.2.4.3 h	Producing Reports, Precinct Count Systems In addition to the common reporting requirements, all precinct count voting systems shall: Prevent the printing of reports and the unauthorized extraction of data prior to the official close of the polling place;
Vol I Sec.2.4.3 i	i. Provide a means to extract information from a transportable programmable memory device or data storage medium for vote consolidation;
Vol I Sec.2.4.3 j	j. Consolidate the data contained in each unit into a single report for the polling place when more than one voting machine or precinct tabulator is used;
Vol I Sec.2.4.3 k	d. Prevent data in transportable memory from being altered or destroyed by report generation, or by the transmission of results over telecommunications lines.
Vol I Sec.2.4.4 a	Post-Voting Functions, Broadcasting Results Some voting systems offer the capability to make unofficial results available to external organizations such as the news media, political party officials, and others. Although this capability is not required, systems that make unofficial results available shall: a. Provide only aggregated results, and not data from individual ballots;
Vol I Sec.2.4.4 b	b. Provide no access path from unofficial electronic reports or files to the storage devices for official data; and
Vol I Sec.2.4.4 c	c. Clearly indicate on each report or file that the results it contains are unofficial.
Vol I Sec.3 (1)	Usability and Accessibility Requirements The voting process shall be accessible to individuals with disabilities. The voting process includes access to the polling place, instructions on how to vote, initiating the voting session, making ballot selections, review of the ballot, final submission of the ballot, and getting help when needed NOTE from this Section: Requirements for general usability apply to all voting systems. Requirements for any alternative languages required by state or federal law are included under this heading. • Requirements to assist voters with physical, sensory, or cognitive disabilities apply, as a minimum, to the accessible voting stations required by HAVA Section 301 (a)(3)(B). They may also assist those not usually described as having a disability, e.g., voters with poor eyesight or limited dexterity.
Vol I Sec.3 (2)	Usability and Accessibility Requirements The ballot shall be presented to the voter in a manner that is clear and usable. Voters should encounter no difficulty or confusion regarding the process for recording their selections.
Vol I Sec.3.1 a1Ai	Usability Requirements.-- Each voting system used in an election for federal office shall meet the following requirements: 1. In general.-- A. Except as provided in subparagraph (B), the voting system (including any lever voting system, optical scanning voting system, or direct recording electronic system) shall-- i. Permit the voter to verify (in a private and independent manner) the votes selected by the voter on the ballot before the ballot is cast and counted;
Vol I Sec.3.1 a1Aiiil	iii. If the voter selects votes for more than one candidate for a single office— I. Notify the voter that the voter has selected more than one candidate for a single office on the ballot;
Vol I Sec.3.1 a1Aiiil	II. Notify the voter before the ballot is cast and counted of the effect of casting multiple votes for the office
Vol I Sec.3.1 a1Aiiil	III. Provide the voter with the opportunity to correct the ballot before the ballot is cast and counted

Functional Requirements List

Requirement ID	Description
Vol I Sec.3.1 a1Bi	B. A state or jurisdiction that uses a paper ballot voting system, a punch card voting system, or a central count voting system (including mail-in absentee ballots and mail-in ballots), may meet the requirements of subparagraph (A)(iii) by i. Establishing a voter education program specific to that voting system that notifies each voter of the effect of casting multiple votes for an office; and
Vol I Sec.3.1 a1Bii	ii. Providing the voter with instructions on how to correct the ballot before it is cast and counted (including instructions on how to correct the error through the issuance of a replacement ballot if the voter was otherwise unable to change the ballot or correct any error).
Vol I Sec.3.1 a1C	C. The voting system shall ensure that any notification required under this paragraph preserves the privacy of the voter and the confidentiality of the ballot.
Vol I Sec.3.1.2 a	a. The voting system shall provide feedback to the voter that identifies specific contests or ballot issues for which he or she has made no selection or fewer than the allowable number of selections (e.g., undervotes)
Vol I Sec.3.1.2 b	b. The voting system shall notify the voter if he or she has made more than the allowable number of selections for any contest (e.g., overvotes)
Vol I Sec.3.1.2 c	c. The voting system shall notify the voter before the ballot is cast and counted of the effect of making more than the allowable number of selections for a contest
Vol I Sec.3.1.2 d	d. The voting system shall provide the voter the opportunity to correct the ballot for either an undervote or overvote before the ballot is cast and counted
Vol I Sec.3.1.2 e	e. The voting system shall allow the voter, at his or her choice, to submit an undervoted ballot without correction
Vol I Sec.3.1.2 f	f. DRE voting machines shall allow the voter to change a vote within a contest before advancing to the next contest.
Vol I Sec.3.1.2 g	g. DRE voting machines should provide navigation controls that allow the voter to advance to the next contest or go back to the previous contest before completing a vote on the contest currently being presented (whether visually or aurally).
Vol I Sec.3.1.3	The voting equipment shall be capable of presenting the ballot, ballot selections, review screens and instructions in any language required by state or federal law. Discussion: HAVA Section 301 (a)(4) states that the voting system shall provide alternative language accessibility pursuant to the requirements of section 203 of the Voting Rights Act of 1965 (42 U.S.C. 1973aa-1a). Ideally every voter would be able to vote independently and privately, regardless of language. As a practical matter, alternative language access is mandated under the Voting Rights Act of 1975, subject to certain thresholds, e.g., if the language group exceeds 5% of the voting age population. The audio interface provided for blind voters may also assist voters who speak English, but who are unable to read it (See Subsection 3.2.2.2).
Vol I Sec.3.1.4 a	a. Consistent with election law, the voting system should support a process that does not introduce any bias for or against any of the selections to be made by the voter. In both visual and aural formats, contest choices shall be presented in an equivalent manner. [. . .characteristics such as font size or voice volume and speed must be the same for all choices.]
Vol I Sec.3.1.4 b	b. The voting machine or related materials shall provide clear instructions and assistance to allow voters to successfully execute and cast their ballots independently.
Vol I Sec.3.1.4 bi	Voting machines or related materials shall provide a means for the voter to get help at any time during the voting session. Discussion: The voter should always be able to get help if needed. DRE voting machines may provide this with a distinctive "help" button. Any type of voting equipment may provide written instructions that are separate from the ballot.
Vol I Sec.3.1.4 bii	ii. The voting machine shall provide instructions for all its valid operations. Discussion: If an operation is available to the voter, it must be documented. Examples include how to change a vote, how to navigate among contests, how to cast a straight party vote, and how to cast a write-in vote.
Vol I Sec.3.1.4 c	c. The voting system shall provide the capability to design a ballot for maximum clarity and comprehension.
Vol I Sec.3.1.4 ci	i. The voting equipment should not visually present a single contest spread over two pages or two columns. [. . . If a contest has a large number of candidates, it may be infeasible to observe this guideline.]
Vol I Sec.3.1.4 cii	ii. The ballot shall clearly indicate the maximum number of candidates for which one can vote within a single contest.

Functional Requirements List

Requirement ID	Description
Vol I Sec.3.1.4 ciii	iii. There shall be a consistent relationship between the name of a candidate and the mechanism used to vote for that candidate.
Vol I Sec.3.1.4 d	d. Warnings and alerts issued by the voting system should clearly state the nature of the problem and the set of responses available to the voter. The warning should clearly state whether the voter has performed or attempted an invalid operation or whether the voting equipment itself has malfunctioned in some way.
Vol I Sec.3.1.4 e	e. The use of color by the voting system should agree with common conventions: (a) green, blue or white is used for general information or as a normal status indicator; (b) amber or yellow is used to indicate warnings or a marginal status; (c) red is used to indicate error conditions or a problem requiring immediate attention.
Vol I Sec.3.1.5 b	b. Any aspect of the voting machine that is adjustable by the voter or poll worker, including font size, color, contrast, and audio volume, shall automatically reset to a standard default value upon completion of that voter's session.
Vol I Sec.3.1.5 c	c. If any aspect of a voting machine is adjustable by the voter or poll worker, there shall be a mechanism to reset all such aspects to their default values.
Vol I Sec.3.1.5 e	e. All voting machines using paper ballots should make provisions for voters with poor reading vision. Discussion: Possible solutions include: (a) providing paper ballots in at least two font sizes, 3.0-4.0mm and 6.3-9.0mm and (b) providing a magnifying device.
Vol I Sec.3.1.5 f	f. The default color coding shall maximize correct perception by voters with color blindness.
Vol I Sec.3.1.6 a	a. Voting machines with electronic image displays shall not require page scrolling by the voter.
Vol I Sec.3.1.6 b	b. The voting machine shall provide unambiguous feedback regarding the voter's selection, such as displaying a checkmark beside the selected option or conspicuously changing its appearance.
Vol I Sec.3.1.6 c	c. If the voting machine requires a response by a voter within a specific period of time, it shall issue an alert at least 20 seconds before this time period has expired and provide a means by which the voter may receive additional time.
Vol I Sec.3.1.6 di	d. Input mechanisms shall be designed to minimize accidental activation. i. On touch screens, the sensitive touch areas shall have a minimum height of 0.5 inches and minimum width of 0.7 inches. The vertical distance between the centers of adjacent areas shall be at least 0.6 inches, and the horizontal distance at least 0.8 inches.
Vol I Sec.3.1.6 dii	ii. No key or control on a voting machine shall have a repetitive effect as a result of being held in its active position.
Vol I Sec.3.1.7	The voting process shall preclude anyone else from determining the content of a voter's ballot, without the voter's cooperation.
Vol I Sec.3.1.7.1 a	When deployed according to the installation instructions provided by the vendor, the voting station shall prevent others from observing the contents of a voter's ballot. a. The ballot and any input controls shall be visible only to the voter during the voting session and ballot submission.
Vol I Sec.3.1.7.1 b	b. The audio interface shall be audible only to the voter.
Vol I Sec.3.1.7.1 c	c. As mandated by HAVA 301 (a)(1)(C), the voting system shall notify the voter of an attempted overvote in a way that preserves the privacy of the voter and the confidentiality of the ballot.
Vol I Sec.3.1.7.2 a	Voter anonymity shall be maintained for alternative format ballot presentation. a. No information shall be kept within an electronic cast vote record that identifies any alternative language feature(s) used by a voter.
Vol I Sec.3.1.7.2 b	b. No information shall be kept within an electronic cast vote record that identifies any accessibility feature(s) used by a voter.
Vol I Sec.3.2	Accessibility Requirements voting system shall— (A) be accessible for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation including privacy and independence) as for other voters; (B) satisfy the requirement of subparagraph (A) through the use of at least one direct recording electronic voting system or other voting system equipped for individuals with disabilities at each polling place

Functional Requirements List

Requirement ID	Description
Vol I Sec.3.2.1 a	<p>Accessibility Requirements</p> <p>The voting process shall incorporate the following features that are applicable to all types of disabilities:</p> <p>a. When the provision of accessibility involves an alternative format for ballot presentation, then all information presented to voters including instructions, warnings, error and other messages, and ballot choices shall be presented in that alternative format.</p>
Vol I Sec.3.2.1 c	<p>c. When the primary means of voter identification or authentication uses biometric measures that require a voter to possess particular biological characteristics, the voting process shall provide a secondary means that does not depend on those characteristics.</p>
Vol I Sec.3.2.2	<p>Accessibility Requirements</p> <p>The voting process shall be accessible to voters with visual disabilities.</p>
Vol I Sec.3.2.2.1 a	<p>The accessible voting station shall be accessible to voters with partial vision.</p> <p>a. The vendor shall conduct summative usability tests on the voting system using partially sighted individuals. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification.</p>
Vol I Sec.3.2.2.1 b	<p>b. The accessible voting station with an electronic image display shall be capable of showing all information in at least two font sizes, (a) 3.0-4.0 mm and (b) 6.3-9.0 mm, under control of the voter.</p>
Vol I Sec.3.2.2.1 c	<p>c. An accessible voting station with a monochrome-only electronic image display shall be capable of showing all information in high contrast either by default or under the control of the voter or poll worker. High contrast is a figure-to-ground ambient contrast ratio for text and informational graphics of at least 6:1.</p>
Vol I Sec.3.2.2.1 d	<p>d. An accessible voting station with a color electronic image display shall allow the voter to adjust the color or the figure-to-ground ambient contrast ratio.</p>
Vol I Sec.3.2.2.1 f	<p>f. An accessible voting station using an electronic image display shall provide synchronized audio output to convey the same information as that which is displayed on the screen.</p>
Vol I Sec.3.2.2.2 a	<p>The accessible voting station shall be accessible to voters who are blind.</p> <p>a. The vendor shall conduct summative usability tests on the voting system using individuals who are blind. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification.</p>
Vol I Sec.3.2.2.2 b	<p>b. The accessible voting station shall provide an audio-tactile interface (ATI) that supports the full functionality of the visual ballot interface, as specified in Subsection 2.3.3.</p> <p>Note the necessity of both audio output and tactilely discernible controls for voter input. Full functionality includes at least:</p> <ul style="list-style-type: none"> • Instructions and feedback on initial activation of the ballot (such as insertion of a smart card), if this is normally performed by the voter on comparable voting stations • Instructions and feedback to the voter on how to operate the accessible voting station, including settings and options (e.g., volume control, repetition) • Instructions and feedback for navigation of the ballot • Instructions and feedback for contest choices, including write-in candidates • Instructions and feedback on confirming and changing selections • Instructions and feedback on final submission of ballot
Vol I Sec.3.2.2.2 bi	<p>i. The ATI of the accessible voting station shall provide the same capabilities to vote and cast a ballot as are provided by other voting machines or by the visual interface of the standard voting machine.</p>
Vol I Sec.3.2.2.2 bii	<p>ii. The ATI shall allow the voter to have any information provided by the voting system repeated.</p>
Vol I Sec.3.2.2.2 biii	<p>iii. The ATI shall allow the voter to pause and resume the audio presentation.</p>
Vol I Sec.3.2.2.2 biv	<p>iv. The ATI shall allow the voter to skip to the next contest or return to previous contests.</p>
Vol I Sec.3.2.2.2 bv	<p>v. The ATI shall allow the voter to skip over the reading of a referendum so as to be able to vote on it immediately.</p>
Vol I Sec.3.2.2.2 ci	<p>c. All voting stations that provide audio presentation of the ballot shall conform to the following requirements:</p> <p>i. The ATI shall provide its audio signal through an industry standard connector for private listening using a 3.5mm stereo headphone jack to allow voters to use their own audio assistive devices.</p>
Vol I Sec.3.2.2.2 cii	<p>ii. When a voting machine utilizes a telephone style handset or headphone to provide audio information, it shall provide a wireless T-Coil coupling for assistive hearing devices so as to provide access to that information for voters with partial hearing. That coupling shall achieve at least a category T4 rating as defined by American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19.</p>

Functional Requirements List

Requirement ID	Description
Vol I Sec.3.2.2.2 cviii	viii. The audio presentation of verbal information should be readily comprehensible by voters who have normal hearing and are proficient in the language. This includes such characteristics as proper enunciation, normal intonation, appropriate rate of speech, and low background noise. Candidate names should be pronounced as the candidate intends.
Vol I Sec.3.2.2.2 cw	ix. The audio system shall allow voters to control the rate of speech. The range of speeds supported should be at least 75% to 200% of the nominal rate.
Vol I Sec.3.2.2.2 d	d. If the normal procedure is to have voters initialize the activation of the ballot, the accessible voting station shall provide features that enable voters who are blind to perform this activation.
Vol I Sec.3.2.2.2 e	e. If the normal procedure is for voters to submit their own ballots, then the accessible voting station shall provide features that enable voters who are blind to perform this submission.
Vol I Sec.3.2.3 a	The voting process shall be accessible to voters who lack fine motor control or use of their hands. a. The vendor shall conduct summative usability tests on the voting system using individuals lacking fine motor control. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification.
Vol I Sec.3.2.5 a	The voting process shall be accessible to voters with hearing disabilities. a. The accessible voting station shall incorporate the features listed under requirement 3.2.2.2 (c) for voting equipment that provides audio presentation of the ballot to provide accessibility to voters with hearing disabilities.
Vol I Sec.3.2.5 b	b. If voting equipment provides sound cues as a method to alert the voter, the tone shall be accompanied by a visual cue, unless the station is in audio-only mode.
Vol I Sec.3.2.7	For voters who lack proficiency in reading English, or whose primary language is unwritten, the voting equipment shall provide spoken instructions and ballots in the preferred language of the voter, consistent with state and federal law. The requirements of 3.2.2.2 (c) shall apply to this mode of interaction.
Vol I Sec.3.2.8	The voting process should be accessible to voters with cognitive disabilities. Discussion: At present there are no design features specifically aimed at helping those with cognitive disabilities. Requirements 3.2.2.1 (f), the synchronization of audio with the screen in a DRE, is helpful for some cognitive disabilities such as dyslexia. Requirements in Subsection 3.1.4 also address cognitive issues relative to voting system usability.
Vol I Sec.4.1.3.1	Election Management System (EMS) Requirements, Recording Requirements Voting systems shall accurately record all election management data entered by the user, including election officials or their designees.
Vol I Sec.4.1.3.1 a	Election Management System (EMS) Requirements, Recording Requirement For recording accuracy, all systems shall: a. Record every entry made by the user;
Vol I Sec.4.1.3.1 b	b. Add permissible voter selections correctly to the memory components of the device;
Vol I Sec.4.1.3.1 c	c. Verify the correctness of detection of the user selections and the addition of the selections correctly to memory;
Vol I Sec.4.1.3.1 d	d. Add various forms of data entered directly by the election official or designee, such as text, line art, logos, and images;
Vol I Sec.4.1.3.1 e	e. Verify the correctness of detection of data entered directly by the user and the addition of the selections correctly to memory;
Vol I Sec.4.1.3.1 g	g. Log corrected data errors by the system.
Vol I Sec.4.1.4.3 bv	v. Provide a capability to retrieve ballot images in a form readable by humans;
Vol I Sec.4.1.4.3 bvi	vi. Ensure that all processing and storage protects the anonymity of the voter.
Vol I Sec.4.1.4.3 ci	DRE System Recording Requirements, Recording Accuracy DRE systems shall meet the following requirements for recording accurately each vote and ballot cast: a. Detect every selection made by the voter;
Vol I Sec.4.1.4.3 cii	ii. Correctly add permissible selections to the memory components of the device;
Vol I Sec.4.1.4.3 ciii	c. Verify the correctness of detection of the voter selections and the addition of the selections correctly to memory;
Vol I Sec.4.1.4.3 cvi	f. Maintain a log of corrected data.

Functional Requirements List

Requirement ID	Description
Vol I Sec.4.1.5.1 bi	<p>Exception Handling (Central Count)</p> <p>This requirement refers to the handling of ballots for a central count system when they are unreadable or when some condition is detected requiring that the cards be segregated from normally processed ballots for human review. In response to an unreadable ballot or a write-in vote all central count paper-based systems shall:</p> <p>i. Outstack the ballot, or</p>
Vol I Sec.4.1.5.1 bii	<p>ii. Stop the ballot reader and display a message prompting the election official or designee to remove the ballot, or</p>
Vol I Sec.4.1.5.1 biii	<p>ii. Mark the ballot with an identifying mark to facilitate its later identification.</p>
Vol I Sec.4.1.5.1 c	<p>Exception Handling (Central Count)</p> <p>Additionally, the system shall provide a capability that can be activated by an authorized election official to identify ballots containing overvotes, blank ballots, and ballots containing undervotes in a designated race. If enabled, these capabilities shall perform one of the above actions in response to the indicated condition.</p>
Vol I Sec.4.1.5.1 di	<p>Ballot Handling, Exception Handling (Precinct Count)</p> <p>d. When ballots are unreadable or when some condition is detected requiring that the cards be segregated from normally processed ballots for human review (e.g. write-in votes) all precinct count systems shall:</p> <p>i. In response to an unreadable or blank ballot, return the ballot and provide a message prompting the voter to examine the ballot</p>
Vol I Sec.4.1.5.1 dii	<p>b. In response to a ballot with a write-in vote, segregate the ballot or mark the ballot with an identifying mark to facilitate its later identification;</p>
Vol I Sec.4.1.5.1 diii	<p>c. In response to a ballot with an overvote the system shall:</p> <ol style="list-style-type: none"> 1) Provide a capability to identify an overvoted ballot; 2) Return the ballot; 3) Provide an indication prompting the voter to examine the ballot; 4) Allow the voter to submit the ballot with the overvote; and 5) Provide a means for an authorized election official to deactivate this capability entirely and by contest
Vol I Sec.4.1.5.1 div	<p>d. In response to a ballot with an undervote the system shall:</p> <ul style="list-style-type: none"> -) Provide a capability to identify an undervoted ballot; -) Return the ballot; -) Provide an indication prompting the voter to examine the ballot; -) Allow the voter to correct the ballot -) Allow the voter to submit the ballot with the undervote -) Provide a means for an authorized election official to deactivate this capability.
Vol I Sec.4.1.5.1 ei	<p>Ballot Handling, Multiple Feed Prevention</p> <p>e. Ballot readers shall prevent multiple feed or detect and provide an alarm indicating multiple feed. Multiple feed occurs when a ballot reader attempts to read more than one ballot at a time.</p> <p>i. If multiple feed is detected, the card reader shall halt in a manner that permits the operator to remove the unread cards causing the error, and reinsert them in the card input hopper.</p>
Vol I Sec.4.1.6.2 ai	<p>DRE System Processing Requirements, Processing Speed</p> <p>DRE voting systems shall meet the following requirements for processing speed:</p> <p>i. Operate at a speed sufficient to respond to any operator and voter input without perceptible delay (no more than three seconds);</p>
Vol I Sec.4.1.6.2 aiii	<p>ii. If the consolidation of polling place data is done locally, perform this consolidation in a time not to exceed five minutes for each device in the polling place.</p>
Vol I Sec.4.1.6.2 bi	<p>DRE System Processing Requirements, Processing Accuracy</p> <p>DRE voting systems shall:</p> <p>i. Produce reports that are completely consistent, with no discrepancy among reports of voting device data produced at any level; and</p>
Vol I Sec.4.1.6.2 bii	<p>b. Produce consolidated reports containing absentee, provisional, or other voting data that are similarly error-free. Any discrepancy, regardless of source, is resolvable to a procedural error, to the failure of a non-memory device, or to an external cause.</p>
Vol I Sec.4.1.8	<p>Hardware Standards, Vote Data Management Requirements</p> <p>The vote data management requirements for all systems address capabilities that manage, process, and report voting data after the data has been consolidated at the polling place or other jurisdictional levels. These capabilities allow the system to:</p> <ol style="list-style-type: none"> a. Consolidate vote data from polling place data memory or transfer devices; b. Report polling place summaries; and c. Process absentee ballots, data entered manually, and administrative ballot definition data. <p>The requirements address all hardware and software required to generate output reports in the various formats required by the using jurisdiction.</p>

Functional Requirements List

Requirement ID	Description
Vol I Sec.4.1.8.1	<p>Vote Data Management Requirements, Data File Management</p> <p>All voting systems shall provide the capability to:</p> <ul style="list-style-type: none"> a. Integrate voting data files with ballot definition files; b. Verify file compatibility; and c. Edit and update files as required.
Vol I Sec.4.1.8.2	<p>Vote Data Management Requirements, Data Report Generation</p> <p>All voting systems shall include report generators for producing output reports at the device, polling place, and summary level, with provisions for administrative and judicial subdivisions as required by the using jurisdiction.</p>
Vol I Sec.5.4	<p>Software Standards, Audit Record Data</p> <p>The audit record data in the following subsections are essential to the complete recording of election operations and reporting of the vote tally. This list of audit records may not reflect the design constructs of some systems. Therefore, vendors shall supplement it with information relevant to the operation of their specific systems.</p>
Vol I Sec.5.4.1	<p>Audit Record Data, Pre-election Audit Records</p> <p>During election definition and ballot preparation, the system shall audit the preparation of the baseline ballot formats and modifications to them, a description of these modifications, and corresponding dates.</p>
Vol I Sec.5.4.1 a	<p>Audit Record Data, Pre-election Audit Records</p> <p>The log shall include:</p> <ul style="list-style-type: none"> a. The allowable number of selections for an office or issue;
Vol I Sec.5.4.1 b	<ul style="list-style-type: none"> b. The combinations of voting patterns permitted or required by the jurisdiction;
Vol I Sec.5.4.1 c	<ul style="list-style-type: none"> c. The inclusion or exclusion of offices or issues as the result of multiple districting within the polling place;
Vol I Sec.5.4.1 d	<ul style="list-style-type: none"> d. Any other characteristics that may be peculiar to the jurisdiction, the election, or the polling places; location;
Vol I Sec.5.4.1 e	<ul style="list-style-type: none"> e. Manual data maintained by election personnel;
Vol I Sec.5.4.1 f	<ul style="list-style-type: none"> f. Samples of all final ballot formats
Vol I Sec.5.4.1 g	<ul style="list-style-type: none"> g. Ballot preparation edit listings.
Vol I Sec.5.4.2 a	<p>Audit Record Data, System Readiness Audit Records</p> <p>The following minimum requirements apply to system readiness audit records:</p> <ul style="list-style-type: none"> a. Prior to the start of ballot counting, a system process shall verify hardware and software status and generate a readiness audit record. This record shall include the identification of the software release, the identification of the election to be processed, and the results of the software and hardware diagnostic tests;
Vol I Sec.5.4.2 b	<ul style="list-style-type: none"> b. In the case of systems used at the polling place, the record shall include the polling place's identification;
Vol I Sec.5.4.2 c	<ul style="list-style-type: none"> c. The ballot interpretation logic shall test and record the correct installation of ballot formats on voting devices;
Vol I Sec.5.4.2 d	<ul style="list-style-type: none"> d. The software shall check and record the status of all data paths and memory locations to be used in vote recording to protect against contamination of voting data;
Vol I Sec.5.4.2 e	<ul style="list-style-type: none"> e. Upon the conclusion of the tests, the software shall provide evidence in the audit record that test data have been expunged;
Vol I Sec.5.4.2 f	<ul style="list-style-type: none"> f. If required and provided, the ballot reader and arithmetic-logic unit shall be evaluated for accuracy, and the system shall record the results. It shall allow the processing, or simulated processing, of sufficient test ballots to provide a statistical estimate of processing accuracy
Vol I Sec.5.4.2 g.	<ul style="list-style-type: none"> g. For systems that use a public network, provide a report of test ballots that includes: <ul style="list-style-type: none"> i) Number of ballots sent; ii) When each ballot was sent; iii) Machine from which each ballot was sent; and iv) Specific votes or selections contained in the ballot.
Vol I Sec.5.4.3 ai	<p>Audit Record Data, In-Process Audit Records</p> <p>At a minimum, the in-process audit records shall contain:</p> <ul style="list-style-type: none"> a. Machine generated error and exception messages to demonstrate successful recovery. Examples include, but are not necessarily limited to: <ul style="list-style-type: none"> i) The source and disposition of system interrupts resulting in entry into exception handling routines;
Vol I Sec.5.4.3 aii	<ul style="list-style-type: none"> a. ii) All messages generated by exception handlers;
Vol I Sec.5.4.3 aiii	<ul style="list-style-type: none"> a. iii) The identification code and number of occurrences for each hardware and software error or failure;

Functional Requirements List

Requirement ID	Description
Vol I Sec.5.4.3 aiv	a .iv) Notification of system login or access errors, file access errors, and physical violations of security as they occur, and a summary record of these events after processing;
Vol I Sec.5.4.3 av	a. 5) Other exception events such as power failures, failure of critical hardware components, data transmission errors, or other type of operating anomaly;
Vol I Sec.5.4.3 bi	Audit Record Data, In-Process Audit Records Critical system status messages other than informational messages displayed by the system during the course of normal operations. These items include, but are not limited to 1) Diagnostic and status messages upon startup;
Vol I Sec.5.4.3 bii	b. 2) The "zero totals" check conducted before open the polling place or counting a precinct centrally;
Vol I Sec.5.4.3 biii	b. 3) For paper-based systems, the initiation or termination of card reader and communications equipment operation; and
Vol I Sec.5.4.3 biv	b. 4) For DRE machines at controlled voting locations, the event (and time, if available) of activating and casting each ballot (i.e. each voter's transaction as an event).
Vol I Sec.5.4.3 c	c. Non-critical status messages that are generated by the machine's data quality monitor or by software and hardware condition monitors; and
Vol I Sec.5.4.3 d	d. System generated log of all normal process activity and system events that require operator intervention, so that each operator's access can be monitored and access sequence can be constructed.
Vol I Sec.5.4.4 a	Audit Record Data, Vote Tally Data Voting systems shall meet these [audit] reporting requirements by providing software capable of obtaining data concerning various aspects of vote counting and producing report of them on a printer. At a minimum, vote tally data shall include: a. Number of ballots cast, using each ballot configuration, by tabulator, by precinct, and by political subdivision;
Vol I Sec.5.4.4 b	b. Candidate and measure vote totals for each contest, by tabulator;
Vol I Sec.5.4.4 c	c. The number of ballots read within each precinct and for additional jurisdictional levels, by configuration, including separate totals for each party in primary elections;
Vol I Sec.5.4.4 d	d. Separate accumulation of overvotes and undervotes for each contest, by tabulator, precinct and for additional jurisdictional levels (no overvotes would be indicated for DRE voting devices);
Vol I Sec.5.4.4 e	e. For paper-based systems only, the total number of ballots both processed and unprocessable; and if there are multiple card ballots, the total of cards read.
Vol I Sec.5.4.4 f	Audit Record Data, Vote Tally Data For systems that produce an electronic file containing vote tally data, the contents of the file shall include the same minimum data cited above for printed vote tally reports.
Vol I Sec.5.5 a	Software Standards, Vote Secrecy (DRE Systems) All DRE systems shall ensure vote secrecy by: a. Immediately after the voter chooses to cast his or her ballot, record the voter's selections in the memory to be used for vote counting and audit data (including ballot images) and erase the selections from the display, memory, and all other storage, including all forms of temporary storage; and
Vol I Sec.5.5 b	b. Immediately after the voter chooses to cancel his or her ballot, erase the selections from the display and all other storage, including buffers and other temporary storage.
Vol I Sec.7.2.1.1 c	c. Permit the voter to cast a ballot expeditiously, but preclude voter access to all other aspects of the vote-counting processes.
Vol I Sec.7.4.1 a	Security Standards, Software and Firmware Installation The system shall meet the following requirements for installation of software, including hardware with imbedded firmware: a. If software is resident in the system as firmware, the vendor shall require and state in the system documentation that every device is to be retested to validate each ROM prior to the start of elections operations;
Vol I Sec.7.4.1 b	b. To prevent alteration of executable code, no software shall be permanently installed ore resident in the system unless the system documentation states that the jurisdiction must provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of the system hardware;
Vol I Sec.7.4.1 c	c. The system bootstrap, monitor, and device-controller software may be resident permanently as firmware, provided that this firmware has been shown to be inaccessible to activation or control by any means other than by the authorized initiation and execution of the vote-counting program, and its associated exception handlers;

Functional Requirements List

Requirement ID	Description
Vol I Sec.7.4.1 d	d. The election-specific programming may be installed and resident as firmware, provided that such firmware is installed on a component (such as a computer chip) other than the component on which the operating system resides;
Vol I Sec.7.4.1 e	e. After initiation of election day testing, no source code or compilers or assemblers shall be resident or accessible.
Vol I Sec.7.4.2 (1)	Security Standards, Protection Against Malicious Software Voting systems shall deploy protection against the many forms of threats to which they may be exposed such as file and macro viruses, worms, Trojan horses, and logic bombs.
Vol I Sec.7.4.4 bii	ii. The record of the source code and executable files shall be made on unalterable storage media. Each piece of media shall have a unique identifier.
Vol I Sec.7.4.4 e	e. The voting system equipment shall be designed to allow the voting system administrator to verify that the software is the certified software by comparing it to reference information produced by the NSRL or other designated repository.
Vol I Sec.7.4.6 a	Software Setup Validation a. Setup validation methods shall verify that no unauthorized software is present on the voting equipment.
Vol I Sec.7.4.6 b	b. The vendor shall have a process to verify that the correct software is loaded, that there is no unauthorized software, and that voting system software on voting equipment has not been modified, using the reference information from the NSRL or from a State designated repository.
Vol I Sec.7.4.6 bi	i. The process used to verify software should be possible to perform without using software installed on the voting system.
Vol I Sec.7.4.6 biii	iii. The process shall not modify the voting system software on the voting system during the verification process.
Vol I Sec.7.4.6 c	c. The vendor shall provide a method to comprehensively list all software files that are installed on voting systems.
Vol I Sec.7.4.6 d	d. The verification process should be able to be performed using COTS software and hardware available from sources other than the voting system vendor.
Vol I Sec.7.4.6 di	i. If the process uses hashes or digital signatures, then the verification software shall use a FIPS 140-2 level 1 or higher validated cryptographic module.
Vol I Sec.7.4.6 dii	ii. The verification process shall either (a) use reference information on unalterable storage media received from the repository or (b) verify the digital signature of the reference information on any other media.
Vol I Sec.7.4.6 e	e. Voting system equipment shall provide a means to ensure that the system software can be verified through a trusted external interface, such as a read-only external interface, or by other means.
Vol I Sec.7.4.6 ei	i. The external interface shall be protected using tamper evident techniques
Vol I Sec.7.4.6 eii	ii. The external interface shall have a physical indicator showing when the interface is enabled and disabled
Vol I Sec.7.4.6 eiii	iii. The external interface shall be disabled during voting
Vol I Sec.7.4.6 eiv	iv. The external interface should provide a direct read-only access to the location of the voting system software without the use of installed software
Vol I Sec.7.4.6 f	f. Setup validation methods shall verify that registers and variables of the voting system equipment contain the proper static and initial values.
Vol I Sec.7.4.6 fi	i. The vendor should provide a method to query the voting system to determine the values of all static and dynamic registers and variables including the values that jurisdictions are required to modify to conduct a specific election.
Vol I Sec.7.5.1	Telecommunications and Data Transmission, Access Control Voting systems that use telecommunications to communicate between system components and locations are subject to the same security requirements governing access to any other system hardware, software, and data function.
Vol I Sec.7.5.1 a (1)	Telecommunications and Data Transmission, Data Integrity Voting systems that use electrical or optical transmission of data shall ensure the receipt of valid vote records is verified at the receiving station. This should include standard transmission error detection and correction methods such as checksums or message digest hashes.

Functional Requirements List

Requirement ID	Description
Vol I Sec.7.5.1 a (2)	<p>Telecommunications and Data Transmission, Data Integrity Verification of correct transmission shall occur at the voting system application level and ensure that the correct data is recorded on all relevant components consolidated within the polling place prior to the voter completing casting of his or her ballot.</p>
Vol I Sec.7.5.1 bi	<p>Telecommunications and Data Transmission, Data Interception Prevention Voting systems that use telecommunications to communicate between system components and locations before the poll site is officially closed shall:</p> <p>a. Implement an encryption standard currently documented and validated for use by an agency of the U.S. Federal Government; and</p>
Vol I Sec.7.5.1 bii	<p>b. Provide a means to detect the presence of an intrusive process, such as an Intrusion Detection System.</p>
Vol I Sec.7.5.2 a	<p>Telecommunications and Data Transmission, Protection Against External Threats Voting systems that use public telecommunications networks shall implement protections against external threats to which commercial products used in the system may be susceptible.</p>
Vol I Sec.7.5.2 ci	<p>Protection Against External Threats, Use of Protective Software Voting systems that use public telecommunications networks shall use protective software at the receiving-end of all communication paths to:</p> <p>a. Detect the presence of a threat in a transmission;</p>
Vol I Sec.7.5.2 cii	<p>b. Remove the threat from infected files/data;</p>
Vol I Sec.7.5.2 ciii	<p>c. Prevent against storage of the threat anywhere on the receiving device;</p>
Vol I Sec.7.5.2 civ	<p>d. Provide the capability to confirm that no threats are stored in system memory and in connected storage media; and</p>
Vol I Sec.7.5.2 cv	<p>e. Provide data to the system audit log indicating the detection of a threat and the processing performed.</p>
Vol I Sec.7.5.2 d	<p>d. Vendors shall use multiple forms of protective software as needed to provide capabilities for the full range of products used by the voting system.</p>
Vol I Sec.7.5.4	<p>Telecommunications and Data Transmission, Shared Operating Environment If ballot recording and vote counting operations are performed in an environment that is shared with other data processing functions, both hardware and software features shall be present to protect the integrity of vote counting and of vote data.</p>
Vol I Sec.7.5.4 a	<p>Telecommunications and Data Transmission, Shared Operating Environment Systems that use a shared operating environment shall:</p> <p>a. Use security procedures and logging records to control access to system functions;</p>
Vol I Sec.7.5.4 b	<p>b. Partition or compartmentalize voting system functions from other concurrent functions at least logically, and preferably physically as well;</p>
Vol I Sec.7.5.4 c	<p>c. Controlled system access by means of passwords, and restriction of account access to necessary functions only; and</p>
Vol I Sec.7.5.4 d	<p>d. Have capabilities in place to control the flow of information, precluding data leakage through shared system resources.</p>
Vol I Sec.7.5.5 a	<p>Telecommunications and Data Transmission, Access to Incomplete Election Returns and Interactive Queries If the voting system provides access to incomplete election returns and interactive inquiries before the completion of the official count, the system shall:</p> <p>a. Be designed to provide external access to incomplete election returns (for equipment that operates in a central counting environment) only if that access for these purposes is authorized by the statutes and regulations of the using agency. This requirement applies as well to polling place equipment that contains a removable memory module, or that may be removed in its entirety to a central place for the consolidation of polling place returns.</p>
Vol I Sec.7.5.5 b	<p>b. Design voting system software and its security environment such that data accessible to interactive queries resides in an external file, or database, that is created and maintained by the elections software under the restrictions applying to any other output report, namely, that:</p> <p>i. The output file or database has no provision for write-access back to the system.</p> <p>li. Persons whose only authorized access is to the file or database are denied write-access, both to the file or database, and to the system.</p>
Vol I Sec.7.6.1 a	<p>Security for Transmission of Official Data Over Public Communications Networks, General Security Requirements for Systems Transmitting Data Over Public Networks All systems that transmit data over public telecommunications networks shall:</p> <p>a. Preserve the secrecy of a voter's ballot choices, and prevent anyone from violating ballot privacy;</p>

Functional Requirements List

Requirement ID	Description
Vol I Sec.7.6.1 b	b. Employ digital signature for all communications between the vote server and other devices that communicate with the server over the network
Vol I Sec.7.6.1 c	c. Require that at least two authorized election officials activate any critical operation regarding the processing of ballots transmitted over a public communications network takes place, i.e. passwords or cryptographic keys of at least two employees are required to perform processing of votes.
Vol I Sec.7.6.2	Systems designed for transmission of telecommunications over public networks shall meet security standards that address the security risks attendant with the casting of ballots from polling places controlled by election officials using voting devices configured and installed by election officials and/or their vendor or contractor, and using in-person authentication of individual voters.
Vol I Sec.7.6.2.2 a	<p>Ability to Operate During Interruption of Service</p> <p>These systems shall provide the following capabilities to provide resistance to interruptions of telecommunications service communicating with external components via telecommunications:</p> <p>a. Detect the occurrence of a telecommunications interruption at the polling place and switch to an alternative mode of operation that is not dependent on the connection between polling place voting devices and external system components</p>
Vol I Sec.7.6.2.2 b	b. Provide an alternate mode of operation that includes the functionality of a conventional electronic voting system without losing any single vote
Vol I Sec.7.6.2.2 c	c. Create and preserve an audit trail of every vote cast during the period of interrupted communication and system operation in conventional electronic voting system mode
Vol I Sec.7.6.2.2 d	d. Upon reestablishment of communications, transmit and process votes accumulated while operating in conventional electronic voting system mode with all security safeguards in effect
Vol I Sec.7.6.2.2 e	e. Ensure that all safeguards related to voter identification and authentication are not affected by the procedures employed by the system to counteract potential interruptions of telecommunications capabilities
Vol I Sec.7.7.1 aii	ii. A complete description of the vulnerabilities associated with this proposed use of wireless, including vulnerabilities deriving from the insertion, deletion, modification, capture or suppression of wireless messages
Vol I Sec.7.7.1 aiii	iii. A complete description of the techniques used to mitigate the risks associated with the described vulnerabilities including techniques used by the vendor to ensure that wireless cannot send or receive messages other than those situations specified in the documentation. Cryptographic techniques shall be carefully and fully described, including a description of cryptographic key generation, management, use, certification, and destruction
Vol I Sec.7.7.1 aiv	iv. A rationale for the inclusion of wireless in the proposed voting system, based on a careful and complete description of the perceived advantages and disadvantages of using wireless for the documented uses compared to using non-wireless approaches
Vol I Sec.7.7.1 e	<p>e. If a voting system includes wireless capabilities, then the voting system shall be able to accomplish the same function if wireless capabilities are not available due to an error or no service.</p> <p>i. The vendor shall provide documentation how to accomplish these functions when wireless is not available.</p>
Vol I Sec.7.7.1 f	f. The system shall be designed and configured so it is not vulnerable to a single point of failure using wireless communications that causes a total loss of any voting capabilities.
Vol I Sec.7.7.1 g	g. If a voting system includes wireless capabilities, then the system shall have the ability to turn on the wireless capability when it is to be used and to turn off the wireless capability when the wireless capability is not in use.
Vol I Sec.7.7.1 h	h. If a voting system includes wireless capabilities, then the system shall not activate the wireless capabilities without confirmation from an elections official.
Vol I Sec.7.7.2 a	a. If a voting system provides wireless communications capabilities, then there shall be a method for determining the existence of the wireless communications capabilities.
Vol I Sec.7.7.2 b	b. If a voting system provides wireless communications capabilities, then there shall be an indication that allows one to determine when the wireless communications (such as radio frequencies) capability is active.
Vol I Sec.7.7.2 c	c. The indication shall be visual.
Vol I Sec.7.7.3 a	<p>a. All information transmitted via wireless communications shall be encrypted and authenticated--with the exception of wireless T-coil coupling--to protect against eavesdropping and data manipulation including modification, insertion, and deletion.</p> <p>i. The encryption shall be as defined in Federal Information Processing Standards (FIPS) 197, "Advanced Encryption Standard (AES).</p> <p>ii. The cryptographic modules used shall comply with FIPS 140-2, Security Requirements for Cryptographic Modules.</p>

Functional Requirements List

Requirement ID	Description
Vol I Sec.7.7.3 b	b. The capability to transmit non-encrypted and non-authenticated information via wireless communications shall not exist.
Vol I Sec.7.7.3 c	c. If audible wireless communication is used, and the receiver of the wireless transmission is the human ear, then the information shall not be encrypted.
Vol I Sec.7.7.4 a	If wireless communications are used, then the following capabilities shall exist in order to mitigate the effects of a denial of service (DoS) attack: a. The voting system shall be able to function properly throughout a DoS attack, since the DoS attack may continue throughout the voting period.
Vol I Sec.7.7.4 b	b. The voting system shall function properly as if the wireless capability were never available for use.
Vol I Sec.7.7.4 c	c. Alternative procedures or capabilities shall exist to accomplish the same functions that the wireless communications capability would have done.
Vol I Sec.7.7.4 d	d. If infrared is being used, the shielding shall be strong enough to prevent escape of the voting system signal, as well as strong enough to prevent infrared saturation jamming.
Vol I Sec.7.7.5 a	a. The security requirements in Subsection 2.1.1 shall be applicable to systems with wireless communications.
Vol I Sec.7.7.5 b	b. The accuracy requirements in Subsection 2.1.2 shall be applicable to systems with wireless communications.
Vol I Sec.7.7.5 c	c. The use of wireless communications that may cause impact to the system accuracy through electromagnetic stresses is prohibited.
Vol I Sec.7.7.5 d	d. The error recovery requirements in Subsection 2.1.3 shall be applicable to systems with wireless communications.
Vol I Sec.7.7.5 f	f. Device authentication shall occur before any access to, or services from, the voting system are granted through wireless communications. i. User authentication shall be at least level 2 as per NIST Special Publication 800-63 Version 1.0.1, Electronic Authentication Guideline.
Vol I Sec.7.9	This section contains requirements for DREs with a Voter Verifiable Paper Audit Trail (VVPAT) component. VVPAT capability is not required for national certification. However, these requirements will be applied for certification testing of DRE systems that are intended for use in states that require DREs to provide this capability. The vendor's certification testing application to the EAC must indicate whether the system being presented for testing includes this capability, as provided under Subsection 1.6.2.5 extensions.
Vol I Sec.7.9.1 a	Display and Print a Paper Record a. The voting system shall print and display a paper record of the voter ballot selections prior to the voter making his or her selections final by casting the ballot.
Vol I Sec.7.9.1 b	b. The paper record shall constitute a complete record of ballot selections that can be used to assess the accuracy of the voting machine's electronic record, to verify the election results, and, if required by state law, in full recounts.
Vol I Sec.7.9.1 c	c. The paper record shall contain all voter selection information stored in the electronic (ballot image) record.
Vol I Sec.7.9.2 a	a. The voting equipment shall allow the voter to approve or void the paper record.
Vol I Sec.7.9.2 b	b. The voting equipment shall, in the presence of the voter, mark the paper record as being approved by the voter if the ballot selections are accepted; or voided or if the voter decides to change one or more selections.
Vol I Sec.7.9.2 c	c. If the records do not match, the voting equipment shall mark and preserve the paper record and shall provide a means to preserve the corresponding electronic record so the source of error or malfunction can be analyzed.
Vol I Sec.7.9.2 d	d. The voting machine shall not record the electronic record until the paper record has been approved by the voter.
Vol I Sec.7.9.2 e	e. Vendor documentation shall include procedures to enable the election official to return a voting machine to correct operation after a voter has used it incompletely or incorrectly. This procedure shall not cause discrepancies between the tallies of the electronic and paper records.
Vol I Sec.7.9.3 bi	b. The electronic ballot image and paper records shall include information about the election. i. The voting equipment shall be able to include an identification of the particular election, the voting site and precinct, and the voting machine.
Vol I Sec.7.9.3 bii	ii. The records shall include information identifying whether the balloting is provisional, early, or on election day, and information that identifies the ballot style in use.
Vol I Sec.7.9.3 biii	iii. The records shall include a voting session identifier that is generated when the voting equipment is placed in voting mode, and that can be used to identify the records as being created during that voting session.

Functional Requirements List

Requirement ID	Description
Vol I Sec.7.9.3 c	c. The electronic ballot image and paper records shall be linked by including a unique identifier within each record that can be used to identify each record uniquely and each record's corresponding record.
Vol I Sec.7.9.3 d	d. The voting machine should generate and store a digital signature for each electronic record.
Vol I Sec.7.9.3 e	e. The electronic ballot image records shall be able to be exported for auditing or analysis on standards-based and /or COTS information technology computing platforms.
Vol I Sec.7.9.3 ei	i. The exported electronic ballot image records shall be in a publicly available, non-proprietary format.
Vol I Sec.7.9.3 eii	ii. The records should be exported with a digital signature, which shall be calculated on the entire set of electronic records and their associated digital signatures.
Vol I Sec.7.9.3 eiv	iv. The voting system vendor shall provide a software program that will display the exported ballot image records and that may include other capabilities such as providing vote tallies and indications of undervotes.
Vol I Sec.7.9.3 f	f. The paper record should be created in a format that may be made available across different manufacturers of electronic voting systems.
Vol I Sec.7.9.3 g	g. The paper record shall be created such that its contents are machine readable. i. The paper record shall contain error correcting codes for the purpose of detecting read errors and for preventing other markings on the paper record from being misinterpreted when machine reading the paper record.
Vol I Sec.7.9.3 h	h. If barcode is used, the voting equipment shall be able to print a barcode with each paper record that contains the human-readable contents of the paper record. Discussion: This requirement is not mandatory if a state prohibits the paper record from containing any information that cannot be read and understood by the voter.
Vol I Sec.7.9.3 hi	i. The barcode shall use an industry standard format and shall be able to be read using readily available commercial technology.
Vol I Sec.7.9.3 hii	ii. If the corresponding electronic record contains a digital signature, the digital signature shall be included in the barcode on the paper record.
Vol I Sec.7.9.3 hiii	iii. The barcode shall not contain any information other than the paper record's human-readable content, error correcting codes, and digital signature information.
Vol I Sec.7.9.4 a	a. The voting machine shall provide a standard, publicly documented printer port (or the equivalent) using a standard communication protocol.
Vol I Sec.7.9.4 c	c. If the connection between the voting machine and the printer has been broken, the voting machine shall detect this event and record it in the DRE internal audit log.
Vol I Sec.7.9.4 d	d. The paper path between the printing, viewing and storage of the paper record shall be protected and sealed from access except by authorized election officials.
Vol I Sec.7.9.4 f	f. The printer shall only be able to function as a printer; it shall not contain any other services (e.g., provide copier or fax functions) or network capability.
Vol I Sec.7.9.4 g	g. The voting machine shall detect errors and malfunctions such as paper jams or low supplies of consumables such as paper and ink that may prevent paper records from being correctly displayed, printed or stored.
Vol I Sec.7.9.4 h	h. If an error or malfunction occurs, the voting machine shall suspend voting operations and should present a clear indication to the voter and election officials of the malfunction.
Vol I Sec.7.9.4 i	i. The voting machine shall not record votes if an error or malfunction occurs.
Vol I Sec.7.9.4 j	j. Printing devices should contain sufficient supplies of paper and ink to avoid reloading or opening equipment covers or enclosures and thus potential circumvention of security features; or be able to reload paper and ink with minimal disruption to voting and without circumvention of security features such as seals.
Vol I Sec.7.9.5 a	a. Voter privacy shall be preserved during the process of recording, verifying and auditing his or her ballot selections. Discussion: The privacy requirements from Section 3 also apply to voting equipment with VVPAT.
Vol I Sec.7.9.5 b	b. When a VVPAT with a spool-to-spool continuous paper record is used, a means shall be provided to preserve the secrecy of the paper record of voter selections.
Vol I Sec.7.9.5 c	c. When a VVPAT with a spool-to-spool continuous paper record is used, no record shall be maintained of which voters used which voting machine or the order in which they voted.

Functional Requirements List

Requirement ID	Description
Vol I Sec.7.9.5 d	d. The electronic and paper records shall be created and stored in ways that preserve the privacy of the voter. Discussion: For VVPAT systems that use separate pieces of paper for the record, this can be accomplished in various ways including shuffling the order of the records or other methods to separate the order of stored records.
Vol I Sec.7.9.5 e	e. The privacy of voters whose paper records contain an alternative language shall be maintained.
Vol I Sec.7.9.5 f	f. Unique identifiers shall not be displayed in a way that is easily memorable by the voter.
Vol I Sec.7.9.5 g	g. Both paper rolls and paper record secure receptacles shall be controlled, protected, and preserved with the same security as a ballot box.
Vol I Sec.7.9.6 a	VVPAT Usability a. All usability requirements from Subsection 3.1 shall apply to voting machines with VVPAT.
Vol I Sec.7.9.6 b	VVPAT Usability b. The voting equipment shall be capable of showing the information on the paper in a font size of at least 3.0 mm and should be capable of showing the information in at least two font ranges; 3.0-4.0 mm, and 6.3-9.0 mm, under control of the voter or poll worker.
Vol I Sec.7.9.6 c	c. The voting equipment shall display, print and store the paper record in any of the written alternative languages chosen for the ballot. i. To assist with manual auditing, candidate names on the paper record shall be presented in the same language as used on the DRE summary screen. ii. Information on the paper record not needed by the voter to perform verification shall be in English. Discussion: In addition to the voter ballot selections, the marking of the paper record as accepted or void, and the indication of the ballot page number need to be printed in the alternative language. Other information, such as precinct and election identifiers, shall be in English to facilitate use of the paper record for auditing.
Vol I Sec.7.9.6 d	d. The paper and electronic records shall be presented to allow the voter to read and compare the records without the voter having to shift his or her position.
Vol I Sec.7.9.6 e	e. If the paper record cannot be displayed in its entirety on a single page, a means shall be provided to allow the voter to view the entire record.
Vol I Sec.7.9.6 f	f. If the paper record cannot be displayed in its entirety on a single page, each page of the record shall be numbered and shall include the total count of pages for the record.
Vol I Sec.7.9.6 g	g. The instructions for performing the verification process shall be made available to the voter in a location on the voting machine.
Vol I Sec.7.9.7 a	a. All accessibility requirements from Subsection 3.2 shall apply to voting machines
Vol I Sec.7.9.7 b	b. If the normal voting procedure includes VVPAT, the accessible voting equipment should provide features that enable voters who are visually impaired and voters with an unwritten language to perform this verification. If state statute designates the paper record produced by the VVPAT to be the official ballot or the determinative record on a recount, the accessible voting equipment shall provide features that enable visually impaired

A.2 TDP Requirements

This appendix lists the required content of the TDP as specified in the State and Federal Standards. The list is extracted from those standard

DRAFT

TDP Requirements List

Requirement ID	Description
6209.2.F.13.c	Polling Place Voting System Requirements: (c) The voting system vendor shall provide documentation as to the structure of the exported records and how they shall be read and processed by software.
6209.2.F.16	Polling Place Voting System Requirements: (16) Vendor documentation shall include procedures for investigating and resolving malfunctions including but not limited to misreporting of votes, unreadable paper records, paper jams, low ink, mis-feeds and power failures.
6209.2.F.17	Polling Place Voting System Requirements: (17) Vendor documentation shall include procedures for ensuring, in the case of malfunctions, that electronic and paper records are correctly recorded and stored.
6209.2.F.2	Polling Place Voting System Requirements: (2) There shall be instructions for performing the verification process made available to the voter in a location on the voting system.
6209.2.F.6	Polling Place Voting System Requirements: (6) In the case of a DRE voting system, procedures by which an election official can be notified and prescribed actions can be taken to address discrepancies if a voter indicates that the electronic and paper records do not match, shall be documented.
6209.2.F.8	Polling Place Voting System Requirements: (8) Vendor documentation shall include procedures for returning a voting system to correct operation after a voter has used it incompletely or incorrectly; this procedure shall not cause discrepancies between the tallies of the electronic and paper records.
6209.6.D.2.a	Examination Criteria: (a) Vendor Responsibility The vendor shall provide a list of all documentation and data required to be included as part of the independent review, and vendor technical personnel shall be available to the State Board during the performance of the Functional Configuration Audit.
6209.6.D.2.b	Examination Criteria: (b) Technical Data The vendor shall provide the following technical data:
6209.6.D.2.b.i	Examination Criteria: (i) copies of all procedures used for module or unit testing, integration testing and system testing;
6209.6.D.2.b.ii	Examination Criteria: (ii) copies of all test cases generated for each module and integration test and sample ballot formats or other test cases used for system;
6209.6.D.2.b.iii	Examination Criteria: (iii) records of all tests performed by the procedures listed above, including error correction and retest.
6209.6.D.2.c1	Examination Criteria: (c) Audit Procedure The State Board, with the assistance of an independent testing authority, shall subject each voting system to a complete functional test, including but not limited to actual use testing of all components used by voters to enter or review votes. Additionally, the State Board and its independent testing authority shall review the vendor's test procedures and test results.
6209.6.D.2.c2	Examination Criteria: This review shall include an assessment of the adequacy of test cases and input data to exercise all system functions and to detect program logic and data processing errors if such be present.
6209.6.D.2.c3	Examination Criteria: The review shall also include an examination of all test data which is to be used as a basis for qualification.
6209.6.D.3.a	Examination Criteria: (a) Vendor Responsibility The vendor shall provide a list of all documentation and data required to be audited by the State Board. Vendor's technical personnel shall be available to the State Board during the performance of the Physical Configuration Audit.
6209.6.D.3.b	Examination Criteria: (b) Technical Data The vendor shall provide the following technical data:
6209.6.D.3.b.i	Examination Criteria: (i) identification of all items which are to be a part of the software releases;
6209.6.D.3.b.ii	Examination Criteria: (ii) identification of all hardware which interfaces with the software;
6209.6.D.3.b.iii	Examination Criteria: (iii) configuration baseline data for all hardware included within the system;
6209.6.D.3.b.iv	Examination Criteria: (iv) copies of all software documentation which is intended for distribution to users, including program listings, specifications, operator manual, user manual and software maintenance manual;
6209.6.D.3.b.v	Examination Criteria: (v) proposed user acceptance test procedure and acceptance criteria;
6209.6.D.3.b.vi	Examination Criteria: (vi) an identification and explanation of any changes between the Physical Configuration Audit and the configuration submitted for the Functional Configuration Audit.

TDP Requirements List

Requirement ID	Description
6209.6.D.3.c1	<p>Examination Criteria: (c) Audit Procedure</p> <p>Required data items include draft and formal documentation of the vendor's software development program which are relevant to the design and conduct of Qualification Tests. The vendor shall identify all documents, or portions of documents, which the vendor asserts contain proprietary information not approved for public release. The State Board or its designee shall agree to use any proprietary information contained therein solely for the purpose of analyzing and testing the software and shall refrain from disclosing proprietary information to any other person or agency without the prior written consent of the vendor or a Court order. (continued below)</p>
6209.6.D.3.c2	<p>Examination Criteria: (continued from above) The State Board or its designee shall review the vendor's source code and documentation to verify that the software conforms to the documentation, and that the documentation is sufficient to enable the user to install, validate, operate and maintain the voting system. The review shall also include an inspection of all records of the baseline version against the vendor's release control system to establish that the configuration, being qualified, conforms to the engineering and test data.</p>
6209.6.F	<p>Examination Criteria: F. Software, Hardware, Operating and Support Documentation</p>
6209.6.F.1	<p>Examination Criteria: (1) Software Qualification</p> <p>The following system software and firmware vendor data items shall be submitted as a precondition of certification of acceptability for elections use.</p>
6209.6.F.2	<p>Examination Criteria: (2) Vendor Documentation</p> <p>Complete product documentation shall be provided to the State Board for voting systems, their components and all auxiliary devices. This documentation shall be sufficient to serve the needs of the voter, the operator, maintenance technicians, and other appropriate county board personnel. It shall be prepared and published in accordance with standard industrial practice for electronic and mechanical equipment such documentation shall include:</p>
6209.6.F.3	<p>Examination Criteria: (3) Software Specification</p> <p>The Software Specification shall contain and describe the vendor's design standards and conventions, environment and interface specifications, functional specifications, programming architecture specifications, and test and verification specifications. Vendor must also provide document identification, an abstract of the specification, configuration control status and a table of contents. The body of the specification shall contain the following material:</p>
6209.6.F.3.a	<p>Examination Criteria: (a) System Overview</p> <p>The vendor shall identify the system hardware and the environment in which the software will operate and the general design and operational considerations and constraints which have influenced the design of the software.</p>
6209.6.F.3.b	<p>Examination Criteria: (b) Program Description</p> <p>The vendor shall provide descriptions of the software system concept, the array of hardware in which it operates, the intended operating environment, the specific software design objectives and development methodology and the logical structure and algorithms used to accomplish the objectives.</p>
6209.6.F.3.c	<p>Examination Criteria: (c) Standards and Conventions</p> <p>The vendor shall provide information which can be used as a partial basis for code analysis and test design. It should include a description and discussion of the standards and conventions used in the preparation of this specification and in the development of the software.</p>
6209.6.F.3.d	<p>Examination Criteria: (d) Specification Standards and Conventions</p> <p>The vendor shall identify all published and private standards and conventions used to document software development and testing. Vendor internal procedures shall be provided as attachments to this Software Specification.</p>
6209.6.F.3.e	<p>Examination Criteria: (e) Test and Verification Standards</p> <p>The vendor shall identify any standards or other documents which are applicable to the determination of program correctness and acceptance criteria.</p>
6209.6.F.3.f	<p>Examination Criteria: (f) Quality Assurance Standards</p> <p>The vendor shall describe all standards or other documents which are applicable to the examination and testing of the software, including standards for flowcharts, program documentation, test planning and test data acquisition and reporting.</p>
6209.6.F.3.g	<p>Examination Criteria: (g) Operating Environment</p> <p>The vendor shall provide a description of the system and subsystem interfaces at which inputs, outputs and data transformations occur. It shall contain or make reference to all operating environment factors which influence the software design.</p>
6209.6.F.3.h	<p>Examination Criteria: (h) Hardware Constraints</p> <p>The vendor shall identify and describe the hardware characteristics which influence the design of the software, such as:</p>
6209.6.F.3.h.i	<p>Examination Criteria: (i) the logic and arithmetic capability of the processor,</p>

TDP Requirements List

Requirement ID	Description
6209.6.F.3.h.ii	Examination Criteria: (ii) memory read/write characteristics,
6209.6.F.3.h.iii	Examination Criteria: (iii) external memory device characteristics
6209.6.F.3.h.iv	Examination Criteria: (iv) peripheral device interface hardware data I/O device protocols, and
6209.6.F.3.h.v	Examination Criteria: (v) operator controls, indicators and displays.
6209.6.F.3.i	Examination Criteria: (i) Software Environment The vendor shall identify all compilers, assemblers, or other software tools to be used for the generation of executable code and a description of the operating system or system monitor. This section shall also contain an overview of the compile-time interaction of the voting system software with library calls and linking.
6209.6.F.3.j	Examination Criteria: (j) Interface Characteristics The vendor shall describe the interfaces between executable code and system input-output and control hardware.
6209.6.F.3.k	Examination Criteria: (k) Software Functional Specification The vendor shall provide a description of the overall functions which the software performs in the context of its mode or modes of operation. The vendor shall also describe the capabilities and methods for detecting and handling exceptional conditions, system failure, data input/output errors, error logging and audit record generation and security monitoring and control.
6209.6.F.3.l	Examination Criteria: (l) Configurations and Operating Modes The vendor shall describe the various software configurations and operating modes of the system; such as preparation for opening of the polling place, vote recording and/or vote processing, closing of the polling place and report generation. For each software function or operating mode, a definition of the inputs (characteristics, tolerances or acceptable ranges) to the function or mode, how the inputs are processed and what outputs are produced (characteristics, tolerances or acceptable ranges) shall be provided.
6209.6.F.3.m	Examination Criteria: (m) External files In the event that external files are used for data input or output, the definition of information context and record formats shall be provided. The vendor shall also describe the procedures for file maintenance, access privileges and security.
6209.6.F.3.n1	Examination Criteria: (n) Security Security requirements and security provisions of the system's software shall be identified for each system function and operating mode. The voting system must be secure against attempts to interfere with correct system operation. The vendor shall identify each potential point of attack. For each potential point of attack, the vendor shall identify the technical safeguards embodied in the voting system to defend against attack, and the procedural safeguards that the vendor has recommended be followed by the election administrators to further defend against that attack. (continued below)
6209.6.F.3.n2	Examination Criteria: (continued from above) Security requirements and provisions shall include the ability of the system to detect, prevent, log and recover from the broad range of security risks identified. These procedures shall also examine system capabilities and safeguards claimed by the vendor to prevent interference with correct system operations. The State Board, with the assistance of its ITA, shall conduct tests to confirm that the security requirements of these Regulations have been completely addressed. Notwithstanding any other provisions of these Regulations, the State Board shall determine whether all or a portion of such security requirements and security provisions shall be available for public inspection, but shall exclude any information which compromises the security of the voting system.
6209.6.F.3.o	Examination Criteria: (o) Programming Specifications The vendor shall provide an overview of the software design, structure and implementation algorithms. Whereas the Functional Specification of the preceding section provides a description of what functions the software performs and the various modes in which it operates, this section should be prepared so as to facilitate understanding of the internal functioning of the individual software modules. Implementation of functions shall be described in terms of software architecture, algorithms and data structures and all procedures or procedure interfaces which are vulnerable to degradation in data quality or security penetration shall be identified.
6209.6.F.3.p	Examination Criteria: (p) Test and Verification Specifications The vendor shall provide a description of the procedures used during software development to verify logical correctness, data quality and security. This description shall include existing standard test procedures, special purpose test procedures, test criteria and experimental design and validation criteria. In the event that this documentation is not available, the Qualification Test agency shall design test cases and procedures equivalent to those ordinarily used as a basis for verification (see below).

TDP Requirements List

Requirement ID	Description
6209.6.F.3.q	<p>Examination Criteria: (q) Qualification Test Specification</p> <p>The vendor shall provide a description of the specification for verification and validation of overall software performance, including acceptance criteria for control and data input/output, processing accuracy, data quality assessment and maintenance, exceptional handling and security. The specification shall identify specific procedures by means of which the general suitability of the software for elections use can be assessed and demonstrated. The vendor's specification and procedure shall be used to establish the detailed requirements of the tests described in "Laboratory Environmental Test Procedures for Hardware and Software" of this Standard.</p>
6209.6.F.3.r	<p>Examination Criteria: (r) Acceptance Test Specification</p> <p>The vendor shall provide a description of the specification for installation, acceptance and readiness verification. This specification shall identify specific procedures by means of which the capability of the software to accommodate actual ballot formats and format logic, and pre-election logic, accuracy and security test requirements of using jurisdictions may be assessed and demonstrated. The vendor's specification shall be used to establish the detailed requirements of the tests described in "Laboratory Environmental Test Procedures for Hardware and Software" of this standard performed to evaluate the adequacy of the vendor's procedures and it shall be suitable for inclusion in the regulations and procedures of user counties when preparing for the conduct of actual elections.</p>
6209.6.F.3.s	<p>Examination Criteria: (s) Appendices</p> <p>The vendor shall provide descriptive material and data supplementing the various sections of the body of the Software Specification. The content and arrangement of appendices shall be at the discretion of the vendor. Topics recommended for amplification and treatment in appendix form include:</p>
6209.6.F.3.s.i	<p>Examination Criteria: (i) Glossary: Provide a listing and brief definition of all software module names and variable names with reference to their locations in the software structure. Include abbreviations, acronyms and terms which are either not commonly used in data processing and software development or which are used in an uncommon semantic context.</p>
6209.6.F.3.s.ii	<p>Examination Criteria: (ii) References: Provide a list of references to all related vendor documents, data, standards and technical sources used in software development and testing.</p>
6209.6.F.3.s.iii	<p>Examination Criteria: (iii) Program Analysis: Provide the results of software configuration analysis, algorithm analysis and selection, timing studies and hardware interface studies reflected in the final software design and coding.</p>
6209.6.F.3.s.iv	<p>Examination Criteria: (iv) Security Analysis: Provide a detailed description of the penetration analysis performed to preclude intrusion by unauthorized persons and fraudulent manipulation of elections data. Identify security policies and measures and selection criteria for audit log data categories.</p>
6209.6.F.4a	<p>Examination Criteria: (4) Operator Information</p> <p>This documentation shall include a physical description of the equipment sufficient to identify all features, controls and displays. It shall include a complete procedure for energizing the equipment, for testing and verifying operational status and for identifying all abnormal equipment states. It shall include a complete operating procedure for inserting ballots to be tabulated, for controlling the tabulation process, for monitoring the status of the equipment, for recovering from error conditions and for preparing output reports. It shall also include troubleshooting instructions.</p>
6209.6.F.4b	<p>Examination Criteria: The documentation shall also include a description of the relationship of the Sensitive Area, Voting Target, and Ballot Position. For paper-based systems, this description shall include a description of the nature of the marks the system will and will not count as votes, for example, the types of marks made with each of a variety of pens and pencils that should be counted and that should not be counted. For DRE voting systems, this description shall include a description of the nature of the voter action required to cast a vote in the Sensitive Area, for example, the force and duration of contact required.</p>
6209.6.F.5.a	<p>Examination Criteria: (5) Maintenance Information:</p> <p>a) This documentation shall contain a complete physical and functional description of the equipment and a theory of operation which fully describes the electrical and mechanical function of the equipment, how the processes of ballot handling and reading are performed, how data are handled in the processor and memory sections, how data output is initiated and controlled, how power is converted or conditioned and how test and diagnostic information is acquired and used.</p>
6209.6.F.5.b	<p>Examination Criteria: (5) Maintenance Information:</p> <p>(b) A complete parts and materials list shall be provided which contains sufficient descriptive information to identify all parts by type, size, value or range and manufacturer's designation.</p>
6209.6.F.5.c	<p>Examination Criteria: (5) Maintenance Information:</p> <p>(c) Technical illustrations and schematic representations of electronic circuits shall be provided with indications of all test and adjustment points and the nominal value and tolerance or waveform to be measured. Fault detection, isolation and correction procedures or logic diagrams shall be prepared for all operational abnormalities identified by design analysis and operating experiences.</p>

TDP Requirements List

Requirement ID	Description
6209.6.F.6	<p>Examination Criteria: (6) Logistics, Facilities, and Training</p> <p>The vendor shall identify all operating and support requirements of the system or component. These requirements include material, facilities and personnel, including furnishings, fixtures, and utilities which will be required to support system operation, maintenance and storage.</p>
6209.6.F.7.a	<p>Examination Criteria: (7) Maintenance Training and Supply</p> <p>(a) The vendor shall identify all corrective and preventive maintenance tasks, including the calibration of the system, as appropriate, and the level at which they shall be performed. Levels of maintenance shall include operator tasks, maintenance personnel tasks and factory repair.</p>
6209.6.F.7.b	<p>Examination Criteria: (b) Operator tasks shall be limited to the activation of controls to identify irrecoverable error conditions and to the replenishment of consumables such as printer ribbons, paper and the like.</p>
6209.6.F.7.c	<p>Examination Criteria: (c) Maintenance personnel tasks shall include all field maintenance actions which require access to internal portions of the equipment. They shall include the conduct of tests to localize the source of a malfunction; the adjustment, repair or replacement of malfunctioning circuits or components and the conduct of tests to verify restoration to service.</p>
6209.6.F.7.d	<p>Examination Criteria: (d) Factory repair tasks shall be minimized, and repairs shall be made on site whenever reasonably possible. Factory repairs shall only include complex and infrequent maintenance functions which require access to proprietary or to specialized facilities and equipment which cannot be obtained by the county board.</p>
6209.6.F.7.e	<p>Examination Criteria: (e) The vendor shall identify by function all personnel required to operate and support the system. For each functional category, the number of personnel and their skills and skill levels shall be specified.</p>
6209.6.F.7.f	<p>Examination Criteria: (f) The vendor shall specify requirements for the training of each category of operating and support personnel, including but not limited to voters, poll workers, and elections staff. The vendor shall prepare all materials required in the training activity and shall provide or otherwise arrange for the provision of as many qualified instructors as are necessary to properly and fully train said personnel in each category.</p>
6209.6.F.7.g	<p>Examination Criteria: (g) The vendor shall recommend a standard complement of supplies, spares and repair parts which will be required to support system operation. This list shall include the identification of these materials and their individual quantities and sources from which they may be obtained. The vendor shall supply, at vendor's expense, any special tools required to repair or maintain the equipment.</p>
6209.6.F.7.h	<p>Examination Criteria: (h) The vendor shall provide complete instructions for all methods of voting which voters may use to cast their vote, including instructions on entering and changing votes, write-in voting, verifying votes and accepting the cast votes. Written and audio instructions shall be provided in each language in which voting shall occur within the state.</p>
Vol I Sec.2.1.1 g	<p>Overall System Capabilities, Security</p> <p>g. Provide documentation of mandatory administrative procedures for effective system security.</p>
Vol I Sec.2.1.10	<p>Overall System Capabilities, Data Retention</p> <p>United States Code Title 42, Sections 1974 through 1974e states that election administrators shall preserve for 22 months "all records and paper that came into (their) possession relating to an application, registration, payment of poll tax, or other act requisite to voting". This retention requirement pertains to systems that will be used at anytime for voting of candidates for Federal offices.</p> <p>Therefore, all systems shall provide for maintaining the integrity of voting and audit data during an election and for a period of at least 22 months afterward.</p> <p>For 22-month document retention, the general rule is that all printed copy records produced by the election database and ballot processing systems shall be so labeled and archived.</p> <p>Regardless of system type, all audit trail information spelled out in Subsection 5.5 shall be retained in its original format, whether that be real-time logs generated by the system, or manual logs maintained by election personnel. The election audit trail includes not only inprocess logs of election-night and subsequent processing of absentee or provisional ballots, but also time logs of baseline ballot definition formats, and system readiness and testing results</p>
Vol I Sec.2.1.5	<p>System Audit, System Audit Purpose and Context</p> <p>Because the actual implementation of specific characteristics may vary from system to system, it is the responsibility of the vendor to describe each system's characteristics in sufficient detail so that test labs and system users can evaluate the adequacy of the system's audit trail. This description shall be incorporated in the System Operating Manual, which is part of the Technical Data Package.</p>
Vol I Sec.2.1.5.1 b iv	<p>iv All error messages for which correction impacts vote recording or vote processing shall be written in a manner that is understandable to an election official who possesses training on system use and operation, but does not possess technical training on system servicing and repair;</p>
Vol I Sec.2.1.5.1 b v	<p>v. The message cue for all systems shall clearly state the action to be performed in the event that voter or operator response is required;</p>

TDP Requirements List

Requirement ID	Description
Vol I Sec.2.1.6 (1)	<p>Overall System Capabilities, Election Management System</p> <p>An EMS [Election Management System] shall generate and maintain a database, or one or more interactive databases, that enables election officials or their designees to perform the following functions:</p> <p>a. Define political subdivision boundaries and multiple election districts as indicated in the system documentation;</p>
Vol I Sec.2.1.6 (7)	<p>g. Accumulate vote totals at multiple reporting levels as indicated in the system documentation;</p>
Vol I Sec.2.1.7.2	<p>Voting Tabulation Program, Voting Variations</p> <p>The TDP accompanying the system shall specifically identify which of the following items can and cannot be accommodated by the system as well as how the system can implement the items supported:</p> <p>Closed primaries; Open primaries Partisan offices Non-partisan offices Write-in voting Primary presidential delegation nominations Ballot rotation Straight party voting Cross-party endorsement Split precincts Vote for N of M Recall issues, with options Cumulative voting Ranked order voting Provisional or challenged ballots.</p>
Vol I Sec.2.2.1.1 c	<p>c. Supporting the maximum number of potentially active voting positions as indicated in the system documentation;</p>
Vol I Sec.2.2.1.2 d	<p>d. Simultaneous display of the maximum number of choices for a single contest as indicated by the vendor in the system documentation;</p>
Vol I Sec.2.2.1.3 c	<p>c. The ballot conforms to vendor specifications for type of paper stock, weight, size, shape, size and location of punch or mark field used to record votes, folding, bleed through, and ink for printing if paper ballot documents or paper displays are part of the system.</p>
Vol I Sec.2.2.2 a	<p>Pre-Voting Functions, Election Programming</p> <p>All systems shall provide for the:</p> <p>a. Logical definition of the ballot, including the definition of the number of allowable choices for each office and contest;</p>
Vol I Sec.2.2.3 a	<p>Pre-Voting Functions, Ballot and Program Installation and Control</p> <p>All systems shall include the following at the time of ballot and program installation:</p> <p>a. A detailed work plan or other documentation providing a schedule and steps for the software and ballot installation, which includes a table outlining the key dates, events, and deliverables;</p>
Vol I Sec.3.1.1	<p>Usability Requirements</p> <p>The vendor shall conduct summative usability tests on the voting system using individuals representative of the general population. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification.</p>
Vol I Sec.3.1.4 b	<p>b. The voting machine or related materials shall provide clear instructions and assistance to allow voters to successfully execute and cast their ballots independently.</p>
Vol I Sec.3.1.4 bii	<p>ii. The voting machine shall provide instructions for all its valid operations.</p> <p>Discussion: If an operation is available to the voter, it must be documented. Examples include how to change a vote, how to navigate among contests, how to cast a straight party vote, and how to cast a write-in vote.</p>
Vol I Sec.3.2.2.1 a	<p>The accessible voting station shall be accessible to voters with partial vision.</p> <p>a. The vendor shall conduct summative usability tests on the voting system using partially sighted individuals. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification.</p>
Vol I Sec.3.2.2.2 a	<p>The accessible voting station shall be accessible to voters who are blind.</p> <p>a. The vendor shall conduct summative usability tests on the voting system using individuals who are blind. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification.</p>

TDP Requirements List

Requirement ID	Description
Vol I Sec.3.2.3 a	The voting process shall be accessible to voters who lack fine motor control or use of their hands. a. The vendor shall conduct summative usability tests on the voting system using individuals lacking fine motor control. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification.
Vol I Sec.4.1.2 (2)	The Technical Data Package supplied by the vendor shall include a statement of all requirements and restrictions regarding environmental protection, electrical service, recommended auxiliary power, telecommunications service, and any other facility or resource required for the proper installation and operation of the system.
Vol I Sec.4.1.4.2 aiii	iii. The Technical Data Package shall specify the required paper stock, size, shape, opacity, color, watermarks, field layout, orientation, size and style of printing, size and location of mark fields used for vote response fields and to identify unique ballot formats, placement of alignment marks, ink for printing, and folding and bleed-through limitations for preparation of ballots that are compatible with the system.
Vol I Sec.4.1.4.2 b	b. The Technical Data Package shall specify marking devices, which, if used to make the prescribed form of mark, produce readable marked ballots such that the system meets the performance requirements for accuracy in Subsection 4.1.1. Marking devices can be either manual (such as pens or pencils) or electronic. These specifications shall identify: i. Specific characteristics of marking devices that affect readability of marked ballots ii. Performance capabilities with regard to each characteristic iii. For marking devices manufactured by multiple external sources, a listing of sources and model numbers that are compatible with the system
Vol I Sec.4.1.5.1 a	Ballot Handling, Capacity (Central Count) The capacity to convert the punches or marks on individual ballots into signals is uniquely important to central count systems. The capacity for a central count system shall be documented by the vendor. This documentation shall include the capacity for individual components that impact the overall capacity.
Vol I Sec.4.3.1 b	b. Include, as part of the accompanying Technical Data Package, an approved parts list
Vol I Sec.4.3.5 (2)	Vendors shall specify the typical system configuration that is to be used to assess availability, and any assumptions made with regard to any parameters that impact the MTTR. These factors shall include at a minimum: e. Recommended number and locations of spare devices or components to be kept on hand for repair purposes during periods of system operation f. Recommended number and locations of qualified maintenance personnel who need to be available to support repair calls during system operation g. Organizational affiliation (i.e., jurisdiction, vendor) of qualified maintenance personnel
Vol I Sec.5.1.1 (2)	Software Standards, Software Sources Correct test design and sufficient test execution must account for the intended and proper configuration of all system components. Therefore, vendors shall submit a record of all user selections made during software installation as part of the Technical Data Package.
Vol I Sec.5.1.1 (3)	Software Standards, Software Sources The vendor shall also submit a record of all configuration changes made to the software following its installation.
Vol I Sec.5.4.1 a	Audit Record Data, Pre-election Audit Records The log shall include: a. The allowable number of selections for an office or issue;
Vol I Sec.5.4.1 b	b. The combinations of voting patterns permitted or required by the jurisdiction;
Vol I Sec.5.4.1 c	c. The inclusion or exclusion of offices or issues as the result of multiple districting within the polling place;
Vol I Sec.5.4.1 d	d. Any other characteristics that may be peculiar to the jurisdiction, the election, or the polling places; location;
Vol I Sec.5.4.1 e	e. Manual data maintained by election personnel;
Vol I Sec.5.4.1 f	f. Samples of all final ballot formats
Vol I Sec.5.4.1 g	g. Ballot preparation edit listings.
Vol I Sec.7.2.1	Access Control, Access Control Policy The vendor shall specify the general features and capabilities of the access control policy recommended to provide effective voting security.
Vol I Sec.7.2.1 a	Access Control Policy, General Access Control Policy The vendor shall provide a description of recommended policies for: a. Software access controls;

TDP Requirements List

Requirement ID	Description
Vol I Sec.7.2.1 b	b. Hardware access controls;
Vol I Sec.7.2.1 c	c. Communications;
Vol I Sec.7.2.1 d	d. Effective password management;
Vol I Sec.7.2.1 e	e. Protection abilities of a particular operating system;
Vol I Sec.7.2.1 f	f. General characteristics of supervisory access privileges;
Vol I Sec.7.2.1 g	g. Segregation of duties; and
Vol I Sec.7.2.1 h	h. Any additional relevant characteristics.
Vol I Sec.7.2.1.1 a	Access Control Policy, Individual Access Privileges Voting system vendors shall: a. Identify each person to whom access is granted, and the specific functions and data to which each person holds authorized access;
Vol I Sec.7.2.1.1 b	b. Specify whether an individual's authorization is limited to a specific time, time interval, or phase of the voting or counting operations; and
Vol I Sec.7.2.1.2 a	Access Control, Access Control Measures Vendors shall provide a detailed description of all system access control measures designed to permit authorized access to the system and prevent unauthorized access. Examples of such measures include: a. Use of data and user authorization;
Vol I Sec.7.2.1.2 b	b. Program unit ownership and other regional boundaries;
Vol I Sec.7.2.1.2 c	c. One-end or two-end port protection devices;
Vol I Sec.7.2.1.2 d	d. Security kernels;
Vol I Sec.7.2.1.2 e	e. Computer-generated password keys;
Vol I Sec.7.2.1.2 f	f. Special protocols;
Vol I Sec.7.2.1.2 g	g. Message encryption; and
Vol I Sec.7.2.1.2 h	h. Controlled access security.
Vol I Sec.7.2.1.2 i	Vendors also shall define and provide a detailed description of the methods used to prevent unauthorized access to the access control capabilities of the system itself.
Vol I Sec.7.3.1 (1)	For polling place operations, vendors shall develop and provide detailed documentation of measures to enable poll workers to physically protect and perform orderly shutdown of voting equipment to counteract vandalism, civil disobedience, and similar occurrences.
Vol I Sec.7.3.1 (2)	The measures shall allow the immediate detection of tampering with vote casting devices and precinct ballot counters.
Vol I Sec.7.3.1 (3)	They also shall control physical access to a telecommunications link if such a link is used
Vol I Sec.7.3.2	Vendors shall develop and document in detail the measures to be taken in a central counting environment. These measures shall include physical and procedural controls related to the handling of ballot boxes, preparing of ballots for counting, counting operations and reporting data.
Vol I Sec.7.4.1 a	Security Standards, Software and Firmware Installation The system shall meet the following requirements for installation of software, including hardware with imbedded firmware: a. If software is resident in the system as firmware, the vendor shall require and state in the system documentation that every device is to be retested to validate each ROM prior to the start of elections operations;
Vol I Sec.7.4.1 b	b. To prevent alteration of executable code, no software shall be permanently installed ore resident in the system unless the system documentation states that the jurisdiction must provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of the system hardware;
Vol I Sec.7.4.2 (2)	Security Standards, Protection Against Malicious Software Vendors shall develop and document the procedures to be followed to ensure that such protection is maintained in a current status.

TDP Requirements List

Requirement ID	Description
Vol I Sec.7.4.4 a	Software Distribution a. The vendor shall document all software including voting system software, third party software (such as operating systems and drivers) to be installed on the certified voting system, and installation programs.
Vol I Sec.7.4.4 ai	Software Distribution i. The documentation shall have a unique identifier (such as a serial number or part number) for the following set of information: documentation, software vendor name, product name, version, the certification application number of the voting system, file names and paths or other location information (such as storage addresses) of the software.
Vol I Sec.7.4.4 aii	Software Distribution ii. The documentation shall designate all software files as static, semi-static or dynamic.
Vol I Sec.7.4.4 dii	ii. The vendor shall document that the process used to verify the software distributed on unalterable storage media is the certified software by using the reference information provided by the NSRL or other designated repository before installing the software.
Vol I Sec.7.4.6 b	b. The vendor shall have a process to verify that the correct software is loaded, that there is no unauthorized software, and that voting system software on voting equipment has not been modified, using the reference information from the NSRL or from a State designated repository.
Vol I Sec.7.4.6 bii	ii. The vendor shall document the process used to verify software on voting equipment.
Vol I Sec.7.4.6 c	c. The vendor shall provide a method to comprehensively list all software files that are installed on voting systems.
Vol I Sec.7.4.6 di	i. If the process uses hashes or digital signatures, then the verification software shall use a FIPS 140-2 level 1 or higher validated cryptographic module.
Vol I Sec.7.4.6 fii	ii. The vendor shall document the values of all static registers and variables, and the initial starting values of all dynamic registers and variables listed for voting system software, except for the values set to conduct a specific election.
Vol I Sec.7.5.2 b	Protection Against External Threats, Identification of COTS Products Voting systems that use public telecommunications networks shall provide system documentation that clearly identifies all COTS hardware and software products and communications services used in the development and/or operation of the voting system, including Operating systems, Communications routers. Modem drivers and Dial-up networking software.
Vol I Sec.7.5.2 bi	Protection Against External Threats, Identification of COTS Products Such documentation shall identify the name, vendor, and version used for each such component.
Vol I Sec.7.5.3	Telecommunications and Data Transmission, Monitoring and Responding to External Threats Voting systems that use public telecommunications networks may become vulnerable, by virtue of their system components, to external threats to the accuracy and integrity of vote recording, vote counting, and vote consolidation and reporting processes. Therefore, vendors of such systems shall document how they plan to monitor and respond to known threats to which their voting systems are vulnerable.
Vol I Sec.7.5.3 a	Telecommunications and Data Transmission, Monitoring and Responding to External Threats This documentation shall provide a detailed description, including scheduling information, of the procedures the vendor will use to: a. Monitor threats, such as through the review of assessments, advisories, and alerts for COTS components issued by the Computer Emergency Response Team (CERT), for which a current listing can be found at http://www.cert.org , the National Infrastructure Protection Center (NIPC), and the Federal Computer Incident Response Capability (FedCIRC), for which additional information can be found at http://www.fedcirc.gov/ ;
Vol I Sec.7.5.3 b	b. Evaluate the threats and, if any, proposed responses;
Vol I Sec.7.5.3 c	c. Develop responsive updates to the system and/or corrective action;
Vol I Sec.7.5.3 d	d. Submit the proposed response to the ITAs and appropriate states for approval, identifying the exact changes and whether or not they are temporary or permanent;
Vol I Sec.7.5.3 e	e. After implementation of the proposed response is approved by the state, assist clients, either directly or through detailed written procedures, how to update their systems and/or to implement the corrective procedures within the timeframe established by the State

TDP Requirements List

Requirement ID	Description
Vol I Sec.7.5.3 f	f. Address threats emerging too late to correct the system at least one month before the election, including: 1) Providing prompt, emergency notification to the ITAs and the affected states and user jurisdictions; 2) Assisting client jurisdictions directly, or advising them through detailed written procedures, to disable the public telecommunications mode of the system; and 3) Modifying the system after the election to address the threat; submitting the modified system to an accredited test lab and the EAC or state certification authority for approval, and assisting client jurisdictions directly, or advising them through detailed written procedures, to update their systems and/or to implement the corrective procedures after approval.
Vol I Sec.7.6.2.1 a	Vendors of voting systems that cast individual ballots over a public telecommunications network shall provide detailed descriptions of: a. All activities mandatory to ensuring effective voting system security to be performed in setting up the system for operation, including testing of security before an election
Vol I Sec.7.6.2.1 b	b. All activities that should be prohibited during voting equipment setup and during the timeframe for voting operations, including both the hours when polls are open and when polls are closed
Vol I Sec.7.7.1 ai	WIRELESS, Controlling Usage a. If wireless communications are used in a voting system, then the vendor shall supply documentation describing how to use all aspects of wireless communications in a secure manner. This documentation shall include: i. A complete description of the uses of wireless in the voting system including descriptions of the data elements and signals that are to be carried by the wireless mechanism
Vol I Sec.7.7.1 aii	ii. A complete description of the vulnerabilities associated with this proposed use of wireless, including vulnerabilities deriving from the insertion, deletion, modification, capture or suppression of wireless messages
Vol I Sec.7.7.1 aiii	iii. A complete description of the techniques used to mitigate the risks associated with the described vulnerabilities including techniques used by the vendor to ensure that wireless cannot send or receive messages other than those situations specified in the documentation. Cryptographic techniques shall be carefully and fully described, including a description of cryptographic key generation, management, use, certification, and destruction
Vol I Sec.7.7.1 aiv	iv. A rationale for the inclusion of wireless in the proposed voting system, based on a careful and complete description of the perceived advantages and disadvantages of using wireless for the documented uses compared to using non-wireless approaches
Vol I Sec.7.7.1 b	b. The details of all cryptographic protocols used for wireless communications, including the specific features and data, shall be documented.
Vol I Sec.7.7.1 c	c. The wireless documentation shall be closely reviewed for accuracy, completeness, and correctness.
Vol I Sec.7.7.1 d	d. There shall be no undocumented use of the wireless capability, nor any use of the wireless capability that is not entirely controlled by an election official.
Vol I Sec.7.7.1 e	e. If a voting system includes wireless capabilities, then the voting system shall be able to accomplish the same function if wireless capabilities are not available due to an error or no service. i. The vendor shall provide documentation how to accomplish these functions when wireless is not available.
Vol I Sec.7.7.2 d	d. If a voting system provides wireless communications capabilities, then the type of wireless communications used (such as radio frequencies) shall be identified either via a label or via the voting system documentation.
Vol I Sec.7.9	This section contains requirements for DREs with a Voter Verifiable Paper Audit Trail (VVPAT) component. VVPAT capability is not required for national certification. However, these requirements will be applied for certification testing of DRE systems that are intended for use in states that require DREs to provide this capability. The vendor's certification testing application to the EAC must indicate whether the system being presented for testing includes this capability, as provided under Subsection 1.6.2.5 extensions.
Vol I Sec.7.9.2 e	e. Vendor documentation shall include procedures to enable the election official to return a voting machine to correct operation after a voter has used it incompletely or incorrectly. This procedure shall not cause discrepancies between the tallies of the electronic and paper records.
Vol I Sec.7.9.3 eiii	iii. The voting system vendor shall provide documentation as to the structure of the exported ballot image records and how they shall be read and processed by software.
Vol I Sec.7.9.3 ev	v. The voting system vendor shall provide full documentation of procedures for exporting electronic ballot image records and reconciling those records with the paper audit records.
Vol I Sec.7.9.4 k	k. Vendor documentation shall include procedures for investigating and resolving printer malfunctions including, but not limited to; printer operations, misreporting of votes, unreadable paper records, and power failures.

TDP Requirements List

Requirement ID	Description
Vol I Sec.7.9.4 I	I. Vendor documentation shall include printer reliability specifications including Mean Time Between Failure estimates, and shall include recommendations for appropriate quantities of backup printers and supplies.
Vol I Sec.7.9.6 g	g. The instructions for performing the verification process shall be made available to the voter in a location on the voting machine.
Vol I Sec.8.2 a	Quality Assurance, General Requirements At a minimum, this program shall: a. Include procedures for specifying, procuring, inspecting, accepting, and controlling parts and raw materials of the requisite quality;
Vol I Sec.8.2 b	b. Require the documentation of the hardware and software development process;
Vol I Sec.8.2 c	c. Identify and enforce all requirements for: 1) In-process inspection and testing that the manufacturer deems necessary to ensure proper fabrication and assembly of hardware; and 2) Installation and operation of software (including firmware).
Vol I Sec.8.2 d	d. Include plans and procedures for post-production environmental screening and acceptance test; and
Vol I Sec.8.2 e	e. Include a procedure for maintaining all data and records required to document and verify the quality inspections and tests.
Vol I Sec.8.3	Components from Third Parties A vendor who does not manufacture all the components of its voting system, but instead procures components as standard commercial items for assembly and integration into a voting system, shall verify that the supplier vendors follow documented quality assurance procedures that are at least as stringent as those used internally by the voting system vendor.
Vol I Sec.8.4 a	The manufactureer or vendor shall be responsible for: a. Performing all quality assurance tests;
Vol I Sec.8.4 b	b. acquiring and documenting test data; and
Vol I Sec.8.4 c	c. Providing test reports for review by the ITA and to the purchaser upon request..
Vol I Sec.8.5	Quality Assurance, Parts & Materials Special Tests and Examinations In order to ensure that voting system parts and materials function properly, vendors shall: a. Select parts and materials to be used in voting systems and components according to their suitability for the intended application. Suitability may be determined by similarity of this application to existing standard practice or by means of special tests b. Design special tests, if needed, to evaluate the part or material under conditions accurately simulating the actual operating environment; an c. Maintain the resulting test data as a part of the quality assurance program documentation.
Vol I Sec.8.6 b	b. Deliver a record of tests, or a certificate of satisfactory completion, with each system or component.
Vol I Sec.8.7 (1)	Quality Conformance Inspections: Vendors...documentation shall a. Be sufficient to serve the needs of the ITA, voters, election officials and maintenance technicians.
Vol I Sec.8.7 (2)	b. Be prepared and published in accordance with standard industrial practice for information technology and electronic and mechnaical equipment
Vol I Sec.8.7 (3)	c. Consist at a minimum of the following 1. System overview
Vol I Sec.8.7 (4)	2. System functionality description
Vol I Sec.8.7 (5)	3. System hardware specification
Vol I Sec.8.7 (6)	4. Software design and specification
Vol I Sec.8.7 (7)	5. System security specification
Vol I Sec.8.7 (8)	6. Syste test and verification specification
Vol I Sec.8.7 (9)	7. System Operational procedures
Vol I Sec.8.7 (A)	8. System Maintenance Procedures
Vol I Sec.8.7 (B)	9. Personnel deployment and training requirements

TDP Requirements List

Requirement ID	Description
Vol I Sec.8.7 (C)	10. Configuration Management Plan
Vol I Sec.8.7 (D)	11. Quality Assurance Program
Vol I Sec.8.7 (E)	12 System Change Notes
Vol I Sec.9.1.3	<p>Configuration Management, Application of Configuration Management Requirements Requirements for configuration management apply to all components of voting systems regardless of the specific technologies employed. These components include:</p> <ul style="list-style-type: none"> a. Software b. Hardware c. Communication d. Documentation; e. Identification and naming and conventions (including changes to these conventions) for software programs and data files; f. Development and testing artifacts such as test data and scripts; g. File archiving and data repositories.
Vol I Sec.9.2.1	<p>Overview of Qualification Tests, Documentation Submitted by the 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.</p>
Vol I Sec.9.2.2	<p>Configuration Management Policy The vendor shall describe its policies for configuration management in the Technical Data Package. This description shall address the following elements:</p> <ul style="list-style-type: none"> • Scope and nature of configuration management program activities • Breadth of application of the vendor's policies and practices to the voting system, i.e., extent to which policies and practices apply to the total system, and extent to which policies and practices of suppliers apply to particular components, subsystems or other defined system elements
Vol I Sec.9.3 a	<p>Overview of Qualification Tests, Voting Equipment Submitted by Vendor The system submitted for testing shall meet the following requirements:</p> <ul style="list-style-type: none"> a. The hardware submitted for qualification shall be equivalent, in form and function, to the actual production versions of the hardware units or the COTS hardware specified for use in the TDP;
Vol I Sec.9.3 c-2	<ul style="list-style-type: none"> 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.
Vol I Sec.9.3.1	<p>Classification and Naming Configuration Items The vendor shall describe the procedures and conventions used to classify configuration items into categories and subcategories, uniquely number or otherwise identify configuration items and name configuration items.</p>
Vol I Sec.9.3.2 a	<p>Configuration Identification, Versioning Conventions When a system component is used to identify higher-level system elements, a vendor shall describe the conventions used to:</p> <ul style="list-style-type: none"> a. Identify the specific versions of individual configuration items and set of items that are used by the vendor to identify higher level system elements such as subsystems;
Vol I Sec.9.3.2 b	<ul style="list-style-type: none"> b. Uniquely number or otherwise identify versions; and
Vol I Sec.9.3.2 c	<ul style="list-style-type: none"> c. Name versions.
Vol I Sec.9.4 a	<p>Baseline and Promotion Procedures The vendor shall establish formal procedures and conventions for establishing and providing a complete description of the procedures and related conventions used to:</p> <ul style="list-style-type: none"> a. Establish a particular instance of a component as the starting baseline
Vol I Sec.9.4 b	<p>Baseline and Promotion Procedures</p> <ul style="list-style-type: none"> b. Promote subsequent instances of a component to baseline status as development progresses through to completion of the initial completed version released to the accredited test lab for testing
Vol I Sec.9.4 c	<p>Baseline and Promotion Procedures</p> <ul style="list-style-type: none"> c. Promote subsequent instances of a component to baseline status as the component is maintained throughout its life cycle until system retirement (i.e., the system is no longer sold or maintained by the vendor)
Vol I Sec.9.5 a	<p>The vendor shall establish such procedures and related conventions, providing a complete description of those procedures used to:</p> <ul style="list-style-type: none"> a. Develop and maintain internally developed items

TDP Requirements List

Requirement ID	Description
Vol I Sec.9.5 b	b. Acquire and maintain third-party items
Vol I Sec.9.5 c	c. Resolve internally identified defects for items regardless of their origin
Vol I Sec.9.5 d	d. Resolve externally identified and reported defects (i.e., by customers and accredited test labs)
Vol I Sec.9.6 a	Release Process The vendor shall establish such procedures and related conventions, providing a complete description of those used to: a. Perform a first release of the system to an accredited test lab
Vol I Sec.9.6 b	Release Process b. Perform a subsequent maintenance or upgrade release of the system or particular components, to an accredited test lab
Vol I Sec.9.6 c	Release Process c. Perform the initial delivery and installation of the system to a customer, including confirmation that the installed version of the system matches exactly the certified system version
Vol I Sec.9.6 d	Release Process d. Perform a subsequent maintenance or upgrade release of the system or a particular component to a customer, including confirmation that the installed version of the system matches exactly the certified system version
Vol I Sec.9.6.2.1 a	Qualification Testing, Qualification Test Plan The ITA shall prepare a Qualification Test Plan to define all tests and procedures required to demonstrate compliance with the Standards, including: a. Verifying or checking equipment operational status by means of manufacturer operating procedures;
Vol I Sec.9.6.2.1 f	f. Confirming that documentation submitted by the vendor corresponds to the actual configuration and operation of the system; and
Vol I Sec.9.6.2.1 g	g. Confirming that documented vendor practices for quality assurance and configuration management comply with the Standards.
Vol I Sec.9.7.1 a	Configuration Audits, Physical Configuration Audit For the PCA, a vendor shall provide: a. Identification of all items that are to be a part of the software release;
Vol I Sec.9.7.1 b	b. Specification of compiler (or choice of compilers) to be used to generate executable programs;
Vol I Sec.9.7.1 c	c. Identification of all hardware that interfaces with the software;
Vol I Sec.9.7.1 d	d. Configuration baseline data for all hardware that is unique to the system;
Vol I Sec.9.7.1 e	e. Copies of all software documentation intended for distribution to users, including program listings, specifications, operations manual, voter manual, and maintenance manual;
Vol I Sec.9.7.1 f	f. User acceptance test procedures and acceptance criteria;
Vol I Sec.9.7.1 g	g. Identification of any changes between the physical configuration of the system submitted for the PCA and that submitted for the FCA, with a certification that any differences do not degrade the functional characteristics
Vol I Sec.9.7.1 h	h. Complete descriptions of its procedures and related conventions used to support this audit by: i. Establishing a configuration baseline of the software and hardware to be tested; and ii. Confirming whether the system documentation matches the corresponding system components.
Vol I Sec.9.7.2 a	Configuration Audits, Functional Configuration Audit The FCA is conducted by the ITA to verify that the system performs all the functions described in the system documentation. The vendor shall: a. Completely describe its procedures and related conventions used to support this audit for all system components;
Vol I Sec.9.7.2 b	b. Provide the following information to support this audit: i. Copies of all procedures used for module or unit testing, integration testing, and system testing; ii. Copies of all test cases generated for each module and integration test, and sample ballot formats or other test cases used for systems tests iii. Records of all tests performed by the procedures listed above, including error corrections and retests.

TDP Requirements List

Requirement ID	Description
Vol I Sec.9.8	<p>Configuration Management Resources</p> <p>The resources documentation requirements focus on assuring that procedures are in place to record information about the tools to help ensure that they, and the data they contain, can be transferred effectively and promptly to a third party should the need arise. Within this context, a vendor is required to develop and provide a complete description of the procedures and related practices for maintaining information about:</p> <ul style="list-style-type: none"> a. Specific tools used, current version, and operating environment specifications b. Physical location of the tools, including designation of computer directories and files c. Procedures and training materials for using the tools
Vol II Sec.2.1	<p>Technical Data Package, Scope</p> <p>If the vendor's developmental test data is incomplete, the test agency shall design and conduct the appropriate tests.</p>
Vol II Sec.2.1.1	<p>Technical Data Package, Scope</p> <p>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.</p> <p>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).</p>
Vol II Sec.2.1.2	<p>Technical Data Package, Scope</p> <p>Both formal documentation and notes of the vendors system development process shall be submitted for qualification tests.</p>
Vol II Sec.2.1.1.3	<p>Scope, Content and Format</p> <p>The vendor shall list all documents controlling the design, construction, operation, and maintenance of the system. Documents shall be listed in order of precedence.</p>
Vol II Sec.2.1.1.1 a	<p>Scope, Required Content for Initial Qualification</p> <p>At a minimum, the TDP shall contain the following documentation:</p> <p>(a) System configuration overview;</p>
Vol II Sec.2.1.1.1 b	<p>(b) System functionality description;</p>
Vol II Sec.2.1.1.1 c	<p>(c) System hardware specifications;</p>
Vol II Sec.2.1.1.1 d	<p>(d) Software design and specifications;</p>
Vol II Sec.2.1.1.1 e	<p>(e) System and test verification specifications;</p>
Vol II Sec.2.1.1.1 f	<p>(f) System security specifications;</p>
Vol II Sec.2.1.1.1 g	<p>(g) User/system operations procedures;</p>
Vol II Sec.2.1.1.1 h	<p>(h) System maintenance procedures;</p>
Vol II Sec.2.1.1.1 i	<p>(i) Personnel deployment and training requirements;</p>
Vol II Sec.2.1.1.1 j	<p>(j) Configuration management plan;</p>
Vol II Sec.2.1.1.1 k	<p>(k) Quality assurance program, and</p>
Vol II Sec.2.1.1.1 l	<p>(l) System change notes.</p>
Vol II Sec.2.1.1.2 1	<p>Scope, Required Content for System Changes and Re-Qualification</p> <p>For systems seeking re-qualification, vendors shall submit System Change Notes as described in Section 2.13, as well as current revisions of all documents that have been updated to reflect system changes.</p>
Vol II Sec.2.1.1.2 2	<p>Scope, Required Content for System Changes and Re-Qualification</p> <p>Systems in existence at the time of the revised standards are released may not have all required developmental documentation. When such a system is subject to evaluation as a result of system modification, the vendor shall provide what information they can.</p>
Vol II Sec.2.1.1.3 1	<p>Scope, Format</p> <p>The TDP shall include a detailed table of contents for the required documents, an abstract of each document and listing of each of the informational sections and appendices presented within each.</p>
Vol II Sec.2.1.1.3 2	<p>Scope, Format 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.</p>

TDP Requirements List

Requirement ID	Description
Vol II Sec.2.1.3 1	<p>Scope, Protection of Proprietary Information</p> <p>Any person or test agency receiving proprietary information shall agree to use it solely for the purpose of analyzing and testing the system, and shall agree to refrain from otherwise using the proprietary information or disclosing it to any other person or agency without the prior written consent of the vendor, unless disclosure is legally compelled.</p>
Vol II Sec.2.1.3 2	<p>Scope, Protection of Proprietary Information</p> <p>The vendor shall identify all documents, or portions of documents, containing proprietary information not approved for public release.</p>
Vol II Sec.2.2	<p>Technical Data Package, System Overview</p> <p>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.</p>
Vol II Sec.2.2.1 a	<p>System Overview, System Description</p> <p>The system description shall include paragraphs, drawings, and diagrams that represent:</p> <p>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);</p>
Vol II Sec.2.2.1 b	<p>b. A description of the operational environment of the system that provides an overview of the hardware, software, and communications structure;</p>
Vol II Sec.2.2.1 c	<p>c. A theory of operation that explains each system function, and how the function is achieved in the design;</p>
Vol II Sec.2.2.1 d	<p>d. Descriptions of the functional and physical interfaces between subsystems and components;</p>
Vol II Sec.2.2.1 e	<p>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 component, including:</p> <ol style="list-style-type: none"> (1) Operating systems; (2) Database software; (3) Communications routers; (4) Modem drivers; and (5) Dial-up networking software;
Vol II Sec.2.2.1 f	<p>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:</p> <ol style="list-style-type: none"> 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;
Vol II Sec.2.2.1 g	<p>(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.</p>
Vol II Sec.2.2.2 a	<p>System Overview, System Performance: The vendor shall provide system performance information that includes descriptions of:</p> <p>a. The performance characteristics of each operating mode and function in terms of expected and maximum speed, throughput capacity, maximum volume (maximum number of voting positions and maximum number of ballot styles represented), and processing frequency.</p>
Vol II Sec.2.2.2 b	<p>b. Quality attributes such as reliability, maintainability, usability, availability, and portability;</p>
Vol II Sec.2.2.2 c	<p>c. Provisions for safety, security, privacy, and continuity of operation; and</p>
Vol II Sec.2.2.2 d	<p>d. Design constraints, applicable standards, and compatibility requirements.</p>
Vol II Sec.2.3 1	<p>Technical Data Package, System Functionality Description</p> <p>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.</p>
Vol II Sec.2.3 2	<p>Technical Data Package, System Functionality Description</p> <p>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.</p>
Vol II Sec.2.3 3	<p>Technical Data Package, System Functionality Description</p> <p>This listing shall provide a simple description of each capability.</p> <p>Detailed specifications shall be provided in other documentation required for the TDP as indicated by the standards for that documentation.</p>
Vol II Sec.2.3 a	<p>Technical Data Package, System Functionality Description</p> <p>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 [Functional Capabilities] 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;</p>

TDP Requirements List

Requirement ID	Description
Vol II Sec.2.3 b	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;
Vol II Sec.2.3 c	c. Required capabilities that may be bypassed or deactivated during installation or operation by the user shall be clearly indicated;
Vol II Sec.2.3 d	d. Additional capabilities that function only when activated during installation or operation by the user shall be clearly indicated; and
Vol II Sec.2.3 e	e. Additional capabilities that normally are active but may be bypassed or deactivated during installation or operation by the user shall be clearly indicated.
Vol II Sec.2.5	Technical Data Package, 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.
Vol II Sec.2.5.1	Software Design and Specification, 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.
Vol II Sec.2.5.2	Software Design and Specification, 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.
Vol II Sec.2.5.3	Software Design and Specification, Software Overview The vendor shall also include a certification that procured software items were obtained directly from the manufacturer, or a licensed dealer or distributor.
Vol II Sec.2.5.3 a	Software Design and Specification, 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;
Vol II Sec.2.5.3 b	b. The general design, operational considerations, and constraints influencing the design of the software;
Vol II Sec.2.5.3 c	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 to the software and to the default configuration options;
Vol II Sec.2.5.3 d	d. Additional information for each item that includes: (1) Item identification; (2) General description; (3) Software requirements performed by the user; (4) Identification of interfaces with other items provide data to, or receive data from, the item; and (5) Concept of execution for the item.
Vol II Sec.2.5.4 1	Software Design and Specification, Software Standards and Conventions The vendor shall provide information that can be used by an ITA or state certification board to support software analysis and test design.
Vol II Sec.2.5.4 2	Software Design and Specification, Software Standards and Conventions 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.
Vol II Sec.2.5.4 a	Software Design and Specification, Software Standards and Conventions The vendor shall provide information that addresses the following standards and conventions: a. System development methodology;
Vol II Sec.2.5.4 b	b. Software design standards, including internal vendor procedures;
Vol II Sec.2.5.4 c	c. Software specification standards, including internal vendor procedures;
Vol II Sec.2.5.4 d	d. Software coding standards, including internal vendor procedures;
Vol II Sec.2.5.4 e	e. Software testing and verification standards, including internal vendor procedures, that can assist in determining the program's correctness and ACCEPT/REJECT criteria;

TDP Requirements List

Requirement ID	Description
Vol II Sec.2.5.4 f	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.
Vol II Sec.2.5.5	Software Design and Specification, Software Operating Environment This section shall describe or make reference to all operating environment factors that influence the software design.
Vol II Sec.2.5.5.1 a	Software Design and Specification, 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;
Vol II Sec.2.5.5.1 b	b. Memory read-write characteristics;
Vol II Sec.2.5.5.1 c	c. External memory device characteristics;
Vol II Sec.2.5.5.1 d	d. Peripheral device interface hardware;
Vol II Sec.2.5.5.1 e	e. Data input/output device protocols; and
Vol II Sec.2.5.5.1 f	f. Operator controls, indicators, and displays.
Vol II Sec.2.5.5.2	Software Design and Specification, 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.
Vol II Sec.2.5.6	Software Design and Specification, Software Functional Specification The vendor shall provide a description of the operating modes of the system and of software capabilities to perform specific functions.
Vol II Sec.2.5.6.1	Software Design and Specification, 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.
Vol II Sec.2.5.6.1 a	Software Design and Specification, Configurations and Operating Modes 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);
Vol II Sec.2.5.6.1 b	b. An explanation of how the inputs are processed, and;
Vol II Sec.2.5.6.1 c	c. A definition of the outputs produced, (again with characteristics, tolerances, or acceptable ranges as applicable).
Vol II Sec.2.5.6.2 a	Software Design and Specification, Software Functions The vendor shall describe the software's capabilities or methods for detecting or handling a. Exception conditions;
Vol II Sec.2.5.6.2 b	b. System failures.
Vol II Sec.2.5.6.2 c	c. Data input/output errors;
Vol II Sec.2.5.6.2 d	d. Error logging for audit record generation;
Vol II Sec.2.5.6.2 e	e. Production of statistical ballot data;
Vol II Sec.2.5.6.2 f	f. Data quality assessment; and
Vol II Sec.2.5.6.2 g	g. Security monitoring and control.
Vol II Sec.2.5.7	Software Design and Specification, Programming Specification 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.
Vol II Sec.2.5.7.1 1	Programming Specifications, 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.
Vol II Sec.2.5.7.1 2	Programming Specifications, Programming Specifications Overview Implementation of the functions shall be described in terms of the software architecture, algorithms, and data structures.

TDP Requirements List

Requirement ID	Description
Vol II Sec.2.5.7.1 3	Programming Specifications, Programming Specifications Overview This section shall be prepared to facilitate understanding of the internal functioning of the individual software modules.
Vol II Sec.2.5.7.2	Programming Specifications, Programming Specifications Details The programming specifications shall describe individual software modules and their component units, if applicable.
Vol II Sec.2.5.7.2 a	Programming Specifications, Programming Specifications Details For each module and unit, the vendor shall provide the following information: a. Module and unit design decisions, if any, such as algorithms used;
Vol II Sec.2.5.7.2 b	b. Any constraints, limitations, or unusual features in the design of the software module or unit;
Vol II Sec.2.5.7.2 c	c. The programming language to be used and rationale for its use if other than the specified module or unit language;
Vol II Sec.2.5.7.2 d	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;
Vol II Sec.2.5.7.2 e	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.
Vol II Sec.2.5.7.2 f	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 model 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; and 5) Exception and error handling.
Vol II Sec.2.5.7.2 g	g. If the software module is a database, provide the information described in Volume II Section 2.5.8.
Vol II Sec.2.5.8	Software Design and Specifications, 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.
Vol II Sec.2.5.8 a	Software Design and Specifications, System Database 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):
Vol II Sec.2.5.8 b	b. Design conventions and standards (which may be incorporated by references) needed to understand the design;
Vol II Sec.2.5.8 c	c. Identification and description of all database entities and how they are implemented physically (e.g. tables, files, etc.);
Vol II Sec.2.5.8 d	d. Entity relationship diagram and description of relationships;
Vol II Sec.2.5.8 e	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); and
Vol II Sec.2.5.8 f	f. For external files, a description of the procedures for file maintenance, management of access privileges, and security.

TDP Requirements List

Requirement ID	Description
Vol II Sec.2.5.9	Software Design and Specifications, Interfaces The vendor shall identify and provide a complete description of all internal and external interfaces, using a combination of text and diagrams.
Vol II Sec.2.5.9.1 a	Interfaces, Interface Identification For each interface identified in the system overview, the vendor shall provide: a. Provide a unique identifier assigned to the interface;
Vol II Sec.2.5.9.1 b	b. Identify the interfacing entities (systems, configuration items, users, etc.) by name, number, version, and documentation references, as applicable, and;
Vol II Sec.2.5.9.1 c	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).
Vol II Sec.2.5.9.2 a	Interfaces, 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;
Vol II Sec.2.5.9.2 b	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);
Vol II Sec.2.5.9.2 c	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;
Vol II Sec.2.5.9.2 d	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) Legality checks, error control, and recover procedures; 4) Synchronization, including connection establishment, maintenance, termination, and 5) Status identification, and any other reporting features; and File note: Item no. 3 was duplicated in Standard
Vol II Sec.2.5.9.2 e	e. Other characteristics, such as physical compatibility of the interfacing entity(ies) (dimensions, tolerances, loads, voltages, plug compatibility, etc).
Vol II Sec.2.5.A	Software Design and Specification, 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 appendixes shall be at the discretion of the vendor.
Vol II Sec.2.6 1	Technical Data Package, System Security Specification 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.
Vol II Sec.2.6 2	Technical Data Package, System Security Specification 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 Access Control Policy; 2.6.2 Access Control Measures, 2.6.3 Equipment and Data Security; [hardware] 2.6.4 Software Installation; 2.6.5 Telecommunications and Data Transmission Security; 2.6.6 Other Elements of an Effective Security System):

TDP Requirements List

Requirement ID	Description
Vol II Sec.2.6.3	<p>Software Design and Specifications, System Security Specification</p> <p>This specification shall describe the level of security provided by the system in terms of 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 [Telecommunications], the means used to keep the security capabilities of the system current to respond to the evolving threats against those systems.</p>
Vol II Sec.2.6.4	<p>Technical Data Package, System Security Specificatio</p> <p>Vendors shall submit a system security specification that addresses the security requirements of Volume I, Section 6 [Security Standards] of the Standards.</p>
Vol II Sec.2.6.1	<p>System Security Specification, Access Control Policy</p> <p>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 6.2.1 [Access Control Policy]. The access control policy shall address the general features and capabilities and individual access privileges indicated in Volume I, Section 6.2.1.</p>
Vol II Sec.2.6.2.1	<p>System Security Specification, Access Control Measures</p> <p>The vendor shall also define and provide a detailed description of the methods used to preclude unauthorized access to the access control capabilities of the system itself.</p>
Vol II Sec.2.6.2.2	<p>System Security Specification, Access Control Measures</p> <p>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 6.2.2 [Access Control Measures].</p>
Vol II Sec.2.6.3	<p>System Security Specification, Equipment and Data Security</p> <p>The vendor shall provide a detailed description of system capabilities and mandatory procedures for purchasing jurisdictions to prevent disruption of voting process and corruption of voting data to meet specific requirements of Volume I, Section 6.3 [Physical Security Measures] of the Standards.</p> <p>This information shall address measures for polling place security and central count location security.</p>
Vol II Sec.2.6.4.1	<p>System Security Specification, Software Installation</p> <p>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 [Software Security] of the Standards.</p>
Vol II Sec.2.6.4.2	<p>System Security Specification, Software Installation</p> <p>This information shall address software installation for all system components.</p>
Vol II Sec.2.6.5 a	<p>System Security Specification, Telecommunications and Data Transmission Security</p> <p>The vendor shall provide a detailed description of the system capabilities and mandatory procedures for purchasing jurisdictions to ensure data transmission to meet the specific requirements of Volume I, Section 6.5 [Telecommunications and Data Transmission]:</p> <p>a. For all systems, this information shall address access control, and prevention of data interception; and</p>
Vol II Sec.2.6.5 b 1	<p>b. For systems that use public communications networks as defined in Volume I, Section 5 [Telecommunications], this information shall also include:</p> <ol style="list-style-type: none"> 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; <p>continued below</p>
Vol II Sec.2.6.5 b 2	<p>continued from above</p> <p>b. For systems that use public communications networks as defined in Volume I, Section 5 [Telecommunications], this information shall also include:</p> <ol style="list-style-type: none"> 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 operations 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.
Vol II Sec.2.6.6	<p>System Security Specification, Other Elements of an Effective Security Program</p> <p>The documentation shall be prepared such that these requirements can be integrated by the jurisdiction into local administrative and operating procedures.</p>

TDP Requirements List

Requirement ID	Description
Vol II Sec.2.6.6 a	System Security Specification, 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;
Vol II Sec.2.6.6 b	b. Internal security procedures, including operating procedures for maintaining the security of the software for each system function and operating mode;
Vol II Sec.2.6.6 c	c. Adherence to, and enforcement of, operational procedures (e.g. effective password management);
Vol II Sec.2.6.6 d	d. Physical facilities and arrangements; and
Vol II Sec.2.6.6 e	e. Organizational responsibilities and personnel screening.
Vol II Sec.2.7 a	Technical Data Package, System Test and Verification Specification The vendor shall provide two types of test and verification specifications: a. Development test specifications; and
Vol II Sec.2.7 b	b. Qualification test specifications.
Vol II Sec.2.7.1 1	System Test and Verification Specification, Development Test Specifications The vendor shall describe the plans, procedures, and data used during the software development and system integration to verify system logic correctness, data quality, and security.
Vol II Sec.2.7.1 2	System Test and Verification Specification, Development Test Specifications 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.
Vol II Sec.2.7.1 a 1	System Test and Verification Specification, Development Test Specifications a. Standard test procedures, including any assumptions or constraints; File Note: Letter 'a' used twice
Vol II Sec.2.7.1 a 2	System Test and Verification Specification, Development Test Specifications This description shall include: a. Test identification and design, including: 1) Test structure; 2) Test sequence or progression; 3) Test conditions;
Vol II Sec.2.7.1 b	b. Special purpose test procedures including any assumptions or constraints;
Vol II Sec.2.7.1 c	c. Test data; including the data source, whether it is real or simulated, and how test data is controlled;
Vol II Sec.2.7.1 d	d. Expected test results;
Vol II Sec.2.7.1 e	e. Criteria for evaluating test results.
Vol II Sec.2.7.2 1	System Test and Verification Specification, Qualification Test Specifications The specifications shall identify procedures for assessing and demonstrating the suitability of the software for elections use.
Vol II Sec.2.7.2 2	System Test and Verification Specification, Qualification Test Specifications The vendor shall provide specifications for verification and validation of overall software performance.
Vol II Sec.2.7.2 a	System Test and Verification Specification, Qualification Test Specifications These specifications shall cover a. Control and data input/output;
Vol II Sec.2.7.2 b	b. Acceptance criteria;
Vol II Sec.2.7.2 c	c. Processing accuracy;
Vol II Sec.2.7.2 d	d. Data quality assessment and maintenance;
Vol II Sec.2.7.2 e	e. Ballot interpretation logic;
Vol II Sec.2.7.2 f	f. Exception handling;
Vol II Sec.2.7.2 g	g. Security; and

TDP Requirements List

Requirement ID	Description
Vol II Sec.2.7.2 h	h. Production of audit trails and statistical data.
Vol II Sec.2.8 1	Technical Data Package, System Operations Procedures 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; 2.8.2 Operational Environment; 2.8.3 System Installation and Test Specification; 2.8.4 Operational Features; 2.8.5 Operating Procedures; 2.8.6 Operations Support; 2.8.7 Appendices)
Vol II Sec.2.8 2	Technical Data Package, 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 [System Functionality Description] above. The nature of the instructions for operating personnel will depend on the overall system design and required skill level of system operations support personnel.
Vol II Sec.2.8.1 1	System Operations Procedures, 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.
Vol II Sec.2.8.1 2	System Operations Procedures, Introduction The roles of operating personnel shall be identified and related to the operating modes of the system.
Vol II Sec.2.8.1 3	System Operations Procedures, Introduction Decision criteria and conditional operator functions (such as a error and failure recovery actions) shall be described.
Vol II Sec.2.8.1 4	System Operations Procedures, Introduction The vendor shall also list all reference and supporting documents pertaining to the use of the system during elections operations.
Vol II Sec.2.8.2	System Operations Procedures, Operational Environment The vendor shall describe the system environment, and the interface between the user or operator and the system.
Vol II Sec.2.8.2 a	System Operations Procedures, Operational Environment The vendor shall identify all facilities, furnishings, fixtures, and utilities that will be required for equipment operations, including equipment that operates: a. Polling place;
Vol II Sec.2.8.2 b	b. Central count facility; and
Vol II Sec.2.8.2 c	c. Other locations.
Vol II Sec.2.8.3	System Operations Procedures, System Installation and Test Specification The vendor shall provide specifications for validation of system installation, acceptance, and readiness.
Vol II Sec.2.8.3 a	System Operations Procedures, System Installation and Test Specification 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;
Vol II Sec.2.8.3 b	b. Voting functions;
Vol II Sec.2.8.3 c	c. Post-voting functions; and
Vol II Sec.2.8.3 d	d. General capabilities.
Vol II Sec.2.8.4 a	System Operations Procedures, 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;
Vol II Sec.2.8.4 b	b. Provide examples of simulated interactions in order to facilitate understanding of the system and its capabilities;
Vol II Sec.2.8.4 c	c. Provide sample data formats and output reports; and
Vol II Sec.2.8.4 d	d. Illustrate and describe all status indicators and information messages.
Vol II Sec.2.8.5 a	System Operations Procedures, 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;

TDP Requirements List

Requirement ID	Description
Vol II Sec.2.8.5 b	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);
Vol II Sec.2.8.5 c	c. Provides procedures that clearly enable the operator to intervene the system operations to recover from an abnormal system state;
Vol II Sec.2.8.5 d	d. Defines and illustrates the procedures and system prompts for situations where operator intervention is required to load, initialize, and start the system;
Vol II Sec.2.8.5 e	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);
Vol II Sec.2.8.5 f	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;
Vol II Sec.2.8.5 g	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
Vol II Sec.2.8.5 h	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 system states.
Vol II Sec.2.8.6 a	System Operations Procedures, 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
Vol II Sec.2.8.6 b	b. Describe procedures for providing technical support, system maintenance and correction of defects, and for incorporating hardware upgrades and new software releases.
Vol II Sec.2.8.7	System Operations Procedures, 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.
Vol II Sec.2.9 1	Technical Data Package, 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.
Vol II Sec.2.9 2	Technical Data Package, System Maintenance Procedures 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.
Vol II Sec.2.9 3	Technical Data Package, System Maintenance Procedures This manual shall include the sections listed below [2.9.1 Introduction, 2.9.2 Maintenance Procedures, 2.9.2.1 Preventive Maintenance Procedures, 2.9.2.2 Corrective Maintenance Procedures, 2.9.3 Maintenance Equipment, 2.9.4 Parts and Materials, 2.9.4.1 Common Standards, 2.9.4.2 Paper-Based Systems, 2.9.5 Maintenance Facilities and Support, 2.9.6 Appendices].
Vol II Sec.2.9.1	System Maintenance Procedures, 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.
Vol II Sec.2.9.1 a	System Maintenance Procedures, Introduction The description shall include a theory of operation that fully describes such items as: a. The electrical and mechanical functions of the equipment;
Vol II Sec.2.9.1 b	b. How the processes of ballot handling and reading are performed (paper-based systems);
Vol II Sec.2.9.1 c	c. How vote selection and casting of the paper ballot are performed (DRE systems);
Vol II Sec.2.9.1 d	d. How transmission of data over a network are [is] performed (DRE systems, where applicable);
Vol II Sec.2.9.1 e	e. How data are [is] handled in the processor and memory units;
Vol II Sec.2.9.1 f	f. How data output is initiated and controlled;

TDP Requirements List

Requirement ID	Description
Vol II Sec.2.9.1 g	g. How power is converted or conditioned; and
Vol II Sec.2.9.1 h	h. How test and diagnostic information is acquired and used.
Vol II Sec.2.9.2	System Maintenance Procedures, Maintenance ProceduresThe vendor shall describe preventive and corrective maintenance procedures for hardware and software.
Vol II Sec.2.9.2.1 a	Maintenance Procedures, Preventive Maintenance ProceduresThe 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;
Vol II Sec.2.9.2.1 b	b. Number and skill levels of personnel required for each task;
Vol II Sec.2.9.2.1 c	c. Parts, supplies, special maintenance equipment, software tools, or other resources needed for maintenance, and;
Vol II Sec.2.9.2.1 d	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).
Vol II Sec.2.9.2.2 1	Maintenance Procedures, Corrective Maintenance ProceduresThe vendor shall identify specific procedures to be used in diagnosing and correcting problems in the system hardware (or user-controlled software).
Vol II Sec.2.9.2.2 2	Maintenance Procedures, 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.
Vol II Sec.2.9.2.2 a	Maintenance Procedures, Corrective Maintenance Procedures Descriptions shall include: a. Steps to replace failed or deficient equipment;
Vol II Sec.2.9.2.2 b	b. Steps to correct deficiencies or faulty operations in software;
Vol II Sec.2.9.2.2 c	c. Modifications that are necessary to coordinate any modified or upgraded software with other software modules;
Vol II Sec.2.9.2.2 d	d. The number and skill levels of personnel needed to accomplish each procedure;
Vol II Sec.2.9.2.2 e	e. Special maintenance equipment, parts, supplies, or other resources needed to accomplish each procedure; and
Vol II Sec.2.9.2.2 f	f. Any coordination required with the vendor, or other party for off-the-shelf items.
Vol II Sec.2.9.3	System Maintenance Procedures, Maintenance Equipment The vendor shall identify and describe any special purpose tests or maintenance equipment recommended for fault isolation and diagnostic purposes.
Vol II Sec.2.9.4	Maintenance Procedures, Parts and MaterialsVendors shall provide detailed documentation of parts and materials needed to operate and maintain the system.
Vol II Sec.2.9.4.1	Parts and Materials, Common StandardsThe vendor shall provide a complete list of approved parts and materials needed for maintenance.
Vol II Sec.2.9.4.1 a-f	Parts and Materials, Common Standards 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.
Vol II Sec.2.9.4.2 1	Parts and Materials, Paper-Based SystemFor marking devices manufactured by multiple external sources, the vendor shall provide a listing of sources and model numbers that are compatible with the system.
Vol II Sec.2.9.4.2 2	Parts and Materials, Paper-Based Systems The TDP shall specify the required paper stock, size, shape, opacity, color, watermarks, field layout, orientation, size and style of printing, size and location of punch or mark fields used for vote response fields and to identify unique ballot formats, placement of alignment marks, ink for printing, and folding and bleed-through limitations for preparation of ballots that are compatible with the system.
Vol II Sec.2.9.5 1	System Maintenance Procedures, Maintenance Facilities and Support The vendor shall identify all facilities, furnishings, fixtures, and utilities that will be required for equipment maintenance.

TDP Requirements List

Requirement ID	Description
Vol II Sec.2.9.5.2	System Maintenance Procedures, Maintenance Facilities and Support In addition, vendors shall specify the assumptions made with regard to any parameters that impact the mean time to repair.
Vol II Sec.2.9.5 a-c	System Maintenance Procedures, Maintenance Facilities and Support 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.
Vol II Sec.2.A	Technical Data Package, Personnel Deployment and Training Requirements The vendor shall describe the personnel resources and training required for a jurisdiction to operate and maintain the system.
Vol II Sec.2.A.1	Personnel Deployment and Training Requirements, Personnel A description shall be presented of which functions may be carried out by user personnel, and those that must be performed by vendor personnel.
Vol II Sec.2.A.1 a	Personnel Deployment and Training Requirements, 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);
Vol II Sec.2.A.1 b	b. System operations for voting system functions performed at the polling place;
Vol II Sec.2.A.1 c	c. System operations for voting system functions performed at the central count facility;
Vol II Sec.2.A.1 d	d. Preventive maintenance tasks;
Vol II Sec.2.A.1 e	e. Diagnosis of faulty hardware or software;
Vol II Sec.2.A.1 f	f. Corrective maintenance tasks; and
Vol II Sec.2.A.1 g	g. Testing to verify the correction of problems.
Vol II Sec.2.A.2 a	Personnel Deployment and Training Requirements, Training The vendor shall specify requirements for the orientation and training of the following personnel: a. Poll workers supporting polling place operations;
Vol II Sec.2.A.2 b	b. System support personnel involved in election programming;
Vol II Sec.2.A.2 c	c. User system maintenance technicians;
Vol II Sec.2.A.2 d	d. Network/system administration personnel (if a network is used);
Vol II Sec.2.A.2 e	e. Data personnel; and
Vol II Sec.2.A.2 f	f. Vendor personnel.
Vol II Sec.2.B 1	Technical Data Package, Configuration Management Plan Vendors shall submit a Configuration Management Plan that address the configuration management requirements of Volume I, Section 8 [Configuration Management] 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.
Vol II Sec.2.B 2	Technical Data Package, Configuration Management Plan The Configuration Management Plan Shall contain the sections identified below: (2.11.1 Configuration Management Policy; 2.11.2 Configuration Identification; 2.11.3 Baseline, Promotion, and Demotion Procedures; 2.11.4 Configuration Control Procedures; 2.11.5 Release Process; 2.11.6 Configuration Audits; 2.11.7 Configuration Management Resources)
Vol II Sec.2.B.1 a	Configuration Management Plan, 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 [8.2 Configuration Management Policy] of the Standards. These requirements pertain to: a. Scope and nature of configuration management program activities; and File note: should read 'Volume I Section 8.2'.

TDP Requirements List

Requirement ID	Description
Vol II Sec.2.B.1 b	b. Breadth of application of vendor's policy and practices to the voting system (i.e., extent to which policies and practices apply to the total system, and extent to which policies and practices of suppliers apply to particular components, subsystems, or other defined system elements). [Italicized section from Volume I, Section 8.2
Vol II Sec.2.B.2 a	Configuration Management Plan, 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 [8.3 Configuration Identification] of the Standards. These requirements pertain to: a. Classifying configuration items into categories and subcategories;File note: Should read 'Volume I Section 8.3'.
Vol II Sec.2.B.2 b	b. Uniquely numbering or otherwise identifying configuration items; and
Vol II Sec.2.B.2 c	c. Naming configuration items.
Vol II Sec.2.B.3 a	Configuration Management Plan, 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 [8.4 Baseline, Promotion, and Demotion Procedures] of the standards. These requirements pertain to: a. Establishing a particular instance of a system component as the starting baseline; File note: Should read 'Volume I Section 8.4'.
Vol II Sec.2.B.3 b	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
Vol II Sec.2.B.3 c	c. Promoting subsequent instances of a component to baseline status as the component is maintained throughout its life cycle (until system retirement, i.e., the system is no longer sold or maintained by the vendor).[Italicized section from Vol. I, Section 8.4]
Vol II Sec.2.B.4 a	Configuration Management Plan, 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 [8.5 Configuration Control Procedures] of the Standards. These requirements pertain to: a. Developing and maintaining internally developed items;File note: Should read 'Volume I Section 8.5'
Vol II Sec.2.B.4 b	b. Developing and maintaining third-party items; File Note: Vol I Sec. 8.5b reads 'acquire and...'
Vol II Sec.2.B.4 c	c. Resolve internally identified defects for items regardless of their origin; and[Italicized section from Vol. I Section 8.5]
Vol II Sec.2.B.4 d	d. Resolve externally identified and reported defects (i.e. by customers and ITAs).File note: Italicized section from Vol. I Section 8.5
Vol II Sec.2.B.5	Configuration Management Plan, 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 [8.6 Release Process] of the Standards. File note: Should read 'Volume I Section 8.6'.
Vol II Sec.2.B.5 a	Configuration Management Plan, Release Process These requirements pertain to: a. A first release of the system to the ITA;
Vol II Sec.2.B.5 b	b. A subsequent maintenance or upgrade release of a system, or particular components, to an ITA;
Vol II Sec.2.B.5 c	c. The initial delivery and installation of the system to a customer (including confirmation that the installed version of the system matches exactly the qualified system version); and[Italicized section from Vol. I Section 8.6]
Vol II Sec.2.B.5 d	d. A subsequent maintenance or upgrade release of a system, or particular components, to a customer, including confirmation that the installed version of the system matches exactly the qualified system version.[Italicized section from Vol. I Section 8.6]
Vol II Sec.2.B.6	Configuration Management Plan, 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 [8.7 Configuration Audits] of the Standards. File note: Should read 'Volume I Section 8.7'.
Vol II Sec.2.B.6 a	Configuration Management Plan, Configuration AuditsThese requirements pertain to: a. Physical configuration audit that verifies the voting system components submitted for qualification to the vendor's technical documentation; and

TDP Requirements List

Requirement ID	Description
Vol II Sec.2.B.6 b	b. Functional configuration audit that verifies the system performs all the functions described in the system documentation.
Vol II Sec.2.B.7 a	Configuration Management Plan, 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 [8.8 Configuration Management Resources] of the Standards. These requirements pertain to information about:a. Specific tools used, current version, and operating environment;File note: Should read 'Volume I Section 8.8'.
Vol II Sec.2.B.7 b	b. Physical location of the tools, including designation of computer directories and files; and
Vol II Sec.2.B.7 c	c. Procedures and training materials for using the tools.
Vol II Sec.2.C 1	Technical Data Package, Quality Assurance Program Vendors shall submit a Quality Assurance Program that addresses the quality assurance requirements of Volume I, Section 7. This plan shall describe all the 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.
Vol II Sec.2.C 2	Technical Data Package, Quality Assurance Program The Quality Assurance Program shall, at a minimum, address the topics indicated below: (2.12.1 Quality Assurance Policy; 2.12.2 Parts & Materials Special Tests and Examinations [hardware]; 2.12.3 Quality Conformance Inspections; 2.12.4 Documentation)
Vol II Sec.2.C.1 a	Quality Assurance Program, 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
Vol II Sec.2.C.1 b	b. Breadth of application of vendors policy and practices to the voting system.
Vol II Sec.2.C.2	Quality Assurance Program, 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 7.5 [Parts& Materials Special Tests and Examinations]. File note: Should read 'Volume 1, Section 7.5'
Vol II Sec.2.C.3	Quality Assurance Program, 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 [7.6 Quality Conformance Inspections] of the Standards. File note: Should read 'Volume I, Section 7.6'
Vol II Sec.2.C.3 a	Quality Assurance Program, Quality Conformance Inspections The record of tests provided shall include for each test performed: a. Test location;
Vol II Sec.2.C.3 b	b. Test date;
Vol II Sec.2.C.3 c	c. Individual who conducted the test; and
Vol II Sec.2.C.3 d	d. Test outcomes.
Vol II Sec.2.C.4	Quality Assurance Program, 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 [7.7 Documentation] of the Standards.File note: Should read 'Volume I Section 7.7'
Vol II Sec.2.D 2	Quality Assurance Program, 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.
Vol II Sec.2.D a	Quality Assurance Program, System Change Notes The system change notes shall include the following information: a. Summary description of the nature and scope of the changes, and reasons for each change;
Vol II Sec.2.D b	b. A listing of the specific changes made, citing the specific system configuration items changed and providing detailed references to the sections of the documentation changed;
Vol II Sec.2.D c	c. The specific sections of the documentation that are changed (or complete revised documents, if more suitable to address a large number of changes);

TDP Requirements List

Requirement ID	Description
Vol II Sec.2.D d	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 the test results.
Vol II Sec.3.2.1 f-1	Breadth of Functionality Testing, Basic Functionality Testing Requirements 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 functionality testing performed by the ITA.
Vol II Sec.4.7.2 2a	Environmental Tests, Operating, Maintainability Test These tests include: a. Examine the physical attributes of the system to determine whether significant impediments exist for the performance of those maintenance activities that are to be performed by the jurisdiction. These activities shall be identified by the vendor in the system maintenance procedures (part of the TDP).
Vol II Sec.5.2-6	Software Testing, Basis of Software Testing 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 software testing performed by the ITA.
Vol II Sec.6.2.1 a	Basis of Integration Testing, Testing Breadth 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;
Vol II Sec.6.2.2-3	Basis of Integration Testing, 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.
Vol II Sec.6.4.2 1	Security Testing, 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.
Vol II Sec.6.6	System Level Integration Testing, Physical Configuration Audit The vendor shall provide a list of all documentation and data to be audited, cross-referenced to the contents of the TDP. Vendor personnel shall be available to assist in the performance of the Physical Configuration Audit.
Vol II Sec.6.6 a-1	System Level Integration Testing, 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 a guide when conducting this audit;
Vol II Sec.6.6 a-2	a. 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 a guide when conducting this audit;
Vol II Sec.6.6 b-1	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.
Vol II Sec.6.6 b-2	b. 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;
Vol II Sec.6.6 c-1	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.
Vol II Sec.6.6 c-2	c. This examination shall establish the system hardware baseline associated with the software baseline;
Vol II Sec.6.6 d	d. To assess the adequacy of user acceptance 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
Vol II Sec.6.6 e-1	e. All subsequent changes to the baseline software configuration made during the course of qualification testing shall be subject to reexamination.
Vol II Sec.6.6 e-2	e. All changes to the system hardware that may produce a change in software operation shall also be subject to reexamination.

TDP Requirements List

Requirement ID	Description
Vol II Sec.6.7	System Level Integration Testing, Functional Configuration Audit 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.
Vol II Sec.6.7 a-1	System Level Integration Testing, Functional Configuration Audit t [Functional Configuration Audit] includes a test of system operations in the sequence I 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.
Vol II Sec.6.7 a-2	System Level Integration Testing, Functional Configuration Audit a. 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
Vol II Sec.6.7 b-2	b. If vendor developmental test data is incomplete, the ITA shall design and conduct all appropriate module and integrated functional tests.
Vol II Sec.6.7 b-3	b. 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.
Vol II App A.4.3.4-1	Test Case Design, Software Functional Test Case Design The test agency shall review the vendor's test plans and data to verify that the individual performance requirements described in Volume II, Section 2, Subsection 2.5.3.5 are reflected in the software. Note: No Sec. 2.5.3.5 exists
Vol II App A.4.3.4-2	Test Case Design, Software Functional Test Case Design As a part of this process, the test agency shall review the vendor's functional test case designs. The test agency shall prepare a detailed matrix of system functions and the test cases that exercise them.
Vol II App A.4.3.4-6	Test Case Design, Software Functional Test Case Design The vendor's test case design may be evaluated by any standard or special method appropriate; however, emphasis shall be placed on those functions where the vendor data on module development reflects significant debugging problems, and on functional tests that resulted in disproportionately high error rates.
Vol II App A.4.3.4-7	Test Case Design, Software Functional Test Case Design The test agency shall define ACCEPT/REJECT criteria for qualification using the Software Specifications and, if the software runs on special hardware, the associated Hardware Specifications to determine acceptable ranges of performance.

A.3 Source Code Standards

The source code standards identified in this section may be tailored for each voting system to conform to the unique characteristics of the programming language used and to include vendor specific coding standards.

DRAFT

Source Code Requirements List

Requirement ID	Description
6209.2.F.10.a	Polling Place Voting System Requirements: (a) All cryptographic software in the voting system shall have been approved by the U.S. Government's Crypto Module Validation Program (CMVP) as applicable.
6209.6.D.3.c2	Examination Criteria: (continued from above) The State Board or its designee shall review the vendor's source code and documentation to verify that the software conforms to the documentation, and that the documentation is sufficient to enable the user to install, validate, operate and maintain the voting system. The review shall also include an inspection of all records of the baseline version against the vendor's release control system to establish that the configuration, being qualified, conforms to the engineering and test data.
Vol I Sec.4.1.4.3 biv	iv. Use a different process to store ballot images, for which the method of recording may include any appropriate encoding or data compression procedure consistent with the regeneration of an unequivocal record of the ballot as cast by the voter.
Vol I Sec.5.1.1 (1)	Software Standards, Software Sources Unmodified software is not subject to code examination; however, source code generated by a package and embedded in software modules for compilation or interpretation shall be provided in human readable form to the ITA.
Vol I Sec.5.1.1 (2)	Software Standards, Software Sources Correct test design and sufficient test execution must account for the intended and proper configuration of all system components. Therefore, vendors shall submit a record of all user selections made during software installation as part of the Technical Data Package.
Vol I Sec.5.1.1 (3)	Software Standards, Software Sources The vendor shall also submit a record of all configuration changes made to the software following its installation.
Vol I Sec.5.1.1 (4)	Software Standards, Software Sources The ITA shall confirm the propriety and correctness of these user selections and configuration changes.
Vol I Sec.5.2.1 (1)	Software Design and Coding Standards, Selection of Programming Languages Software associated with the logical and numerical operations on vote data shall use a high level programming language, such as: Pascal, Visual Basic, Java, C and C++.
Vol I Sec.5.2.1 (2)	Software Design and Coding Standards, Selection of Programming Languages The requirement for the use of high level language for logical operations does not preclude the use of assembly language for hardware-related segments, such as device controllers and handler programs.
Vol I Sec.5.2.1 (3)	Software Design and Coding Standards, Selection of Programming Languages Also, operating system software may be designed in assembly language.
Vol I Sec.5.2.2 (1)	Software Design and Coding Standards, Software Integrity Self-modifying, dynamically loaded, or interpreted code is prohibited, except under the security provisions outlined in Section 7.4.
Vol I Sec.5.2.2 (2)	Software Design and Coding Standards, Software Integrity External modification of code during execution shall be prohibited.
Vol I Sec.5.2.2 (3)	Software Design and Coding Standards, Software Integrity Where the development environment (programming language and development tools) includes the following features, the software shall provide controls to prevent accidental or deliberate attempts to replace executable code: <ul style="list-style-type: none">- Unbounded arrays or strings (includes buffers used to move data)- Pointer variables; and- Dynamic memory allocation and management.
Vol I Sec.5.2.3	Software Design and Coding Standards, Software Modularity and Programming Voting system application software, including COTS software, shall be designed in a modular fashion. However, COTS software is not required to be inspected for compliance with this requirement.
Vol I Sec.5.2.3 a	Software Design and Coding Standards, Software Modularity and Programming A module is designed in accordance with the following rules: a. Each module shall have a specific function that can be tested and verified independently of the remainder of the code. In practice, some additional modules (such as library modules) may be needed to compile the module under test, but the modular construction allows the supporting modules to be replaced by special test versions that support test objectives;
Vol I Sec.5.2.3 b (1)	b. Each module shall be uniquely and mnemonically named, using names that differ by more than a single character.
Vol I Sec.5.2.3 b (2)	b. In addition to the unique name, the modules shall include a set of header comments identifying the module's purpose, design, conditions, and version history, followed by the operational code.

Source Code Requirements List

Requirement ID	Description
Vol I Sec.5.2.3 b (3)	b. Headers are optional for modules of fewer than ten executable lines where the subject module is embedded in a larger model that has a header containing the header information.
Vol I Sec.5.2.3 b (4)	Software Design and Coding Standards, Software Modularity and Programmin b. Library modules shall also have a header comment describing the purpose of the library and version information;
Vol I Sec.5.2.3 c (1)	c. All required resources, such as data accessed by the module, should either be contained within the module or explicitly identified as input or output to the module.
Vol I Sec.5.2.3 c (2)	c. Within the constraints of the programming language, such resources shall be placed at the lowest level where shared access is needed.
Vol I Sec.5.2.3 c (3)	c. If that shared access level is across multiple modules, the definitions should be defined in a single file (called header files in some languages, such as C) where any changes can be applied once and the change automatically applies to all modules upon compilation or activation;
Vol I Sec.5.2.3 d	d. A module is small enough to be easy to follow and understand. Program logic visible on a single page is easy to follow and correct.
Vol I Sec.5.2.3 e (1)	e. Each module shall have a single entry point, and a single exit point, for normal process flow.
Vol I Sec.5.2.3 e (2)	e. For library modules or languages such as the object-oriented languages, the entry point is to the individual contained module or method invoked.
Vol I Sec.5.2.3 e (3)	e. The single exit point is the point where control is returned. At that point, the data that is expected as output must be appropriately set.
Vol I Sec.5.2.3 e (4)	e. The exception for the exit point is where a problem is so severe that execution cannot be resumed. In this case, the design must explicitly protect all recorded votes and audit log information and must implement formal exception handlers provided by the language; and
Vol I Sec.5.2.3 f	f. Process flow within the modules shall be restricted to combinations of the control structures defined in Volume II, Section 5. These structures support the modular concept, especially the single entry/exit rule above. They apply to any language feature where program control passes from one activity to the next, such as control scripts, object methods, or sets of executable statements, even though the language itself is not procedural.
Vol I Sec.5.2.4 a	Software Design and Coding Standards, Control Constructs Voting system software shall use the control constructs as identified in Volume II, Section 5: a. Acceptable constructs are Sequence, If-Then-Else, Do-While, Do-Until, Case, and the General loop (including the special case for loop);
Vol I Sec.5.2.4 ai (1)	i. If the programming language used does not provide these control constructs, the vendor shall provide them (that is, comparable structure logic).
Vol I Sec.5.2.4 ai (2)	i. The constructs shall be used consistently throughout the code.
Vol I Sec.5.2.4 ai (3)	b. No other constructs shall be used to control program logic and execution;
Vol I Sec.5.2.4 aii	ii. While some programming languages do not create programs as linear processes, stepping from an initial condition, through changes, to a conclusion, the program components nonetheless contain procedures (such as "methods" in object-oriented languages). Even in these programming languages, the procedures must execute through these control constructs (or their equivalents, as defined and provided by the vendor); and
Vol I Sec.5.2.4 aiii (1)	iii. Operator intervention or logic that evaluates received or stored data shall not re-direct program control within a program routine.
Vol I Sec.5.2.4 aiii (2)	iii Program control may be re-directed within a routine by calling subroutines, procedures, and functions, and by interrupt service routines and exception handlers (due to abnormal error conditions).
Vol I Sec.5.2.4 aiii (3)	d. Do-While (False) constructs and intentional exceptions (used as GoTos) are prohibited.
Vol I Sec.5.2.5 a (1)	Software Design and Coding Standards, Naming Conventions Voting system software shall use the following naming conventions: a. Object, function, procedure, and variable names shall be chosen so as to enhance the readability and intelligibility of the program.
Vol I Sec.5.2.5 a (2)	a. Insofar as possible, names shall be selected so that their parts of speech represent their use, such as nouns to represent objects, verbs to represent functions, etc.
Vol I Sec.5.2.5 b	b. Names used in code and in documentation shall be consistent.

Source Code Requirements List

Requirement ID	Description
Vol I Sec.5.2.5 c (1)	c. Names shall be unique within an application.
Vol I Sec.5.2.5 c (2)	c. Names shall differ by more than a single character.
Vol I Sec.5.2.5 c (3)	c. All single-character names are forbidden except for those variables used as loop indexes.
Vol I Sec.5.2.5 c (4)	c. In large systems where subsystems tend to be developed independently, duplicate names may be used where the scope of the name is unique within the application.
Vol I Sec.5.2.5 c (5)	Software Design and Coding Standards, Naming Conventions c. Names should always be unique where modules are shared
Vol I Sec.5.2.5 d	d. Language keywords shall not be used as names of objects, functions, procedures, variables, or in any manner not consistent with the design of the language.
Vol I Sec.5.2.6 a	Software Design and Coding Standards, Coding Conventions Voting system software shall adhere to basic coding conventions. The coding conventions used shall meet one of the following conditions: a. The vendors shall identify the published, reviewed, and industry-accepted coding conventions used and the ITAs shall test for compliance
Vol I Sec.5.2.6 b	b. The ITAs shall evaluate the code using the coding convention requirements specified in Volume II, Section 5.
Vol I Sec.5.2.7 a (1)	Software Design and Coding Standards, Comments Convention Voting system software shall use the following comment conventions: a. All modules shall contain headers.
Vol I Sec.5.2.7 a (2)	a. For small modules of 10 lines or less, the header may be limited to identification of unit and revision information.
Vol I Sec.5.2.7 a (3)	a. Other header information should be included in the small unit headers if not clear from the actual lines of code.
Vol I Sec.5.2.7 ai	a. Header comments shall provide the following information: i) The purpose of the unit and how it works;
Vol I Sec.5.2.7 aii	a. Header comments shall provide the following information: ii) Other units called and the calling sequence;
Vol I Sec.5.2.7 aiii	a. Header comments shall provide the following information: 3) A description of input parameters and outputs;
Vol I Sec.5.2.7 aiv	a. Header comments shall provide the following information: 4) File references by name and method of access (read, write, modify, append, etc.);
Vol I Sec.5.2.7 av	a. Header comments shall provide the following information: 5) Global variables used; and
Vol I Sec.5.2.7 avi	a. Header comments shall provide the following information: 6) Date of creation and a revision record;
Vol I Sec.5.2.7 b (1)	b. Descriptive comments shall be provided to identify objects and data types.
Vol I Sec.5.2.7 b (2)	b. All variables shall have comments at the point of declaration clearly explaining their use.
Vol I Sec.5.2.7 b (3)	b. Where multiple variables that share the same meaning are required, the variables may share the same comment;
Vol I Sec.5.2.7 c	c. In-line comments should be provided to facilitate interpretation of functional operations, tests and branching;
Vol I Sec.5.2.7 d	d. Assembly code shall contain descriptive and informative comments such that its executable lines can be clearly understood;
Vol I Sec.5.2.7 e	e. All comments shall be formatted in a uniform manner that makes it easy to distinguish them from the executable code.
Vol I Sec.7.9.3 a	a. All cryptographic software in the voting system shall be approved by the U.S. Government's Cryptographic Module Validation Program, as applicable.
Vol I Sec.9.4.1.3	Test Categories, Focus of Software Evaluation The ITA may inspect COTS generated software source code in the preparation of test plans and to provide some minimal scanning or sampling to check for embedded code or unauthorized changes. Otherwise, the COTS source code is not subject to the full code review and testing. For purpose of code analysis, the COTS units shall be treated as unexpanded macros.

Source Code Requirements List

Requirement ID	Description
Vol I Sec.9.5.1.2 -1	Test Applicability, Software Specialized software for ballot preparation, election programming, vote recording, vote tabulation, vote consolidation and reporting, and audit trail production shall be subjected to code inspection.
Vol II Sec.5.2 1	Software Testing, Basis of Software Testing Unmodified, general purpose COTS non-voting software (e.g., operating systems, programming language compilers, data base management systems, and Web browsers) is not subject to the detailed examinations specified in this section. Note: included in Functional Test checklist
Vol II Sec.5.2 2	Software Testing, Basis of Software Testing However, the ITA shall examine such software to confirm that the software has not been modified. Portions of COTS software that have been modified by the vendor in any manner are subject to review. Note: included in Functional Test checklist
Vol II Sec.5.2 3	Software Testing, Basis of Software Testing Unmodified COTS software is not subject to code examination. However, source code generated by a COTS package and embedded in software modules for compilation or interpretation shall be provided in human readable form to the ITA. Note: included in Functional Test checklist
Vol II Sec.5.2 4	Software Testing, Basis of Software Testing The ITA may inspect COTS source code units to determine testing requirements or to verify the code is unmodified. Note: included in Functional Test checklist
Vol II Sec.5.2 5	Software Testing, Basis of Software Testing The ITA may inspect COTS generated software source code in preparation of test plans and to provide some minimal scanning or sampling to check for embedded code or unauthorized changes. Otherwise, COTS source code is not subject to the full code review and testing. Note: included in Functional Test checklist
Vol II Sec.5.2 6	Software Testing, Basis of Software Testing For the purpose of code analysis, the COTS units shall be treated as unexpanded macros. Note: included in Functional Test checklist
Vol II Sec.5.2-1	Software Testing, Basis of Software Testing Unmodified, general purpose COTS non-voting software (e.g. operating systems, programming language compilers, data base management systems, and Web browsers) is not subject to the detailed examinations specified in this section. However, the ITA shall examine such software to confirm the specific version of software being used against the design specification to confirm that the software has not been modified. Portions of COTS software that have been modified by the vendor in any manner are subject to review.
Vol II Sec.5.2-2	Software Testing, Basis of Software Testing Unmodified COTS software is not subject to code examination. However, source code generated by a COTS package and embedded in software modules for compilation or interpretation shall be provided in human readable form to the ITA.
Vol II Sec.5.2-3	Software Testing, Basis of Software Testing The ITA may inspect COTS source code to determine testing requirements or to verify the code is unmodified.
Vol II Sec.5.2-4	Software Testing, Basis of Software Testing The ITA may inspect the COTS generated software source code in preparation of test plans and to provide some minimal scanning or sampling to check for embedded code or unauthorized changes. Otherwise, the COTS source code is not subject to the full code review and testing. For purposes of code analysis, the COTS units shall be treated as unexpanded macros.
Vol II Sec.5.3 a	Software Testing, Initial Review of Documentation Prior to initiating the software review, the ITA shall verify that the documentation submitted by the vendor in the TDP is sufficient to enable: a. Review of the source code. File Note: 5.3.b found in Software Test Review section below.
Vol II Sec.5.4.1 a-1	Source Code Review, Control Constructs Voting system software shall use the control constructs identified in this section as follows: a. If the programming language used does not provide these control constructs, the vendor shall provide them (that is, comparable control structure logic).
Vol II Sec.5.4.1 a-2	a. The constructs shall be used consistently throughout the code. No other constructs shall be used to control program logic and execution;

Source Code Requirements List

Requirement ID	Description
Vol II Sec.5.4.1 b	b. While some programming languages do not create programs as linear processes, stepping from an initial condition, through changes, to a conclusion, the program components nonetheless contain procedures (such as "methods" in object-oriented languages). Even in these programming languages, the procedures must execute through these control constructs (or their equivalents, as defined and provided by the vendor); and
Vol II Sec.5.4.1 c-1	c. Operator intervention or logic that evaluates received or stored data shall not re-direct program control within a program routine.
Vol II Sec.5.4.1 c-2	c. Program control may be re-directed within a routine by calling subroutines, procedures, and functions, and by interrupt service routines and exception handlers (due to abnormal error conditions).
Vol II Sec.5.4.1 c-3	c. Do-While (False) constructs and intentional exceptions (used as GoTos) are prohibited.
Vol II Sec.5.4.2	Source Code Review, Assessment of Coding Conventions The ITA shall test for compliance with the coding conventions specified by the vendor.
Vol II Sec.5.4.2 a-1	Source Code Review, Assessment of Coding Conventions If the vendor does not identify an appropriate set of coding conventions in accordance with the provisions of Volume I, Section 4.2.6.a [Coding Conventions], the ITA shall review the code to ensure that it: a. Uses uniform calling sequences.
Vol II Sec.5.4.2 a-2	a. All parameters shall either be validated for type and range on entry into each unit or the unit comments shall explicitly identify the type and range for the references of the programmer and tester.
Vol II Sec.5.4.2 a-3	Source Code Review, Assessment of Coding Conventions a. Validation may be performed implicitly by the compiler or explicitly by the programmer;
Vol II Sec.5.4.2 b-1	Source Code Review, Assessment of Coding Conventions b. For C based language and others to which this applies, has the return explicitly defined for callable units such as functions or procedures (do not drop through by default) and, in the case of functions, have the return value explicitly assigned.
Vol II Sec.5.4.2 b-2	b. Where the return is only expected to return a successful value, the C convention of returning zero shall be used or the use of another code justified in the comments.
Vol II Sec.5.4.2 b-3	b. If an uncorrected error occurs so the unit must return without correctly completing its objective, a non-zero return value shall be given even if there is no expectation of testing the return.
Vol II Sec.5.4.2 b-4	b. An exception may be made where the return value of the function has a data range including zero;
Vol II Sec.5.4.2 c	c. Does not use macros that contain returns or pass beyond the next statement;
Vol II Sec.5.4.2 d	d. For those languages with unbound arrays, provides controls to prevent writing beyond the array, string, or buffer boundaries;
Vol II Sec.5.4.2 e	e. For those languages with pointers or which provide for specifying absolute memory locations, provides controls that prevent the pointer or address from being used to overwrite executable instructions or to access inappropriate areas where vote counts or audit records are stored;
Vol II Sec.5.4.2 f	f. For those languages supporting case statements, has a default choice explicitly defined to catch values not included in the case list;
Vol II Sec.5.4.2 g	g. Provides controls to prevent any vote counter from overflowing. Assuming the counter size is large enough such that the value will never be reached is not adequate;
Vol II Sec.5.4.2 h	h. Is indented consistently and clearly to indicate logical levels;
Vol II Sec.5.4.2 i -1	i. Excluding code generated by commercial code generators, is written in small and easily identifiable modules, with no more than 50% of all modules exceeding 60 lines in length, no more than 5% of all modules exceeding 120 lines in length, and no modules exceeding 240 lines in length.
Vol II Sec.5.4.2 i -2	i. The reviewer should consider the use of formatting, such as blocking into readable units, which supports the intent of this requirement where the module itself exceeds the limits.
Vol II Sec.5.4.2 i -3	i. The vendor shall justify any module lengths exceeding this standard;
Vol II Sec.5.4.2 j	j. Where code generators are used, the source file segments provided by the code generators should be marked as such with comments defining the logic invoked and, if possible, a copy of the source code provided by the ITA with the generated source code replaced with an unexpanded macro call or its equivalent;
Vol II Sec.5.4.2 k	k. Has no line of code exceeding 80 columns in width (including comments and tab expansions) without justification;

Source Code Requirements List

Requirement ID	Description
Vol II Sec.5.4.2 l	l. Contains no more than one executable statement and no more than one flow control statement for each line of source code;
Vol II Sec.5.4.2 m-1	m. In languages where embedded executable statements are permitted in conditional expressions, the single embedded statement may be considered a part of the conditional expression.
Vol II Sec.5.4.2 m-2	m. Any additional executable statements should be split out to other lines;
Vol II Sec.5.4.2 n	n. Avoids mixed-mode operations. If mixed mode usage is necessary, then all uses shall be identified and clearly explained by comments;
Vol II Sec.5.4.2 o	o. Upon exit () at any point, presents a message to the user indicating the reason for the exit();
Vol II Sec.5.4.2 p-1	p. Uses separate and consistent formats to distinguish between normal status and error or exception messages.
Vol II Sec.5.4.2 p-2	p. All messages shall be self-explanatory and shall not require the operator to perform any look-up to interpret them, except for error messages that require resolution by a trained technician;
Vol II Sec.5.4.2 q	q. References variables by fewer than five levels of indirection (i.e.; a.b.c.d or a[b].c->d);
Vol II Sec.5.4.2 r	r. Has functions with fewer than six levels of indented scope, counted as follows [reference FEC Standard for example].
Vol II Sec.5.4.2 s	s. Initializes every variable upon declaration where permitted;
Vol II Sec.5.4.2 t	t. Specifies explicit comparisons in all if() and while () conditions. For instance:i. if(flag) is prohibited and shall be written in the formatii. If(flag==TRUE) for both single and multiple conditions.
Vol II Sec.5.4.2 u-1	u. Has all constants other than 0 and 1 defined or enumerated, or shall have a comment which clearly explains what each constant means in the context of its use.
Vol II Sec.5.4.2 u-2	u. Where "0" and "1" have multiple meanings in the code unit, even they should be identified.Example: "0" may be used as FALSE, initializing a counter to zero, or as a special flag in a non-binary category.
Vol II Sec.5.4.2 v	v. Only contains the minimum implementation of the "a=b ? c : d" syntax.Expansions such as "j=a?(b?c:d):e" are prohibited.
Vol II Sec.5.4.2 w-1	w. Has all assert() statements coded such that they are absent from a production compilation.
Vol II Sec.5.4.2 w-2	w. Such coding may be implemented by ifdef()s that remove them from or include them in the compilation.
Vol II Sec.5.4.2 w-3	w. If implemented, the initial program identification in setup should identify that assert() is enable and active as a test version.
Vol II Sec.5.4-1	Software Testing, Source Code Review The ITA shall compare the source code to the vendor's software design documentation to ascertain how completely the software conforms to the vendor's specifications.
Vol II Sec.5.4-2	Software Testing, Source Code Review Source code inspection shall also assess the extent to which the code adheres to the requirements in Volume I, Section 4 [Software Standards].
Vol II Sec.6.2.1 a	Basis of Integration Testing, Testing Breadth 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;
Vol II Sec.6.2.1 b	b. Where more detailed source code review is needed; and
Vol II Sec.6.2.1 c	c. Both of the above.
Vol II Sec.6.6 b-1	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.
Vol II Sec.6.6 b-2	b. 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;
Vol II Sec.6.6 e-1	e. All subsequent changes to the baseline software configuration made during the course of qualification testing shall be subject to reexamination.

Source Code Requirements List

Requirement ID	Description
Vol II Sec.6.6 e-2	e. All changes to the system hardware that may produce a change in software operation shall also be subject to reexamination.

DRAFT

DRAFT

Appendix B: Test Scenarios

B.1 Ballot Preparation

1. *Jurisdiction Specification*

(setup of installation options)

2. *(Geographical Breakdown)* (specify precincts, split precincts, districts, polling places)

(voting machine definition and allocation)

(political party definition)

(Office / contest definition)

3. *Election Specific Definition*

(open/closed primary support)

(cross party voting)

(general election)

(straight party voting)

(contest types supported)

Vote for one

Vote n of m (10 running – 3 elected – must vote for 3 different people)

Cumulative vote (Can vote 3 times for same person)

Ranked vote

Judicial (Vote a judge out – then vote on a new one)

Recall

Proposition (Bond Issue)

(maximum number of elections supported (number of pages))

4. *Candidate Definition*

(max candidates / contest)

(candidate order) (rotation)

5. *Create Ballot Styles*

(multiple styles/election)

(association w/precincts/polling places)

(preview ballot styles)

6. *Election backup and restore*

(use previous election information in following election)

7. *Multiple languages*

Test languages that are required,

8. *HAVA – Audio/ disabilities*

(verify ballot preparation for blind / disabled voters)

9. *Test ballot generation*

(prepare special marked ballots for testing voting system)

10. *Voting (DRE)*

(invalid _ undervote, overvote, mis-marked)

(separation of test ballots)

(write in handling)

(provisional Ballots)

(persons w/disabilities)

Multiple languages

(fleeing voter // timeout handling)

(duplicate voting by single voter)

(voter authentication –login)

((sudden power failure / interruption)

(correcting / reviewing)

Validating contest types / options

Non-partisan contests/ issues

(primary election)

 CLOSED primaryh

 Open primaryh

 Cross-party voting

(general election)

 Straight party

Fonts / contrast / colors

Early voting

11. *Machine startup and test*

Poll worker authentication and login

Zero total reports

Self diagnostics

Ballot loading / correct ballot styles for machine

12. *Poll closing*

(poll closing summary reports)

(Polling place – consolated total for polling place)

(voting during open poll times only)

(export from redundant memories , recover from damaged media)

13. Voter receipt

(accurate record of voting)
(random order maintained)
(viewed but not collected by voter)

B.2 Voting (Paper ballot)

(no duplicate tabulation)
(invalid _ undervote, overvote, mis-marked)
(error – paper jam – misread)
(scanning accuracy)
(paper weight/specs.)
(sensitivity setting)
(separation of test ballots)
(write in handling)
(multiple languages)
(fonts/color/)
(sudden power failure / interruption)
(tabulation absentee ballots)

B.3 Central Tally

(all reporting provided)
(resolution of write-ins , provisional votes, irregular voting)
(tabulation by category : absentee, normal, provisional)
(no provision of totals while polls are open)
(protection against duplicate counting)
(unable to alter transport media prior to input)
(recount capability)

Appendix C: TDP Initial Matrix Checklist

INITIAL TDP REVIEW (TO DETERMINE MSA INFORMATION) This table is from the Ciber process doc ad is for 2002 – we need to update it to 2005.

ITEM	1990 FEC Standard	2002 FEC Standard
Pre-voting, voting, post-voting	<p>Each should be separately addressed</p> <p>Per FEC:</p> <p><u>Pre-Voting functions:</u> ballot layout, installation of general-purpose ballot counting, software or firmware, preparation and installation of election-specific software or firmware, programming, preparation and testing of system hardware, system readiness and verification test.</p> <p><u>Post Voting:</u> Provide a means for closing polling place and obtaining reports.</p>	<p>Vol. I Sect. 2.1: For organizational purposes, the functional capabilities are categorized by the phase of election activity in which they are required:</p> <p><u>Overall capabilities:</u> functional capabilities throughout the election process including security, accuracy, integrity, system auditability, election management system, vote tabulation, ballot counters, telecommunications, and data retention.</p> <p><u>Pre-voting capabilities:</u> ballot preparation, preparation of election-specific software including firmware, production of ballots or ballot pages, installation of ballots and ballot counting software including firmware, and system and equipment tests.</p> <p><u>Post-voting capabilities:</u> closing the polling place; obtaining reports by voting machine, polling place, and precinct; obtaining consolidated reports; obtaining reports of audit trails.</p>
Ballot Interpretation Logic	<p>Sect. 4.7: Vendor shall identify any items which cannot be accommodated by the system: closed and open primary elections; partisan and nonpartisan offices; straight party voting options; slate or group voting options; cross-party endorsement; primary presidential delegation nominations; rotation of names within an office; recall issues with options; reassembly of multi-card ballots; split precincts; vote for N of M; write-in; over and under votes; totally blank ballots.</p>	<p>Vol I, Sec. 2.2.8.2: The TDP accompanying the system shall specifically identify which of the following items <i>can</i> and <i>cannot</i> be supported by the system, as well as <i>how</i> the system can implement the items supported:</p> <ol style="list-style-type: none"> a. Closed primaries; b. Open primaries; c. Partisan offices; d. Non-partisan offices; e. Write-in voting; f. Primary Pres. Delegation nominations; g. Ballot rotation; h. Straight party voting; i. Cross-party endorsements; j. Split precincts; k. Vote for N of M; l. Recall issues w/options;

ITEM	1990 FEC Standard	2002 FEC Standard
		m. Ranked order voting; and n. Provisional or challenged ballots.
Test information	(a) Including test plan/script or documentation to create one (b) internal testing information	
Software spec	Including software development process	Vol II Sec. 2.1.1 below
Design spec	Does not have to be a “formal” document.	Vol II Sec. 2.1.1 below
Sample reports	include	Vol II Sec. 2.1: 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).
Source code	necessary	Vol II Sec. 2.1: 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).
Functional spec	Does not have to be a “formal” document	Vol II Sec. 2.1.1 below
Requirements spec	Does not have to be a “formal” document.	Vol II Sec. 2.1.1 below
Manuals	(a) Software Spec (b) Operations Manual (often a User’s Guide*) (c) Maintenance Manual. *Make sure User’s Guide covers prevoting, voting, and postvoting (can be in one manual).	Vol II Sec. 2.1.1 below
System Architecture/overview	Map of complete system	
		Vol. II Sec. 2.1.1.a: At a minimum, the TDP shall contain the following documentation: <ul style="list-style-type: none"> a. System configuration overview; b. System functionality description; (<i>does not have to be a formal document</i>) c. System hardware specs (<i>COTS only; look for mfg. Specs—non-COTS is reviewed by hardware ITA</i>); d. Software design & specs; e. System and test verification specs; (<i>both developmental and qualification test info</i>) f. System security specs; g. User/system operators procedures (<i>including pre-voting and post-voting</i>);

ITEM	1990 FEC Standard	2002 FEC Standard
		<ul style="list-style-type: none"> h. System maint. Procedures (COTS only; non-COTS reviewed by hardware ITA); i. Personnel deployment and training requirements; j. Conf. mgmt plan; k. QA prog; and l. System change notes (requalifying systems only).
		Vol. II Sec. 2.1.1.2: For systems seeking requalification, vendors shall submit System Change Notes as well as current revisions of all documents that have been updated to reflect system changes.
Accessibility	Optional	Vol. I Sec. 2.2.7.1 Accessibility, Common Standards: To facilitate accessibility, all voting systems must be capable of meeting the following conditions (highlights below): High forward reach; maximum level forward reach; vertical plane; height; operable controls.
Accessibility	Optional	Vo. I, Sec. 2.2.7.2 DRE Standards DRE voting systems shall provide, as part of their configuration, the capability to provide access to voters with a broad range of disabilities. This capability shall (highlights below): Not require a voter to bring own assistive technology to polling place; Provide audio information and stimulus; Provide wireless coupling for assistive devices for hard of hearing; Meet ANSI standards to avoid electromagnetic interference for hearing devices; Permit adjustments on electronic image displays; Touchscreens must provide mechanically operated controls or keys; Alert voter to expiration of time period; Provide visual clues for sound systems for hearing impaired; Provide secondary means of voter identification if primary means not applicable to voter.

Initial review is to determine if these items exist. In-depth review of FEC requirements acceptability will follow.

Appendix D: Required Functions Checklist

Will generate once questions on functionality are discussed with NY BOE

DRAFT

Appendix E: System Integration Test Ballots

The following ballots are provided in .pdf format. Press Ctrl and click on the Icon to see them.



Figure 1: Press Ctrl and click on this icon for General Election



Figure 2: Press Ctrl and click on this icon for Primary Election

DRAFT