New York State Board of Elections
Voting System Verification Testing

Final Master Test Plan

Document Number SL-MTP-08-V-NYSBOE-0337, Rev 1.0
April 10, 2008

Prepared for:

Name	New York State Board of Elections
Address	40 Steuben Place Albany, New York 12207

Prepared by:

SysTest labs®

216 16th Street Mall
Suite 700
Denver, CO 80202

NVLAP®
NVLAP LAB CODE 200733-0

Accredited by the Election Assistance Commission (EAC) for Selected Voting System Test Methods or Services
EAC Lab Code 0701

Revision History

Date	Description of Revision	Author	Revision No.
3/7/08	Draft Initial Test Plan – SysTest Labs internal distribution and review	B.Phillips, R.Reed	Rev 0.1
3/24/08	Updated Draft	J.Henry, D.Angell	Rev 0.2
3/25/08	Updates from Review Meeting Added	J.Henry, D.Angell	Rev 0.21
3/26/08	Draft Prepared for Review	J.Henry	Rev 0.22
3/28/08	Review comments added	J.Henry, D.Angell, S.Brown, P.Bialka, E.Froehlich	Rev 0.23
3/31/08	Additional Review Comments added	J.Henry, D.Angell, S.Brown, P.Bialka, E.Froehlich	Rev 0.24
4/01/08	Added Review Comments from Red Team	J.Henry, D.Angell, S.Brown, P.Bialka, E.Froehlich	Rev 0.25
4/10/08	Delivery of Master Test Plan	J.Henry, D.Angell, S.Brown, P.Bialka, E.Froehlich	Rev 1.0

TABLE OF CONTENTS

List of Tables:

List of Figures:

1 INTRODUCTION

1.1 Project Overview

The New York State Board of Elections (NYSBOE) requires that before any voting system may be eligible to be purchased in New York State (NYS), it must be certified by the NYSBOE that such system(s) meet the requirements of the NYS Election Law, Section 6209 of Subtitle V of Title 9 of the Official Compilation of Codes, Rules and Regulations of the State of New York, and the federal 2005 Voluntary Voting System Guidelines (VVSG), Volumes 1 and 2. SysTest Labs has been engaged by the NYSBOE to provide verification testing services to support the process of voting system certification by the NYSBOE.

1.2 Purpose

The purpose of this Final Master Test Plan (defined as **Deliverable 6: Final Master Test Plan**) is to create clear and precise documentation of the test methods and processes that SysTest Labs, as NYSBOE's Independent Test Authority (ITA), will use throughout the course of voting system verification testing. The Final Master Test Plan was developed to the Institute of Electrical and Electronics Engineers (IEEE) Standard for Software Test Documentation, IEEE Std 829-1998, as these are more comprehensive than the 2005 VVSG standards. Any VVSG standards that are not called for in the IEEE standards are included within this document to ensure this Test Plan is all-inclusive. This

Documenting the test methods and processes will serve as the basis for ensuring that all major milestones and activities required for effective verification testing can efficiently and successfully be accomplished. This Final Master Test Plan will be modified and enhanced as required throughout the verification testing engagement. The purpose of this document:

- Defines the overall test approach.
- Identifies required voting system hardware and software to be tested.
- Identifies hardware, software, and tools to be used to support the testing efforts.
- Defines the types of tests to be performed.
- Defines the types of election and vote data required for effective testing.
- Defines the types of security threats and vulnerabilities against which each voting system will be tested.
- Identifies and establishes traceability from the Requirements Matrix to test cases, and from test cases to the Requirements Matrix.
- Defines the process for recording and reporting test results.
- Defines the process for regression testing and closure of discrepancies.

Comment [rz1]: This document should also serve as a foundation for the development of machine specific test plans and test cases.

1.3 Scope of Testing

SysTest Labs will provide verification testing on each voting system identified by the NYSBOE based on the guidelines established for voting system verification testing as defined by the NYSBOE. This effort includes all levels of software, firmware, system and hardware environmental/Electromagnetic Compatibility (EMC) testing required to demonstrate that each voting system meets the requirements of the 2005 VVSG and NYS laws and regulations. For each voting system identified for verification, Voting System Specific Test Plans (defined as **Deliverable 7: Voting System Specific Test Plans**) will be developed by SysTest Labs to provide Vendor specific testing methods and processes. SysTest Labs' high level tasks for voting system verification testing, as defined by SysTest Labs' National Voluntary Lab Accreditation Program (NVLAP) audited and approved Quality System Manual include:

- Physical Configuration Audit (PCA)
  - Trusted Builds. Identify the Trusted Build process to establish the system version and components being tested and ensure that the qualified executable release is built from the tested components.
  - Software and Hardware Configuration Audit. Verification of software and hardware functional and physical configurations.
- Functional Configuration Audit (FCA)
  - Review of prior ITA Testing and Results.
  - Review of other state verification testing or risk analysis results.
  - Review of prior hardware environmental testing results.
  - Where applicable, iterative hardware environmental testing.
  - Module testing and review of the module test case design documents, data, and results as provided by each Vendor.
  - Iterative system testing of voting system components and fully integrated systems to validate functionality, logic processing, accuracy, performance, security, and system level integration. This testing includes regression testing and the run for record testing.
  - Accuracy testing and validation of a voting system's ability to accurately read and tally a large number of ballot positions without error.
  - Security testing and validation that a voting system meets or exceeds all security related requirements as well as assessing the effectiveness of a voting system's security controls.
- Management of Vendor supplied deliverables, SysTest Labs' test artifacts, and software, firmware, hardware and system test configurations.
- Generation of detailed and repeatable test cases that ensures the voting system meets all applicable requirements of the 2005 VVSG, NYS laws and regulations, and associated Vendor specific requirements. This is defined as **Deliverable 8: Perform Testing As Outlined in Test Plans**.

Comment [rz2]: Change "demonstrate that each voting system meets the requirements" to say "testing of each voting system against all the requirements"

Comment [rz3]: Say testing against all security related requirements here and any other place in this document such language is used.

Comment [NPE4]: "Meet" assumes it passes every test which is highly unlikely.

Comment [rz5]: Say is tested against

- Generation of test data required for all test cases.
- Traceability and tracking of test cases to the requirements of the 2005 VVSG and NYS laws and regulations. This is shown in Attachment A – NYS Voting NYSBOE LOT 1 Systems Master Requirements Matrix.
- Software, Firmware, System, and Hardware test execution.
- Reporting of all test results. This is defined as both **Deliverable 9: Voting System Individual Test Reports**, and **Deliverable 10: Final Test Reports**.

SysTest Labs will develop and submit to the NYSBOE a Final Voting System Specific Test Report (defined as **Deliverable 10: Final Test Reports)** for each VSUT (Voting System Under Test) that details all test results and findings as a result of each verification test effort, as well as a recommendation to certify or not to certify based on the test results for each VSUT.

1.4 Pre-Validation Review

The SysTest Labs test process includes conducting a Pre-Validation review of the TDP (Technical Data Package) which is an assessment of the quality of any previous testing performed by the Vendor, EAC (Election Ass-1.224 -6(d)anc

1.5 Final Master Test Plan Attachments

The following attachments are an integral part of this Final Master Test Plan:

Attachment A – *NYS Voting NYSBOE LOT 1 Systems Master Requirements Matrix*
Attachment B – *Master TDP Review Plan, Document Number SL-MTP-08-V-NYSBOE-0347*

1.6 Scope of a Voting System

This section provides a brief definition of the scope of a voting system's components. The items shown in Table 1- *Summary of a Voting System's Components* are a generic representation of a full voting system and are not intended to be all-encompassing. The specific components associated with each Vendor's system will be explicitly defined in the applicable Voting System Specific Test Plan. The list of software, firmware, and hardware components, including model numbers and versions, and configurations included in each Vendor's verification testing effort are defined solely by the Vendors in the TDP delivered to both SysTest Labs and the NYSBOE.

Table 1 - Summary of a Voting System's Components

Component	Item	Description
Software & Database Management System	Election Management System	Software used for: • Creating Election Definitions • Creating ballot styles and layouts • Publishing & printing paper ballots • Publishing electronic ballots for DREs • Export of election definition to removable memory • Transfer of Results to Central Count location • Central Count results reporting
Hardware & Firmware	Ballot Marking Device	Device used in the polling place that uses a touch screen or similar technology to record vote selections and produces a paper ballot that can be scanned by either precinct-count optical scanner or high speed optical scanner.

Comment [rz10]: EMS can contain hardware and firmware as well.

Component	Item	Description
Hardware & Firmware	DRE	Direct Recording Electronic (DRE) touch screen voting machine. Voting is achieved by loading the appropriate election definition, which in turn causes display of the voter's applicable ballot, the voter selecting the vote choices via the touch screen or through ADA devices, and casting the ballot after review of all voting choices. In addition, the DRE may include a Voter Verifiable Paper Audit Trail (VVPAT) device for printing of ballot records, which enable voters to verify their choices before casting their ballots.
Hardware & Firmware	Precinct-count Optical Scanner	A precinct-count optical scanner is a mark sense-based ballot and vote counting device located at a precinct and is typically operated by scanning one ballot at a time.
Hardware & Firmware	High Speed Optical Scanner	High Speed Optical Scanner is a mark sense-based ballot and vote counting device typically located at a central count facility and is operated by an automated multi-sheet feeding capability.
Hardware & Firmware	External Memory Card Loaders/Readers	These devices are used to upload election definitions to external memory, e.g., flash cards, PCMCIA cards, etc. and download election results to central count consolidation.

1.7 Assumptions

The development of a reasonable test plan may require a trade-off between the amount of time spent with the finite set of system conditions and possible assumptions against which to perform the verification and validation (V&V) tasks.

Comment [rz11]: Can SysTest expand on this comment?

- There will not be any witness builds; all builds will be Trusted Builds.

- All details regarding the TDP review tasks and process will be included as part of the Master TDP Review Plan (Attachment B – *Master TDP Review Plan*).
- The PCA will be completed prior to beginning the FCA.
- The Vendor will have the opportunity to address and correct all discrepancies identified during the test process. Discrepancies will be resolved and fixes provided to SysTest Labs with sufficient time for review, assessment, retest, and regression test prior to the beginning of the 'Run-For-Record Test Pass' task date as identified in the Master Program Plan (MPP)[1].
- IEEE standards specify that this document should contain the sections Responsibilities, Staffing and Training Needs, Schedule, and Risks and Contingencies. These are all covered as part of the MPP and are not part of this Master Test Plan.

Comment [rz12]: This will not be true in the final Run for Record as there will be no opportunity for the vendor to address run for Record findings prior to the submission of the final test reports. Additionally SysTest may not allow for discrepancy corrections when the impact invalidates too much prior testing as this could jeopardize the testing timeframe in general

1.8 Applicable Standards and References

1.8.1 Required Voting System Standards

All testing will determine whether or not each voting system meets the requirements from the following Standards and New York law and regulations:

1. 2005 VVSG, Volumes 1 and 2
2. NYS 2007 Election Law (Amended Through October 16, 2006)
3. NYS 6209 Regulations
4. New York State Office of General Services Purchasing Memorandum – Centralized Contracts for the Acquisition of Voting Systems and Ballot Marking Devices, November 6, 2007 (NYS BMD Requirements)

1.8.2 Applicable Test Method Standards

All testing will be conducted based on the following testing standards and guidelines:

1. *Quality System Manual*, Version, 1.0.1, SysTest Labs, February 18, 2008
2. *National Institute of Standards and Technology (NIST) 800-53A*, Guide for Assessing Security Controls in Federal Information Systems, December 2007

Comment [NPE13]: A third category should include anything in VVSG Volume 2 that is not in the other two.

[1] *STATE OF NEW YORK STATE BOARD OF ELECTIONS Integrated Master Program Plan For NYSBOE Voting System Examination And Certification Testing*, SysTest Labs, 28 February, 2008

1.8.3 References

The following references were used in development of SysTest Labs' Quality Assurance Manual.

1. *NIST HANDBOOK 150 2006 EDITION* National Voluntary Laboratory Accreditation Program PROCEDURES AND GENERAL REQUIREMENTS (February 2006)
2. *NIST HANDBOOK 150-22 2005* National Voluntary Laboratory Accreditation Program VOTING SYSTEM TESTING (DRAFT Version 1.0)
3. *NIST HANDBOOK 150-22 2007 Edition (DRAFT)* National Voluntary Laboratory Accreditation Program VOTING SYSTEM TESTING (DRAFT December 2007)
4. *EAC Testing and Certification Program Manual*, United States Election Assistance Commission, December 2006 (Version 1.0 Effective January 1, 2007)
5. *VSTL Accreditation Program Manual*, United States Election Assistance Commission, December 2007, DRAFT. (Version 1.0)
6. Help America Vote Act (HAVA) – Section 301
7. IEEE Standard for Software Test Documentation IEEE Std 829-1998, Approved September 16 1998
8. IEEE Standard for Software Verification and Validation IEEE Std 1012-1998, June 8, 2005
9. IEEE Standard for Software Quality Assurance Plans IEEE Std 730-1998, Approved June 25 1998
10. IEEE Standard for Software Configuration Management Plans IEEE Std 828-1998, June 25, 1998
11. IEEE Recommended Practice for Software Requirements Specifications IEEE Std 830-1998, October 20, 1998
12. IEEE Standard for Software Unit Testing IEEE Std 1008-1987, December 29, 1986
13. ISO 17025 General requirements for the competence of testing and calibration laboratories, Second edition, May, 15, 2005
14. IEEE Standard Glossary of Software Engineering Terminology IEEE Std 610.12-1990 (R2002), September 11, 2002

1.9 Terms, Abbreviations and Definitions

The following terms and definitions, as shown in Table 2 - *Terms, Abbreviations and Definitions*, shown below, are used throughout this document:

Table 2 - Terms, Abbreviations and Definitions

Term	Abbreviation	Definition
American Association for Laboratory Accreditation	A2LA	A nonprofit, non-governmental, public service, membership society whose mission is to provide comprehensive services in laboratory accreditation and laboratory-related training.
Ballot Marking Device	BMD	An accessible computer-based voting system that produces a marked ballot (usually paper) that is the result of voter interaction with visual or audio prompts.
CaliberRM	n/a	A Borland application tool that manages requirements
Compact Flash card	CF	This is a type of flash memory card in a standardized enclosure often used in voting systems to store ballot and/or vote results data.
Commercial Off the Shelf Software	COTS	Computer software that is ready-made and available for sale, lease, or license to the general public
Direct Recording Electronic	DRE	Voting systems that, using Touch Screen or other user interfaces, directly record the voter's selections in each race or contest on the ballot in electronic form.
Election Assistance Commission	EAC	An independent, bipartisan commission created by the Help America Vote Act (HAVA) of 2002 that operates the federal government's voting system certification program.
Election Management System	EMS	Typically a database management system used to enter jurisdiction information (district, precincts, languages, etc.) as well as election specific information (races, candidates, voter groups (parties), etc.). In addition, the EMS is also used to layout the ballots, download the election data to the voting devices, upload the results and produce the final results reports.

Term	Abbreviation	Definition
Electromagnetic Compatibility	EMC	The goal of EMC is to validate the correct functioning of different equipment in the same environment and the avoidance of any interference effects between them.
Functional Configuration Audit	FCA	The testing activities associated with the Functional testing of the system
Independent Test Authority	ITA	This is a test lab that is not connected with the vendor or manufacturer of the voting system.
Institute of Electrical and Electronics Engineers	IEEE	A non-profit organization, IEEE is the world's leading professional association for the advancement of technology.
Master Program Plan	MPP	A SysTest Labs' document defining the program responsibilities, staffing and training needs, schedule, and risks and contingencies.
National Institute of Standards and Technology	NIST	NIST is a non-regulatory federal agency within the U.S. Dept. of Commerce. Its mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.
National Voluntary Laboratory Accreditation Program	NVLAP	A division of NIST that provides third-party accreditation to testing and calibration laboratories.
New York State	NYS	Acronym for the State of New York
New York State Board Of Elections	NYSBOE	The New York State Board of Elections is a bipartisan agency vested with the responsibility for administration and enforcement of all laws relating to elections in New York State.

Term	Abbreviation	Definition
New York State Technology Enterprise Corporation	NYSTEC	NYSTEC is a private, not-for-profit engineering company with offices in the state of New York. It acts as a trusted technology advisor to government agencies and private institutions.
Personal Computer Memory Card International Association	PCMCIA	An international standards body that defines and promotes the PC Card (formerly known as "PCMCIA card") and ExpressCard standards. This is another type of electronic memory card in a standardized enclosure often used in voting systems to store ballot and/or vote results data.
Physical Configuration Audit	PCA	The testing activities associated with the physical aspects of the system (hardware, documentation, builds, source code, etc.)
Request For Information (form)	RFI	A form used by testing laboratories to request, from the NYSBOE, interpretation of a technical issue related to testing of voting systems.
Requirements Matrix	N/A	This is the matrix created by NYSBOE/NYSTEC and maintained by SysTest Labs that traces the requirements to the various test cases, test steps, and test methods.
Technical Data Package	TDP	This is the data package that is supplied by the vendor and includes: Functional Requirements, Specifications, End-user documentation, Procedures, System Overview, Configuration Management Plan, Quality Assurance Program, and manuals for each of the required hardware, software, firmware components of each voting system.
Voluntary Voting Systems Guidelines Volumes 1 & 2	VVSG	A set of specifications and requirements against which voting systems can be tested to determine if the systems provide all of the basic functionality, accessibility and security capabilities required of these systems.

Term	Abbreviation	Definition
Voter Verifiable Paper Audit Trail	VVPAT	An independent verification system for voting machines designed to allow voters to verify that their vote was cast correctly, to detect possible election fraud or malfunction, and to provide a means to audit the stored electronic results.
Voting System Test Lab	VSTL	This is the lab where the voting system is being tested.
Voting System Under Test	VSUT	The designation for a voting system that is currently being tested.

2 TEST ITEMS AND FEATURES

2.1 Features to be Tested

The basis for all verification testing for the NYSBOE is the Requirements Matrix. The Requirements Matrix is shown in Attachment A. The Requirements Matrix is stored and maintained in SysTest Labs' CaliberRM™ requirements management tool and includes the following (defined as **Deliverable 3: Testing Requirements Confirmation Matrix**):

- 2005 VVSG, Volume 1
- 2005 VVSG, Volume 2
- NYS 2007 Election Law
- NYS 6209 Regulations
- NYS BMD Requirements
- Test Cases
- Traceability from Requirements to Test Cases and from Test Cases to Requirements

Each Vendor is required to submit a TDP. The Master TDP Review Plan contains the details of what will be reviewed. Section 1.6 *Scope of a Voting System* provides an overall description of the items that make up a typical voting system. These items form the core of the test items for all NYSBOE Verification Testing and will be explicitly defined in each Vendor's Voting System Specific Test Plan. A small subset of the items to be tested is listed below.

- Vendor Specific Software
  - Executable Software
- Vendor Specific Hardware
  - Card Readers
  - DRE
  - Precinct-count and/or High Speed Optical Scanners
  - Data Transmission Devices
  - Ballot Marking Devices
  - Printers

In addition to the items shown above, SysTest Labs will review the items shown below to assess their applicability to each Vendor's specific voting system test effort (see Master TDP Plan for details).

Comment [rz14]: See comments in TDP Review Plan.

- Prior ITA Testing Methods and Results.
- Prior Hardware Environmental Test Methods and Results.
- Prior Other States Certification, Security, or Risk Analysis Testing Review Results.

- Prior SysTest Labs Test Methods and Results.

Comment [NPE15]: REPEAT FROM ABOVE: Some caution is required here since the only use of prior testing is if the submitted system is identical to the prior system.

Per contractual obligations shown in the NYSBOE (Request for Proposal (RFP) for Independent Testing Authority Services Proposal #1396[2]) specific to **Deliverable 4: Evaluation of Prior Work,** results from these item reviews may be used in the verification testing efforts and therefore, not require duplicate testing. Per instructions from the NYSBOE, if applicable, the results may be leveraged in the verification testing efforts and therefore, not require duplicate testing. SysTest Labswill forward to the NYSBOE for review and approval those items it deems as sufficient to satisfy stated requirements.

-

2.2 Features Not to be Reviewed, Assessed and/or Tested

There are no defined features of a voting system that will not be reviewed, assessed and/or tested.

2.3 Test Item Pass/Fail Criteria

After the TDP review process has been successfully completed, the Vendor's submitted TDP documents and software shall be used, along with the associated requirements in the Requirements Matrix, to customize a standard set of test procedures for each test case specified for the voting system.

Testing will be conducted as an independent verification and validation across the entire voting system. Voting system performance to pass/fail criteria shall be measured against expected results for each test case and related set of test procedures. Each feature will pass or fail depending upon the results of the test action(s). If the actual output from an action is equal to the expected output specified by a test case, then the action passes; if not, it fails. Should any action within a test case fail, the entire feature or sub-feature may fail. The specific criteria for test case success or failure will be documented in each Test Case.

Comment [rz16]: Won't this be extremely difficult when some 2000 requirements are tested against approximately 10 test cases? Systest must ensure that pass fail criteria exists for each requirement and that a failure of one requirement does not invalidate an entire test case. Given the relatively small number of test cases SysTest has this mapping and failure impact could be significant as preconditions on a test case may be necessary to continue.

If a test step, case or procedure fails, it cannot be assumed that the system is defective. A failure can only be interpreted as a difference between expected results, which are derived from project documentation, and actual results. There is always the possibility that expected results can be in error due to misinterpretation(s) of incomplete or inaccurate project documentation.

---

[2] A Request for Proposal (RFP) is being solicited by the New York State Office of General Services On behalf of the New York State Board of Elections for Independent Testing Authority Services for Voting System Examination and Certification Testing, Proposal Number 1396, September 4, 2007

When documenting the pass/fail of a test case, there will be enough evaluation evidence that an independent body can determine what evaluation work was performed for each voting system and can concur with the verdict.

The pass/fail criteria defined in the test cases in Appendix A is intended to provide a high level definition for the Required or Optional functionality verification (test success criteria). Vendor-specific pass/fail criteria and test success criteria will be further defined in the Vendor's Voting System Specific Test Plans.

2.4 Test Suspension Criteria and Resumption Requirements

Comment [rz17]: SBOE should be involved in any decision to stop or start a test case.

There are several situations that can cause suspension of testing. These include the severity and type of discrepancies encountered during testing, moderate/significant delays in the delivery of items required for testing, and the introduction of a moderate/significant amount of new requirements and related functionality after testing has begun. These situations can impact the testing engagement as well as other outside testing engagements that may rely upon the same testing resources. To ensure a timely, efficient, and effective use of resources, this section defines the criteria, as shown in Table 3 - *Test Suspension Criteria and Resumption Requirements* below, for suspending and resuming testing. . The Vendor is expected to provide resolution to any test suspension items in a timeframe that allows SysTest Labs to meet the expected verification test task timelines as identified in the MPP.

Table 3 - Test Suspension Criteria and Resumption Requirements

Suspension Item	Criteria	Criteria for Resumption

Suspension Item	Criteria	Criteria for Resumption
Type/Severity of Discrepancy	• Hardware - Catastrophic failure of tested system or components that prevents ALL testing from continuing. • Software - Critical defects or anomalies that prevent ALL testing from continuing. • Data Corruption or Loss of Data – Critical hardware failure or software defect that causes data to be corrupted or lost. • Inadequate OS and DBMS security configuration and/or documentation	• Repair or replacement of failed hardware components, check-in of new or repaired components and successful rerun of the Operational Status Check. Personnel and environment resources available to resume testing effort. • Fix for Critical defects or anomalies made, updated Source Code received and reviewed, update to Trusted Build performed. Personnel and environment resources available to resume testing effort.
Delay in Delivery of Items Required for Testing	• Hardware and/or software required not available at the time indicated in the MPP.	• Hardware and/or software required received, checked in and reviewed. Operational Status Check and/or Trusted Build performed. Personnel and environment resources available to resume testing effort.

Suspension Item	Criteria	Criteria for Resumption
New Requirements	• New requirements that are not currently accommodated in existing Voting System Specific Test Plan and Test Cases.	• Voting System Specific Test Plan and Test Cases updated with new requirements and approvals obtained from all stakeholders. Personnel and environment resources available to resume testing effort.
New Functionality	• Functionality that would increase capabilities beyond initial design of the system. • Functionality that moderately/significantly changes the current capabilities of the system.	• Voting System Specific Test Plan and Test Cases updated with new functionality and approvals obtained from all stakeholders. Personnel and environment resources available to resume testing effort.

3 TEST TYPES

This section of the Final Master Test Plan provides a high level definition of the overall types of tests that SysTest Labs will use to provide verification testing of each Vendor's Voting System for the NYSBOE.

3.1 Physical Configuration Audit

The Physical Configuration Audit (PCA) activities are covered in Attachment B to the Master TDP Review Plan. Included are two activities that must be completed prior to test execution, the Trusted Build, and the Software and Hardware Configuration Audit.

3.1.1 Trusted Build

The Trusted Build for each Vendor's voting system software and firmware will be conducted prior to SysTest Labs' test execution efforts and will be completed on site at a SysTest Labs facility or at a secure lab at the Vendor's facility approved by the NYSBOE and SysTest Labs. The Trusted Build process is intended to establish the system version and components being tested and ensures that the qualified executable release is built from the tested components. The requirements for Witness Builds will be implemented as a part of SysTest Labs' Trusted Build process and includes the 2005 VVSG requirements identified for Witness Builds. The Trusted Build will be performed by SysTest Labs personnel and includes:

Comment [rz18]: Does this include all test efforts including TDP review and source code review?

Comment [NPE19]: Without assistance by the vendor.

- Building hardware characteristics
- Building environment images
- Building file hashes
- Compiling all software and firmware source code into executable files
- Creating the final software installation files, including any COTS applications or tools that are used to support the voting system, e.g., virus protection.

The tasks for the Trusted Build are detailed in Section 5.1.1 *Trusted Build.*

3.1.2 Software and Hardware Configuration Audit

The software and hardware configuration audit will be conducted prior to SysTest Labs' test execution efforts and will be completed on site at the SysTest Labs facility. This will verify that:

- The test system configuration conforms to vendor specifications.
- That the test system configuration is consistent with the configuration assessed in any previous ITA/VSTL reports.

- The test system configuration is consistent with the system used in hardware environmental tests for the current validation effort
- An operational status check is conducted.

The tasks for Software and Hardware Configuration Audit are detailed in Section 5.1.2 *Software and Hardware Configuration Audit*.

3.2 Functional Configuration Audit

3.2.1 Review of Prior ITA Test Cases and Results

Comment [rz20]: SysTest labs has already stated that there were no test results in the prior ITA's work other than hardware. This document should be updated to reflect that only hardware test results are under consideration.

SysTest Labs will evaluate the quality and coverage of prior verification testing completed by the previous NYSBOE ITA. This activity will review the test cases to determine if any of the prior verification test results can be substituted for current verification testing activities. The goal is to leverage the efforts completed by the previous ITA and approved by NYSBOE for the exact same versions of voting systems or voting system components and therefore, save both time and money while ensuring testing effectiveness. The tasks for this review are detailed below in Section 5.2.1 Review of Prior ITA Test Cases and Results. The results from this analysis are part of **Deliverable 4: Evaluation of Prior Work.**

3.2.2 Review of Other State Verification Testing or Risk Analysis Results

Comment [NPE21]: REPEAT FROM ABOVE: Some caution is required here since the only use of prior testing is if the submitted system is identical to the prior system.

SysTest Labs will complete an FCA review of other state certification reports, voting system test or risk assessment final reports (e.g. California, Ohio and Colorado). The outcome of these reviews may result in additional requirements, test cases and/or test steps being added to either the Master Verification Test Plan or Vendor Specific Verification Test Plan(s). The tasks for this review are detailed in Section 5.2.2 *Review of Other State Verification Testing or Risk Analysis Results* The results from this analysis are part of **Deliverable 4: Evaluation of Prior Work.=-**

3.2.3 Review of Prior Hardware Environmental Testing

Comment [NPE22]: REPEAT FROM ABOVE: Some caution is required here since the only use of prior testing is if the submitted system is identical to the prior system.

SysTest Labs will evaluate the quality and coverage of prior hardware environmental testing completed by NVLAP (National Voluntary Laboratory Accreditation Program) or A2LA (American Association for Laboratory Accreditation) accredited test labs for overall system capabilities, pre-voting, voting, and post-voting functions as well as adherence to hardware environmental and EMC standards. This activity will determine if any of the prior hardware environmental test results can be substituted for current hardware environmental testing activities. The goal is to leverage the efforts completed by approved and/or accredited test labs that have tested the exact same versions of voting system hardware components and therefore, save both time and money while ensuring testing effectiveness. The tasks for the review of prior

hardware environmental testing are detailed below in Section 5.2.3. *Review of Prior Hardware Environmental Testing*.

3.2.4 Hardware Environmental Testing

SysTest Labs, through our approved Hardware Test Subcontractors ("Subcontractors"), will perform hardware environmental and EMC testing, as required, on all custom hardware components. Hardware components that are determined to be Commercial-Off-the-Shelf (COTS) products may not be required to be subjected to hardware environmental and EMC testing if the criteria for the tests performed on the COTS items is equal to or more extensive than those defined in the Requirements Matrix. SysTest Labs will assess if a product is COTS and submit the list to NYSBOE for review and acceptance. The tasks for hardware environmental testing are detailed below in Section 5.2.4 *Hardware Environmental Testing*.

3.2.5 Module Testing

SysTest Labs will review the module test case design documents, data, and results as provided by each Vendor. In evaluating each module, with respect to flow control parameters and data on both entry and exit, SysTest Labs assesses for discrepancies between the Software Specifications and the design of the Test Case. Discrepancies will be provided to the Vendor for response and correction. The tasks for module testing are detailed below in Section 5.2.5 *Module Testing*.

3.2.6 System Testing

The goal of system testing is to assess the response of the voting software and integrated voting system when subjected to a range of conditions.

SysTest Labs has developed a series of standard system test cases intended to demonstrate that all elements of the Requirements Matrix have been met as well as test cases that relate to Failure Injection, Data Driven Conditions, User Interface Testing, Data Referential Integrity, End-to-End operational use, Stress, Volume, Performance, and Accessibility and Usability testing to ensure that SysTest Labs is able to validate expected results, leveraging the benefits that come with these types of tests. The tasks for system testing are detailed in Section 5.2.6 *System Testing*.

Comment [rz23]: If this is true, each requirement in the matrix should map to a test case, It seems that this has not happened yet.

The initial set of system test cases designed for voting system verification testing for the NYSBOE are listed in Appendix A – Test Cases. As the Voting System Specific Test Plans get developed for each Vendor's voting system, SysTest Labs will expand on the standard system test cases as required for each Vendor's voting system. The unique test procedures or test steps required for each

Vendor's voting system will be developed and included as an attachment in each Voting System Specific Test Plan.

3.2.6.1 Regression Testing

As part of its system testing, SysTest Labs will perform Regression Testing. Regression testing consists of selective retesting of a system, major subsystem or component part(s) to verify that modifications made to remedy a specific discrepancy (or discrepancies) have not caused unintended effects and that the system and the component still complies with its specified requirements. The tasks for regression testing are detailed in 5.2.6.1 *Regression Testing*.

3.2.6.2 Run For Record Testing

Comment [NPE24]: The final "Run for Record" is expected to be a complete run of all test cases with no vendor changes before, during, or after.

As part of the system testing, SysTest Labs will perform a final regression test of the fully integrated voting systems. This test is referred to as a "Run For Record Test". This will not encompass the entire set of test cases, but rather a subset of the test cases that best exercise and regression test the voting system. The tasks for Run for Record testing are detailed in Section 5.2.6.2 *Run For Record Testing*.

3.2.6.3 Discrepancy Closure

A discrepancy can be closed if the response from the vendor adequately describes how the vendor has made modifications to the code, hardware and/or documentation to meet the VSS/VVSG requirement and SysTest Labs has confirmed through review and/or testing that the requirement has been met. The tasks for discrepancy closure are detailed below in Section 5.2.6.3 *Discrepancy Closure*.

3.2.7 Accuracy Testing

Accuracy testing is a critical test of any voting system. Accuracy Testing consists of validating a voting system's ability to accurately read and tally a large number of ballot positions without error. The standards state that a voting system must be able to read and accurately tally a minimum of 1,549,703 ballot positions with no errors or 3,126,404 ballot positions with one error. The approach to accuracy testing for the NYSBOE verification test effort will involve execution of tests against certain components of the voting system, specifically the polling place devices, e.g., DREs, ballot marking device and precinct-count optical scanners, and the vote totaling or consolidation systems, including high speed scanners. These tests will use a specially designed ballot intended to make the process of accuracy testing and validation of the results as effective and efficient as possible.

It should be noted that the purpose of this accuracy test is not to duplicate the process of logic and accuracy testing of a ballot designed for a realistic election. That testing will be completed during functional testing.

The tasks for accuracy testing are detailed in Section 5.2.7 *Accuracy Testing*.

3.2.8 Security Testing

Comment [NPE25]: Excellent definition of security testing requirements.

Comment [rz26]: In reading this section it appears that SysTest understands the security testing requirements well.

NYSBOE's specific expectations for security testing includes both the process of validating that a voting system meets or exceeds all security related requirements defined specifically in the Requirements Matrix as well as assessing the effectiveness of a voting system's security controls[3]. NYSBOE also expects that security and functional testing will not be separate activities, but instead, security testing will be incorporated throughout the functional testing. The testing is intended to validate the presence and effectiveness of a voting system's security controls, e.g., prevention of unauthorized access or intrusion, prevention or detection of deletion or modification of data, protection and maintenance of audit trail data, and prevention or detection of modification or elimination of security mechanisms. The testing is also intended to determine how easily a control can be circumvented through negative testing. The planned approach for testing a voting system's level of security will be a focused effort as well as a process that incorporates security testing throughout all system level testing. The focused effort will be tests cases specifically designed to validate that the voting system and its processes meet all applicable security requirements and test cases designed to attempt to circumvent the security controls that are present. Incorporated security testing throughout all system level testing will include having test steps and validation points throughout the system test cases to ensure that security is maintained to the level required in the Requirements Matrix. In addition to the active security testing just identified, the following reviews and assessments will be performed:

- The Vendor's documentation will be reviewed to ensure sufficient detail is present to operate the voting system in a secured implementation.
- The voting system's source code will be reviewed for security related vulnerabilities (refer to the Physical Configuration Audit (PCA) as part of the Master TDP Review Plan, Document Number SL-MTP-08-V-NYSBOE-0347).
- Where the Vendor's statements assert the voting system is secured via processes, physical mechanisms and physical seals. Procedures will test the presence and effectiveness of such controls.

---

[3] *Voting System Testing Expectations Overview For New York State Board of Elections*, New York State Technology Enterprise Corporation, January 16, 2008, Version 1

- Negative testing will be performed to identify vulnerabilities that could be used to circumvent controls or compromise the system.

In security testing, SysTest Labs will identify and provide to the NYSBOE for review and approval, specific threat criteria for which the voting systems will be tested against. SysTest Labs will identify the risk to each specific threat should a flaw or exception be identified during testing of a voting system. Any instance where an anomaly or possible security flaw is identified, the discrepancy is reported and the potential risk is documented and evaluated. The tasks for FCA security testing are detailed in Section 5.2.8 *Security Testing*.

3.3 NYSBOE Interpretations

The test engagement described in this Final Master Test Plan utilizes the standard test methods. Should SysTest Labs require an interpretation, a "Request for Interpretation by the NYSBOE" form (RFI) will be initiated and presented to the NYSBOE for interpretation per the Communication Management Plan, section 2.7.3[4].

An Interpretation issued by the NYSBOE will serve to clarify what a given standard requires and how to properly evaluate compliance. SysTest Labs may request an NYBSOE interpretation because a technical issue requires further interpretation regarding a test method. This request can arise from communications with the vendor, from the Project Manager, or from the ITA test team via any ITA manager.

If an NYSBOE interpretation might be needed, the Manager immediately alerts the SysTest Labs' Program Manager, who analyzes the issue and, if deemed necessary, asks the NYSBOE for an interpretation via email. This process must be expedited to ensure the ITA process can continue.

The request to the NYSBOE must:

- Have the RFI form completed and sent in writing to the NYSBOE Program Director. This can be by email, fax, or postal service.
- Be limited to a single issue.
- Provide a reference to the particular standard(s) (2005 VVSG, NYS 2007 Election Law, NYS 6209 Regulations, NYS BMD Requirements) and the related specific requirement(s).
- Provide clear, concise facts and details. State the facts that are giving rise to the ambiguity and describe why its an ambiguity.

---

[4] *Communications Management Plan For NYSBOE Voting System Examination And Certification Testing,* SysTest Labs, March 26, 2008, Version 3.0

- Provide a proposed interpretation: interpret the voting system standard in the context of the facts presented and provide the basis and reasoning behind the proposal.
- Be included in the Voting System Specific Test Case and the Final Voting System Specific Test Report after the NYSBOE interpretation is received.

4 VERIFICATION TEST ARTIFACTS

An illustration of the documentation and deliverables that will be developed and submitted as a part of the NYSBOE verification testing effort are shown in Figure 1 - *Verification Testing Artifacts*. All grayed out items in Figure 1 are not part of this document and details can be found in the Master TDP Review Plan (a component of **Deliverable 5: Review of Technical Data Packages (TDPs)**. A list of the other test related deliverables is shown in Table 4 - *Verification Testing Deliverables*

Figure 1 - Verification Testing Artifacts

Table 4 - Verification Testing Deliverables

Item	Description
Final Master Test Plan	A clear and precise plan of overall test methods and processes that SysTest Labs will use throughout the course of voting system verification testing (this document). This document is defined as **Deliverable 6: Final Master Test Plan**.
Voting System Specific Test Plans	A clear and precise plan of specific test methods and processes that SysTest Labs will use for voting system verification testing of a unique and specific Vendor's voting system(s). These documents are defined as **Deliverable 7: Voting System Specific Test Plans**.
Test Cases	A document specifying inputs, predicted results, and a set of execution conditions for a test item(s). The test case will contain specific information regarding the input being performed, the requirements being tested against, and the expected output. A test case is comprised of one or more test steps. More than one test step and/or test case might be executed to satisfy a specific requirement. The input required to execute the test case may require special procedural requirements such as: • Special set up • Operator intervention, • Output determination procedures, • Special wrap up Any special procedural requirement will be identified and documented. These tests are defined as **Deliverable 8: Perform Testing As Outlined in Test Plans**.
Test Election Definitions	A list of all terms describing function, design, documentation, and testing attributes of voting system hardware and software specific to this Final Master Test Plan. The definitions listed specific to test steps, test cases, and test procedures will establish meaning in the context of this document. For the purpose of this document, the term "software" includes firmware, documentation, data, and execution control statements (e.g., command files, job control language). Acronyms will be included and defined as appropriate.

Item	Description
Test Procedures	A document specifying the steps for executing a set of test cases used to analyze software and/or hardware. The Test Procedure will identify all documentation referenced, hardware tested on, and any other requirements such as unique facility needs or specially trained personnel as it applies to setting up and running the test case(s). The system and application software required to execute the test case(s) are also identified. For all identified requirements, SysTest Labs will design and develop tests cases, test data, and test procedures and will add these to SysTest Labs' list of ITA Test Cases for the NYSBOE verification test execution. Test execution steps may include: • Defining actions needed to create test environment. • Defining how to log test results and any other events pertinent to the test. • Defining necessary actions to execute the procedure. • Defining how the test measurements will be made. • Defining necessary actions to suspend or stop testing, when unscheduled events dictate. • Defining necessary actions to restart testing.
Test Results	A summarization of relevant details about the results of the execution of testing. Identify the items tested, indicating their version/revision level. The environment where the testing activities took place will be identified. The test cases and test results will define the dependent (and in some cases independent) variables being tested. The results of these tests (or responses) will be recorded. Results may include: • Inputs • Expected results • Actual results • Anomalies • Date and time • Procedure step • Environment

Comment [rz27]: Final results should always include these items along with the test procedures.

Item	Description
	• Testers • Observers Any variances of the test items from their test case or test procedure will be reported along with identifying specific reasons for each variance.
Discrepancy reports	There will be two distinct types of discrepancy reports created during each test campaign. These are "Discrepancy reports" and "Source Code Discrepancy Reports". Discrepancy Reports document Functional-, Documentation-, Informational-, and Hardware-related problems, defects, discrepancies, etc. identified during review and assessment of documentation for a voting system. Source Code Discrepancy Reports document problems, discrepancies, or defects identified during review of the source code. In either case, the discrepancies entered into each report documents the inability of the voting system to satisfy a specific requirement as defined in the Requirements Matrix. Informational- refers to discrepancies that are encountered during review and assessment, but are not related to the Requirements Matrix.
Hardware Environment & EMC Test Plan	A clear and precise plan of test methods and processes that SysTest Labs will use throughout the course of voting system verification for the hardware environment and EMC testing.
Hardware Environment & EMC Test Execution Report	A report containing all results from the hardware environmental and EMC review, assessment and/or testing activities. The report will include a summary of the activities, results, a list of all discrepancies discovered and associated resolutions, and recommendations.
Test Execution Report	A report containing the detailed results and pass/fail summary from the functional testing for the vendor voting system specific testing.

Item	Description
	• A complete analysis of the results from software and systems testing with a listing of all discrepancies and resolutions.
Final Voting System Specific Test Report	A document, in hard copy and electronic format, for the NYSBOE that provides a Pass/Fail summary of for the voting system and details of all results from examinations, assessments, evaluations, and testing.. Each individual Final Voting System Specific Test Report will provide the following information: • The results from review and validation of the TDP documentation a listing of all resolved discrepancies and and associated resolutions along with any unresolved discrepancies. • The results from review and validation of the TDP source code including a listing of all resolved discrepancies and associated resolutions along with any unresolved discrepancies. • A listing of all Test Cases, election definitions, ballot definitions and any other data created and used during test execution. • A complete analysis of the results from software and systems testing including a listing of all resolved discrepancies and associated resolutions along with any unresolved discrepancies. • The results from hardware environmental analysis and testing including a listing of all resolved discrepancies and associated resolutions along with any unresolved discrepancies. • A final assessment and evaluation of the voting system's ability to comply with the Requirements Matrix.

Comment [rz28]: The following are also required to be in the final test report:
-**All test procedures** and test cases that are mapped from the requirements matrix
-All supporting log files, pictures, tester notes etc..
-All information, or links to it necessary for a 3rd party to reach the same result as SysTest upon review of the materials.

5 TEST TASKS

NYSBOE Verification Testing detailed testing tasks required to ensure compliance to the approved Requirements Matrix are provided in this section. High level test cases associated with test execution activities are provided in Appendix A – Test Cases. It should be noted that the results and discrepancy reports for each of the review/assessment and test activities are documented and maintained throughout each activity until the activity has been completed. Upon completion of the verification test engagement, all results are provided in the Final Voting System Specific Test Report and archived with all testing artifacts.

Comment [rz29]: Please describe how NYSBOE will have access to this archive during and after the testing activity.

5.1 Physical Configuration Audit

5.1.1 Trusted Build

All trusted builds are initiated once all the PCA source code review activity, as detailed in the Master TDP Review Plan, has been successfully completed and there are no open or outstanding source code related discrepancies. However, should source code be required to be modified as a result of FCA testing activities, all code modifications will be re-reviewed and any subsequent re-reviews of source code will require a new Trusted Build. The PCA Trusted Build activities relative to NYSBOE verification test effort involves the following tasks and subtasks in conformance with the requirements of 2005 VVSG, Volumes 1 and 2. Trusted Builds also include the 2005 VVSG requirements identified for Witness Builds.

Comment [rz30]: This implies that source code testing is completed prior to functional testing beginning. It should be understood and documented accordingly that source code reviews will be needed throughout functionality testing. This has been agreed to by SysTest and NYSBOE and is indicated throughout the requirements matrix where code review is related to each requirement.

- Interviews:
  - Key Vendor staff are interviewed to evaluate processes and process conformance in the areas of configuration management and quality assurance.
- Preparation for the Trusted Build:
  - Obtaining and reviewing the EAC Testing & Certification Program Manual, Version 1.0, and reviewing Vendor's step-by-step procedures for constructing the build platform.
  - Verifying the target build platform.
  - Acquiring the necessary test equipment and materials to support the Trusted Build process.
- Execution of the Trusted Build:
  - SysTest Labs will accomplish the following throughout the build process, ensuring that the results of these actions are thoroughly documented:
    - Build environment images at various key points:
      - After Operating System, compiler and other tools installation and configuration.

Comment [rz31]: Steps should be added to ensure that compliers used are in fact COTS and not vendor provided compliers. If compliers or build scripts are vendor provided then they must be subject to full source code review. Also, reference the NYSBOE Certified Voting Systems Escrow Requirements document for additional guidance.

        - After installation of Source Code, vendor-supplied files, including COTS applications.
        - After the Build.
    - Build environment and file hashes at various key points:
        - After Operating System, compilers and other tools installation and configuration.
        - After installation of Source Code, vendor-supplied files, including COTS applications.
        - After the Build.
    - Build environment hardware characteristics.
    - Compiling all software and firmware source code into executable files.
    - Create the final software installation files, including any COTS applications or tools that are used to support the voting system, e.g., virus protection.
  - SysTest Labs will perform the Trusted Build by executing the vendor's detailed step-by-step build procedures (As provided in the TDP) and only the configuration items listed in those procedures will be placed on the machine. In addition:
    - The build machine provided by the Vendor will be erased by the ITA to ensure the build will be conducted on an initialized machine.
    - COTS Operating Systems and software used in testing will be verified as authentic for the Trusted Build environment as well as equipment under test. For equipment under test, Operating System installations are performed by SysTest Labs' staff. For the Trusted Build environment, the Operating System is installed by SysTest Labs' staff.
    - SysTest Labs includes a listing of all COTS application files as well as all operating system files in a pre-election configuration, including related hash codes and file signatures.
    - Should components of the system be modified or replaced during the testing process, the SysTest Labs shall conduct a new "Trusted Build" of the system to ensure that the verified executable release of the system is built from tested components.
- A Final Trusted Build will be created for use in the Run for Record testing upon completion of all:
  - TDP document and code reviews and re-reviews.
  - Execution of all Test Cases, and any subsequent regression testing.
  - Resolution of all non-informational discrepancies.
  - Updating of all documentation required to create a Final Trusted Build.
- Conclusion of the Trusted Build:
  - At the conclusion of the Trusted Build process, SysTest Labs completes all final record keeping and archiving procedures at SysTest Labs' facility.

Comment [rz32]: Please reference VVSG Vol1 7.4.4-5 here to ensure all appropriate provisions are followed for the final trusted builds.

Comment [NPE33]: Should this be "Run for Record" not Trusted Build"?

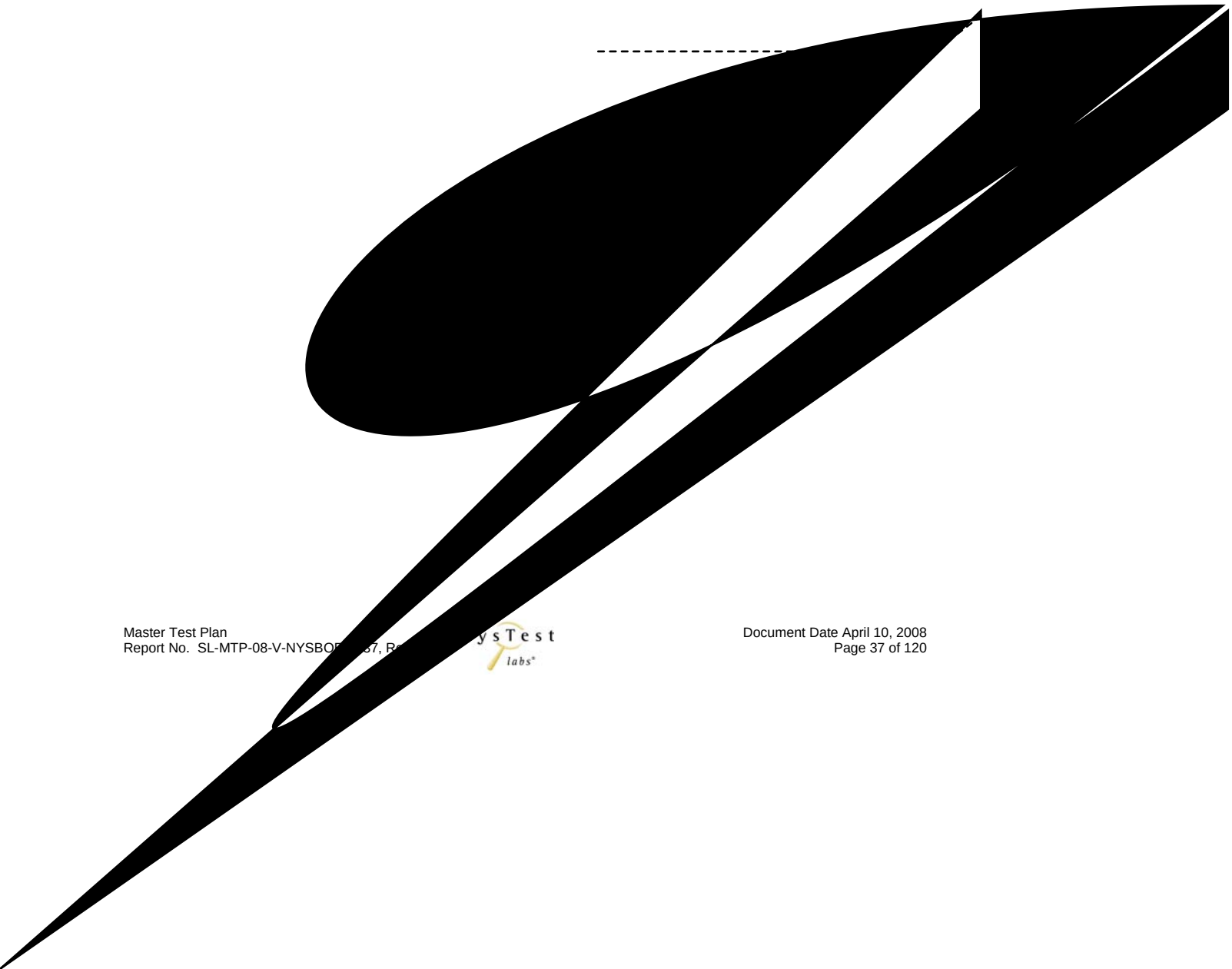
- SysTest Labs will generate the final media that is submitted to the NYSBOE's approved escrow agent.

5.1.2 Software and Hardware Configuration Audit

The Software and Hardware Audit compares the voting system components (hardware and software) to the TDP submitted by the Vendor. The Vendor provides a list of all documentation and data to be audited, cross-referenced to the contents of the TDP. This audit establishes a configuration baseline of the software and hardware to be tested.

This process includes the following:

- Verify that the system config1(app1.2247(nn)6(con)-7(form222)-7(h))6(t)-9ren c scomevVvatp1.2247(nns



This effort will require access to all prior verification test plans, test reports and test results as well as detailed information regarding the configurations and versions of each component within the voting system. Test plans, reports and results from prior verification testing performed by the previous NYSBOE ITA will be analyzed to determine if the results can be accepted for verification. If the testing does meet the criteria as defined above, it will be considered to satisfy the requirements. The tests and results that are accepted are then exempted from the current NYSBOE verification test effort and will be reflected as such in the Requirements Matrix specified for the voting system.

The results from this activity (which is a part of **Deliverable 4: Evaluation of Prior Work**) is a list of system tests that will be sent to the NYSBOE for verification and approval that these are not to be required or included in this current verification testing effort for a specific Vendor's voting system.

5.2.2 Review of Other State Verification Testing or Risk Analysis Results

Comment [NPE35]: REPEAT FROM ABOVE: Some caution is required here since the only use of prior testing is if the submitted system is identical to the prior system.

SysTest Labs will conduct FCA reviews of other state certification reports, voting system test or risk assessment final reports. These reviews will be performed in order to determine if functional, security or operational issues encountered in testing performed for other states may require that additional tests, not currently encompassed within the Requirements Matrix, be performed in order to validate whether these issues are present, or not, in the voting systems submitted for NYSBOE verification.

Tasks required for this review:

- Identify any functional, security or operational issues identified within other state certification reports, voting system test or risk assessment final reports.
- Validate whether these issues create the need for additional testing to be added to NYSBOE-related test efforts. Communications with or interpretations by the NYSBOE and/or the EAC may be necessary to accomplish this.
- Ensure that valid issues identified in this review are addressed by any or all of the following:
  - Additional requirements being added to the Requirements Matrix.
  - Additional test cases being added to the Final Master Test Plan or Voting System Specific Test Plan(s).
  - Additional test steps added to existing test cases.

Comment [rz36]: If the intent here is to ensure that vulnerabilities discovered on systems in other states then the scope of the analysis should be expanded to include the analysis that was done not by an ITA but rather by other organizations. (i.e. Everest Report)

Comment [NPE37]: REPEAT FROM ABOVE: Some caution is required here since the only use of prior testing is if the submitted system is identical to the prior system.

5.2.3 Review of Prior Hardware Environmental Testing

Comment [rz38]: This is the only prior testing that may be useful. Other references to prior testing that is not specific to hardware should be removed.

SysTest Labs will evaluate the quality and coverage of prior hardware environmental testing completed by NVLAP or A2LA accredited test labs for

overall system capabilities, pre-voting, voting, and post-voting functions as well as adherence to hardware environmental and EMC standards. This activity will determine if any of the prior hardware environmental test results can be substituted for current hardware environmental testing activities. The goal is to leverage the efforts completed by approved and/or accredited test labs that have tested the exact same versions of voting system hardware components and therefore, save both time and money while ensuring testing effectiveness.

The acceptance and use of previous hardware environmental testing and verification performed by accredited NVLAP or A2LA facilities is based on the following criteria:

- The configuration of the equipment being presented for testing is substantially identical to the equipment that was previously tested and certified and that all changes made to the hardware configuration of the equipment being presented for testing, from the hardware that was previously tested and certified, are confirmed to be de minimus changes.
- The standards and requirements under which the previous testing and verification was performed are equal to or more demanding than the current requirements.
- There have been no significant changes to the test methods.
- The lab that completed the hardware environmental testing and verification meets the NYSBOE's requirements for accreditation as defined in NIST HANDBOOK 150-22: 2005 and NIST HANDBOOK 150-22: 2007.

Test plans, reports and results from previous hardware testing performed by accredited NVLAP or A2LA laboratories will be analyzed to determine if the results can be accepted for verification. If the testing does meet the criteria as defined above, it will be considered to satisfy the requirements.

The results from this activity is a part of **Deliverable 4: Evaluation of Prior Work** and will be a list of EMC and Environmental tests that will not be required to be included in this current verification testing effort for a specific Vendor's voting system submitted to NYSBOE for approval. If NYSBOE approves, then the equipment is then exempted from specific tests as reflected in the Requirements Matrix for EMC and Environmental testing.

5.2.4 Hardware Environmental Testing

SysTest Labs will review and cross-reference the documentation items from the TDP supplied by the Vendor to determine what testing is required to meet the EAC 2005 VVSG hardware environmental and EMC test requirements. SysTest Labs will examine the vendor tests, and the execution of additional tests, to verify that the system hardware performs all the functions described in the

vendor's documentation submitted for the TDP. This examination includes 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.

The documentation items reviewed will include but not be limited to the following:

- System Hardware specifications
- Hardware schematics
- Bill of Materials (BOM)
- Photographs of hardware and components
- System Overview
- Operator/Maintenance Manual
- Product Safety Declaration

If vendor developmental test data is incomplete, SysTest Labs will design and conduct all appropriate module and integrated functional tests. The functional configuration audit will be performed in SysTest Labs' facility and shall use and verify the accuracy and completeness of the System Operations, Maintenance, and Diagnostic Testing Manuals.

A test of hardware operations shall include the following activities:

- Review the documentation items from the TDP supplied by the Vendor to determine what testing is required to meet the EAC 2005 VVSG hardware environmental and EMC test requirements. The documentation items will include but not be limited to the following:
    - System Hardware specifications
    - Hardware schematics
    - Bill of Materials (BOM)
    - Photographs of hardware and components
    - System Overview
    - Operator/Maintenance Manual
    - Product Safety Declaration
- Perform a configuration item audit to validate that all hardware components identified as a required part of the voting system have been identified and provided.

- Perform an analysis of all proposed COTS items to ascertain if the items are COTS and if their test criteria is equal to or more extensive than those defined in the Requirements Matrix.
- Develop a standalone hardware environmental and EMC Test Plan specifically for each voting system.
- Perform hardware environmental and EMC testing, as defined in Table 5 - *2005 VVSG Hardware Environmental Test Sections and Descriptions.*
- Report all test results and deficiencies identified during testing.
- Provide re-testing of fixes required due to deficiencies identified during testing.
- Develop and submit written documentation of all hardware environmental and EMC test plans and results.

Table 5 - 2005 VVSG Hardware Environmental Test Sections and Descriptions

Test Type	2005 VVSG Section	Test Description
2005 VVSG Volume I	**4.1.2.4**	Electrical Supply Testing
	4.3.8	Safety Evaluation
2005 VVSG Volume II	**4.6.2**	Bench Handling Test
	4.6.3	Vibration Test
	4.6.4	Low Temperature Test
	4.6.5	High Temperature Test
	4.6.6	Humidity Test
	4.7.1	Temperature/Power Variation Tests
	4.7.1.1	Data Accuracy
	4.7.2	Maintainability Test
	4.7.3	Reliability Test
	4.7.4	Availability Test
	4.8	Power Disturbance
	4.8	Electromagnetic Radiation
	4.8	Electrostatic Disruption
	4.8	Electromagnetic Susceptibility
	4.8	Electrical Fast Transient

Test Type	2005 VVSG Section	Test Description
	4.8	Lightning Surge
	4.8	Conducted RF
	4.8	Immunity
	4.8	Magnetic Fields Immunity

5.2.5 Module Testing

SysTest Labs will review the module test case design documents, data, and results as provided by each Vendor. In evaluating each module, with respect to flow control parameters and data on both entry and exit, SysTest Labs will assess for discrepancies between the Software Specifications and the design of the Test Case. Discrepancies will be provided to the Vendor for response and correction.

SysTest Labs will design additional module test cases, as required, to provide coverage of modules containing untested paths with potential for additional errors. SysTest Labs will also review the Vendor's module test data in order to verify that the requirements of the Software Specifications have been demonstrated by the data. In the event that the Vendor's module test data are insufficient, SysTest Labs will provide a description of additional module tests prerequisite to the initiation of functional tests.

The data is also checked during source code review in conformance with other sections of the standards relating to unbound arrays, parameter type and range validation, pointer controls, vote counter overflow, etc.

If it is determined during source code review that potential risks exist at module entry/exit points, then specific functional test cases are designed to test these areas. If during source code review an issue is identified with entry/exit points of the module, then discrepancies are written and submitted to the Vendor for resolution.

5.2.6 System Testing

System Testing involves exercising the specific functions of each component of a voting system as well as the entire voting system. Based on Section 1.6 *Scope of a Voting System*, System Testing will focus on the functionality of an election management system, the polling place devices, and devices required for communications and data loading and will then focus on functionality of the integrated voting system. In addition to non-recurring system testing, regression

testing will occur throughout the system testing cycle as new releases of the software are delivered (following a re-review of the source code and a new Trusted Build). Regression testing will ensure that existing functionality continues to work as expected and that fixes to discrepancies have been adequately addressed.

There are various types of system testing. Table 6 - *Types of System Testing* provides the descriptions of these kinds of tests and their associated benefit.

Table 6 - Types of System Testing

Type of Testing	Description	Benefit
Functional	Functional testing includes the following types of tests:	
• Nominal Conditions	Testing all nominal functional capabilities of all components of the voting system as it relates to the Requirements Matrix.	Nominal conditions testing ensures that the voting system meets all elements specified in the Requirements Matrix.

snction0ing 8ll 4
C0 Tw 9.an ent34(in)5(g)956

Type of Testing	Description	Benefit
• Usability	The purpose of UI Testing is to test all of the screen and data elements that exist on each and every screen. SysTest Labs will verify responses to input, text syntax, error message content, and audit message input.	These tests verify every action will work that a user can perform on a screen. These tests will also verify that any screen or data element will not take the user by surprise.
• Data Referential Integrity	This testing will verify that parent-child and linked table data are accurate. In other words, ensuring the appropriate connectivity between precincts, jurisdictions, candidates, contests, vote results, totals, etc. are maintained.	Referential integrity ensures that the relationships between tables remain synchronized.
• End-to-End	This is testing in a true end-user environment following all pre-election day, election day, and post election day voting rules and processes.	This is used to demonstrate that a system can be used to perform its job following the exact set of processes and steps that would be used by the target customer or end-user.
• Regression	Testing that validates that existing functionality is unchanged with the introduction of new functionality and correction of defects.	Manual test script execution and parallel tests will test end-to-end functionality.

Type of Testing	Description	Benefit
• Run For Record	Final Validation and Regression Test of the System in a true end-user environment, following all pre-election day, election day, and post election day voting rules and processes.	Results are the best the system can perform within the test timeframe available. Verify that fixes have not introduced impacts on other functional aspects of the system and demonstrate that a system can be used to perform its job following the exact set of processes and steps that would be used by the target customer or end-user.
Volume Test	Testing the voting system's response to conditions that range from processing more than the expected number of ballots/voters per precinct to processing more than the expected number of precincts to any other similar volume conditions.	Determine if there are limits to the voting system's ability to operate under conditions that tend to overload the system's capacity to process, store, and report data.
Stress Tests	Testing the voting system's responses to transient overload conditions by subjecting polling place devices to ballot processing at high volume rates.	Evaluates the voting system and software's response to hardware-generated interrupts and wait states.
Accessibility Test	Exercises system capabilities of voters with disability features.	Validates that the voting system meets all applicable ADA and HAVA requirements for voters with disabilities, as specified in the Requirements Matrix.
Performance Tests	Tests accuracy, processing rate, ballot format, handling capability and other performance attributes specified by the Vendor.	Performance testing ensures that the voting system meets all performance elements specified in the Requirements Matrix.

Comment [NPE39]: The "Run for Record" is not a regression test but a full set of tests to ensure that all vendor fixes work as expected.

Type of Testing	Description	Benefit
Recovery	Exercise system's ability to recover from hardware, software, and data errors.	Ensures that the system is able to successfully recover should there be a system or data error.

5.2.6.1 Regression Testing

As part of the system testing, SysTest Labs' approach to regression testing is defined below:

- Always rerun the test case that found the discrepancy. If other actions were executed to re-demonstrate the discrepancy to the Vendor's development organization, they will be performed again during the regression test activities. Ensure the effect of the fix is repeatable.
- The following is completed to determine if additional regression testing is required:
  - Evaluate the discrepancy that was fixed and the extent of the fix within the source code to fully understand the impact, i.e., assess the criticality of the functional area and the severity of the discrepancy. For example, did the discrepancy crash the polling place device or the EMS server, was vote data or audit record data corrupted, was the "Voter" prohibited from completing the vote session, were poll workers prohibited from completing the functions, does the code affect other unrelated aspects of the system functionality, etc.
  - Depending upon how much information is provided by the Vendor's development organization, evaluate the magnitude of the changes to fix the discrepancy and their associated modules and interface touch points.
  - Based on the extent of the fix, testing will be done to ensure there are no unintended consequences impacting other aspects of the system. Prior tests will be rerun as needed to ensure all impacted code branches are revalidated.

Comment [rz40]: Need to discuss with SysTest. There is no detail here to ensure that proper regression testing is happening. If a change is made, all testing may need to stop until an analysis is completed to determine the impact on other tests. Also missing here is the review of all source code changes made by the vendor to address the problem and what the impact is on downstream branches that could invalidate other tests.

5.2.6.2 Run For Record Testing

Comment [NPE41]: This is a final run of all test cases to ensure that all vendor modifications are fixed.

As part of system testing, when SysTest Labs has performed the final Trusted Build, (Reference Section 5.1.1 *Trusted Build*) SysTest Labs will perform a subset of test cases to exercise no less than 80% of the overall requirements across all vendor initiatives. This is a final regression test on the overall system as a last step opportunity to verify the previous regression tests were accurate and complete during the break/fix cycles. It is a final checkpoint to verify non-related aspects of the code were not inadvertently affected by previous fixes.

Comment [rz42]: Not acceptable. Systest is required to test all requirements in the Run for Record.

The code and hardware will be frozen and any discrepancies found will be considered part of the finished product. This is the concluding run of test cases before SysTest Labs creates the Final Test Verification Report.

5.2.6.3 Discrepancy Closure

Comment [rz43]: This seems fine as long as vendors realize that the only test that actually matters to NYSBOE is the final run for record where each requirement will e tested for pass/fail status. Requrements that may have had discrepancies open and closed will be retested.

A discrepancy can be closed if the response from the Vendor adequately describes how the Vendor has made modifications to the code, hardware and/or documentation to meet the requirement in the Requirements Matrix and SysTest Labs has confirmed through re-review and/or re-testing that the requirement has been met.

- A description of the reason why the discrepancy can be closed must be noted in the Description field of the appropriate Discrepancy Report, along with the date it was added and the name of the person making the entry.
- If a Vendor's response indicates that they believe that the identified discrepancy is NOT a discrepancy per the Requirements Matrix, an Interpretation Request must be prepared and submitted to the NYSBOE.

5.2.7 Accuracy Testing

The following steps provide an overview of process for execution of Accuracy Tests:

- The Accuracy Test specific election and ballot definition is created in the voting system's EMS.
- The Accuracy Test specific election and ballot definition is loaded onto the device being tested via a Compact Flash Card or memory card, or via electronic connection depending on the device being tested.
- Execute standard startup and initialization processes for the device being tested.
- Select "candidates" and vote the ballots (if a DRE or BMD device is being tested) or scan pre-marked paper ballots (if a precinct-count optical scanner or BMD is being tested).
- Close polls, run the reports for Totals and Audit Log.
- Transfer vote results data to the EMS for reporting.
- Validate test results.

5.2.8 Security Testing

Comment [NPE44]: This definition of security testing is not as comprehensive as the one in section 3.2.8 and should be updated to be consistent.

Security testing attempts to identify flaws in voting systems where undesired or unauthorized human or machine activity may compromise an election through system failure, data manipulation, data interception or other means.

Comment [rz45]: Source code review must be a component of security testing. It is unclear why it would not be included in this list of activities.

Security testing is related to two main testing activities.

- **Hardware Testing -** Hardware Testing insures equipment will stand up to environment conditions, machines are accurate, physical access to machine components is restricted, machine hardware is reliable and attempts to compromise machine security is detectable. A hardware malfunction could impact the accuracy of voting data or provide unauthorized access to secure information. Specific hardware limitations or restrictions impact the test procedures needed to validate security of the system.
- **System Testing -** System Testing is a combination of hardware and software tests that verify the voting systems have sufficient system and data protection mechanisms, that when combined with other review processes, provide a secure voting environment. This section of the document relates to the Software aspect of System Testing.

Comment [NPE46]: Including source code testing.

There are numerous security test cases. Table 7 - *Types of Security Testing* provides a high level description of the types of security testing required to validate that a voting system will meet the requirements defined in the Requirements Matrix. This list is not intended to be all inclusive. As test cases are detailed for each Vendor's specific voting system, the types of security tests and the conditions associated with each will be further defined to ensure that all requirements in each segment of the Requirements Matrix are validated per voting system.

Table 7 - Types of Security Testing

Type of Testing	Description
Role	Privileges are not allowed to be: • Exceeded. 2005 VVSG Vol 1: 7.2.1.1.c. • Changed to run reports. Voters are inhibited from: • Accessing equipment before polls open. • Running reports. Changes to privileges are prohibited for ID's and passwords thus preventing unauthorized report printing, results

Type of Testing	Description
	transmission, results downloading and resetting of elections. Voter equipment access or keys are limited to ensure: • Only the user interface is accessible. • Only a single vote may be cast. • Closed polls are secure. • Counts are not available to voters. • Unauthorized accounts from system functions. Fraudulent ballots are not accepted by the system ensuring only valid ballots are counted.
Access	Access validation to the system ensures that only applicable system entry is allowed. This includes: • Seals and/or password required to open polls. 2005 VVSG Vol 1: 2.3.1.3. • Security seal and/or password prevent unauthorized opening of polls. • Incorrect or blank password cannot be used to open polls. 2005 VVSG Vol 1: 7.2.1.2. • System provides access controls that limit or detect access to critical system components. 2005 VVSG Vol 1: 2.2.1.1.a.
System Security	Executables can only run in intended manner and order 2005 VVSG Vol 1: 2.1.1. Executable preconditions must be met. Tampering safeguards during repair, interventions or failure. Security provision compatibility with procedures and admin tasks. Incorporate a means of implementing a capability if access to a system function is to be restricted or controlled.
System Log	System log error activity verification. 2005 VVSG Vol 1: 5.4.3. Voting activity verification. 2005 VVSG Vol 1: 5.4.3.d. Log protection. 2005 VVSG Vol 1: 5.4.3.
Audit Records	Audit Record Cannot be Turned Off. 2005 VVSG Vol 1: 2.1.

Type of Testing	Description
Software Security	Software security validation ensures that the accessibility to firmware is appropriately prohibited. This includes verifying that access from ports or through an open case is restricted. 2005 VVSG Vol 1: 7.4.1.c Verify the separation of election specific firmware and operating system are stored 2005 VVSG Vol 1: 7.4.1.d.
Threat Protection	Memory threat & virus scanning mechanisms. 2005 VVSG Vol 1: 7.5.2.d. Rootkit Scanning Mechanisms.
Audit Log	Audit logs and data files cannot be altered through the use of an alternate boot sequence without detection, and the test will consist of attempting to boot the devices using alternative media during boot sequences. Audit logs and data files cannot be altered through the use of editing tools without detection. The test will consist of attempting to edit the audit log to confirm that the system either: • Does not allow edits of the audit log or data files, or • Detects and reports all attempts at editing the audit log or data files.
Vote Count Integrity	Layered protection in shared environment 30. 2005 VVSG Vol 1: 7.5.4.
Data Protection	Access control lists preclude data leakage 2005 VVSG Vol 1: 7.5.4.d. Routers and firewalls preclude data leakage. Electronic policies prevent copy of data. Voting system access to incomplete election returns. 2005 VVSG Vol 1: 7.5.5.
External Access	Blocked central count environment access to incomplete election returns. 2005 VVSG Vol 1: 7.5.5.a. Voting machines with removable memory modules.

6 TEST DATA

6.1 Test Election Definitions

Using vendor documentation, SysTest Labs will define what an election contest will entail and how to create it for each Test Case. Defining an election involves:

- Determining specifically how a vendor's hardware and software handles an election contest.
- Determining if election is general or primary.
    - Defines the election precincts/splits, contests, candidates, and issues exactly as defined by election officials.
    - Defines the appropriate options for ballot content, verifying the appropriate contests/issues are displayed as determined in election creation.
- Determining types of contests and pass/fail criteria. Contest variables may include:
    - Partisan offices
    - Closed primaries
    - Open primaries
    - Primary presidential delegation nominations
    - Straight party voting
    - Ballot rotation
    - Cross-party endorsement
    - Split precincts
    - Vote 1 only
    - Vote 1 of many
    - Vote multiple of many
    - Write-in voting
    - No write-in voting
    - Overvotes
    - Undervotes
    - Blank ballots

- No candidates
- One candidates
- Many candidates
- Proposition/Referendum
- Provisional or challenged ballots

- Determining party preferences.
- Determining pre-election requirements (e.g., opening polls, printing zero report).
- Determining pre-voting steps (e.g., loading election to media).
- Determining post-voting steps (e.g., closing polls, tallying votes).

6.2 Test Vote Data

SysTest Labs will review, evaluate and use vendor documentation to create Vote Data or the test 'voters' for test cases. This Vote Data is created in matrix form and is used to ensure vote accuracy based on common standards.

The different combinations of candidates selected by each voter in the Vote Data Matrix validate the system's ability to:

- Record the appropriate options for casting and recording votes across a range of voting options.
- Record each vote precisely as indicated by the voter and be able to produce an accurate report of all votes cast.

The process for casting a ballot is defined in detail in individual test case steps. The test ballots are designed with formats and voting patterns sufficient to verify performance of the test election software. Ballots are cast in a number sufficient to demonstrate proper processing, error handling, and generation of audit data.

6.3 Data Recording

SysTest Labs will measure verification-testing progress against the Requirements Matrix. SysTest Labs will record all test results with each test case and related discrepancy report (as required). The status of all testing activity will be recorded via status report E-mails to NYSBOE. This is **Deliverable 2: Ongoing Project Management Services**.

6.4 Test Data Reduction

The test data defines the minimum number of combinations or alternatives of input and output conditions that constitute an acceptable test of the identified parameters. SysTest Labs will process the test data by manually recording data in the Test Case records and SysTest Labs' templates. SysTest Labs will identify any discrepancies found as well as update the discrepancy list with any resolutions submitted and retested. Screen shots will be generated or photos taken showing physical errors as they occur. All actual results will be identified should they differ from the expected results.

Comment [rz47]: All data relevant to the testing of a requirement must be made available to NYSBOE. Test reports should contain references to supporting data as needed so the reviewer can follow and make conclusions.

7 MATERIALS REQUIRED FOR TESTING

7.1 Software/Firmware

The Software and Firmware that is required for testing are specific to the Vendor and will be identified as part of the Voting System Specific Test Plan.

7.2 Equipment/Hardware

The Equipment and Hardware that is required for testing are specific to the Vendor and will be identified as part of the Voting System Specific Test Plan.

7.3 Test Materials

Items identified in Table 8 - *Test Materials* reflect all test materials required to perform hardware, software, security and integrated system tests. These are generic test materials and detailed required materials that are specific to a vendor will be identified within the Voting System Specific Test Plan.

Table 8 - Test Materials

Item
Ballot Box
Precinct kits / consumables: pens, secrecy sleeves, thermal printing tape, flash card, lithium ion battery, optical cleaning kits.
Compact flash card reader
Compact flash cards
PCMCIA card reader
PCMCIA cards
Installation disks
Proprietary removable data device readers
Proprietary removable data devices
Laser printer
Ink cartridges for laser printer(s) and/or BMD(s)

Item
Correctly sized paper ballots.
Null Modem Adapter: Adapt EPROM burner device to Trusted Build PC for firmware installation on chips.
Laser Printer and USB Cable: Laser Printer and cable used to connect to EMS servers for running testing reports.
Paper and manila Folders: For printing reports and organizing paperwork and test ballots.
Headset and microphone: For audio recording of voting information for testing to the Requirements Matrix.
Audio Measurement Device: For measuring the audio level of voting information for testing to the Requirements Matrix.
Power Strips: Used to provide power connections for multiple devices during testing.
Black ink pens or ball point pens with black ink.
Pencils with black lead.

7.4 Proprietary Data

SysTest Labs will indicate which portions of reports are considered proprietary information. SysTest Labs understands that material not classified as proprietary, including test plans and test reports, will become available to the public. Proprietary information will be submitted in a separate attachment to the NYSBOE, and marked "Proprietary."

8 TEST PROCEDURE AND CONDITIONS

8.1 Facility Requirements

Testing is performed on site at SysTest Labs in Colorado. All TDP and test documentation is stored in the secure project directory on SysTest Labs' secure NYSBOE Server.

SysTest Labs always ensures voting room doors are secured at all times, unless the current activity requires otherwise. Vendors are not permitted in the voting room unless a discrepancy discussion warrants their presence. In this case, the vendor's representative is escorted into the voting test lab by SysTest Labs' personnel. When they are satisfied they understand the discrepancy, they leave the voting test lab. Vendors are never left unattended in a voting test lab. The vendor's representative is only allowed in the voting test lab when testing has been suspended, no other activity is taking place, and they are escorted by SysTest Labs' personnel.

Environmental and EMC hardware testing for hardware components of each voting system will be executed at accredited environmental hardware testing facilities.

8.2 Test Setup

Each voting system specific test platform will be configured as part of the Physical Configuration Audit, in the standard configuration identified in the Vendor's TDP documents. The software will be installed, versions verified and made operational. The hardware will also be set up and versions verified according to the Vendor's TDP documents. Once the hardware and software has been set up, SysTest Labs will proceed with testing the system.

SysTest Labs' FCA Hardware Environmental Test Assessment will establish the baseline hardware configuration required for each voting system specific test and will be included as part of the Voting System Specific Test Plan. Should any changes to the hardware configuration be required as a result of any testing, SysTest Labs will assess the changes and determine what regression tests are required to ensure compliance to the Requirements Matrix.

8.3 Test Sequence

While there is no required sequence for performing voting system software verification testing and audits, there are prerequisite tasks for some testing. Tasks

and any applicable predecessor tasks, as outlined in 2005 VVSG, Volume 2: 1.4, are identified in Table 9 - *High-Level Verification Milestones in Sequence*.

Table 9 - High-Level Verification Milestones in Sequence

Verification Task	Prerequisite Task
Initial examination of system and TDP; and Scope Definition	Verify all components and documentation necessary for testing have been submitted. Define the Scope and effort needed for testing.
Vendor Quality Assessment	Review Vendor's Quality Assurance Program and Configuration Management Plan documentation.
NYSBOE Final Master Test Plan	Develop a Final Master Test Plan. Acceptance of Final Master Test Plan.
NYSBOE Voting System Specific Test Plan	Develop the Master Voting System Specific Test Plans. Acceptance by NYSBOE of Voting System Specific Test Plans. Review of TDPs and all prior certification testing
FCA – Voting System Specific Test Case Development	Documentation TDP review. Mapping of voting system specific requirements and supported functionality to the Requirements Matrix.
FCA – Voting System Specific Test Procedure Development	Voting System Specific Test Cases identified. Mapping of voting system specific requirements and supported functionality to the Requirements Matrix.
PCA – System Configuration Audit	Equipment received at SysTest Labs, staff trained on system, and documentation available, including discrepancy reporting.
Source Code Review	The Master TDP Review Plan is completed and approved.
Trusted Build	Completion of PCA source code review with no open discrepancies.

Verification Task	Prerequisite Task
FCA – Hardware Environmental Testing	Completion of FCA test case preparation and PCA system configuration audit. Initiation of hardware and performance testing, including discrepancy reporting.
FCA – Accuracy Testing	Completion of all FCA Accuracy related test cases and test procedures. Test Data available. Environmental testing completed. Discrepancies reported.
FCA – System Testing	Completion of all FCA System related test cases and test procedures. Test Data available. Discrepancies reported.
FCA – Security Testing	Completion of all FCA Security related test cases and test procedures. Test Data available. Discrepancies reported.
FCA – Regression and Discrepancy Testing	Receipt of applicable discrepancy fixes (source code, documentation, hardware, firmware) or Vendor's response.
Examine the system maintenance manual	The Master TDP Review Plan is completed and approved.
Final Voting System Specific Test Report	Successful completion of all audits, reviews, and validation tasks. Discrepancies resolved and re-validated, or noted as not resolved. All results mapped back to associated requirements.
Delivery of Final Voting System Specific Test Report	Final Voting System Specific Test Report Delivered to NYSBOE.

8.4 Test Operations Procedures

The SysTest Labs Test Team will provide step-by-step procedures for each test case to be performed. Each step shall be assigned a test step number; this number, along with critical test data and test procedure information, shall be tabulated onto a test execution form for test control and the recording of test results. These test execution forms contain sufficient detail to allow for consistent and repeatable test execution.

Comment [rz48]: The Requirements Matrix should map toe the test procedures within each test case. All of this information will be available to NYSBOE as part of the final reports.

An inventory will be performed to verify the voting equipment received contains hardware and software elements as defined by the TDP and the PCA System Configuration Audit prior to commencement of FCA Testing.

The PCA will include verification that the system can be configured using the system operations manuals.

Throughout the testing effort, test steps will be marked as follows:

- *Accept* – Test is accepted as successful.
- *Reject* – Test is rejected as unsuccessful.
- *NT* – Not Testable is used for test procedures that cannot be followed. For example, if failure of one test procedure precludes attempting subsequent test procedures, the latter will be marked as NT. Also, for expected functionality that is not implemented, the test procedure will be marked as NT.
- *NS* – Not Supported is used for requirements not supported in the tested configuration.
- *NA* – Not Applicable - If a test procedure is not applicable to the current verification test effort, it will be marked as NA. The NA designation would also be entered for any subsequent step that is not applicable.

Test results marked as *Reject*, *NT*, and *NA* will include comments by the Tester explaining the reason for the result.

Issues encountered during testing will be documented in a discrepancy report. Issues that do not conform to the Requirements Matrix will be marked as *Hardware Discrepancies*, *Functional Discrepancies*, or *Documentation Discrepancies* (a discrepancy occurs when the hardware, software or firmware, or the documentation does not meet defined requirements in the Requirements Matrix). Each discrepancy will contain, at a minimum, the following information:

- A unique identifier
- Vendor's name

- Voting system name and version
- Trusted build version
- Trusted build date
- Date discrepancy opened
- Status (*open, awaiting vendor response, in regression test, closed*)
- Date of last update to discrepancy
- Type of discrepancy (*hardware, functional, documentation, informational*)
- Details of discrepancy (test case, test case step, narrative and comments, requirement, etc.)
- Tester names
- Type of test (*system, security, accuracy*, *hardware*)
- Test case and test steps
- Applicable requirement(s)
- Vendor's response

Each Vendor must address all discrepancies. Discrepancy that are encountered during testing, but are not related to the Requirements Matrix will be added to the discrepancy report and noted as *Informational*. All responses by each Vendor are included in the discrepancy report. All discrepancy reports will be included as an attachment to the Voting System Specific Verification Report.

8.5 Test Error Recovery

The SysTest Labs Test Team will verify that the voting system can recover from a non-catastrophic failure of a device, or from any error or malfunction that is within an operator or election official's ability to correct.

When an error occurs, the appropriate restore, resume and recover procedures in the vendor's documentation will be followed to attempt to alleviate the error condition. If this effort is unsuccessful, a discrepancy noting the failure will be added to the appropriate discrepancy report.

9 APPENDIX A – TEST CASES

Comment [rz49]: Most of the test cases listed in appendix A appear not to be numbered while the Requirements Matrix (in somp places) maps to numbered steps within these test cases.

Table 10 - Election Core

Test Detail	Test Methodology
Test Case Name	**(Election Core definition)**
NOTE	*This Election Core definition is **always** to be used in conjunction with another test case. All base requirements are defined here for validating election testing. For specific testing variations, see the following test cases that incorporate this **Election Core**.*
Scope	A system level test that uses The 2005 Voting System Guidelines to validate required functionality and performance. Testing includes accuracy, ballot format handling capability, reporting, and usability of the hardware, software and procedures in the entire voting system.
Objective	*Refer to each test case for specific **Objectives**.*
Standards Documents	Voluntary Voting system guidelines 2005, vol. 1 Voluntary Voting system guidelines 2005, vol. 2 Specific standards are noted in following steps.
Variables: Voting Variations	The vendor's TDP documents specifically identify which Voting Variations *can* and *cannot* be supported by the system. The documents are reviewed and evaluated. The supported items are verified in one or more election test case. The following is a partial list of items specified in the VVSG: (V1:2.1.7.2), that pertain to New York requirements. • Closed primaries • Partisan offices • Write-in voting • Primary presidential delegation nominations • Ballot rotation • Cross-party endorsement • Split precincts • Vote for N of M • Provisional or challenged ballots *Refer to each test case for the election specific **Voting Variations**.*
Variables: Election Variations	*Refer to each test case for specific **Election Variations**.*

Comment [rz50]: This core test case is missing the reference to the NYS Law and 6209 procedures.

Test Detail Test Case Name	Test Methodology (Election Core definition)
	Additionally, verification is done to ensure that Ballot boxes and ballot transfer boxes, which serve as secure containers for the storage and transportation of voted ballots, adhere to standards (V1:4.1.4.2.d) For each iteration that the election is run: • All supplies necessary for testing are retrieved. • Verification is performed on the System to ensure that the correct versions of software, firmware and hardware, election and ballot is installed and set up as defined in the user documentation • A supervisory level access 'user' and password' is created or available • The Readiness Check List is completed if applicable • The date and tester(s) are documented Testers are informed that the test environment must remain static, if not, no changes shall occur without documentation in the test record and the authorization of the project manager.
Documentation: **Test Data & Test Results**	For each iteration that the election is run: • Capture all voting steps in order to maintain repeatability of the test • Record election, ballot, and vote data fields on the corresponding worksheet tabs • Save all worksheet tabs for all iterations of the test case • Record results of test run by entering 'Accept/Reject' on the Test Results Matrix • Provide comments when observing deviations, discrepancies or notable observations • Log discrepancies on the Discrepancy Report
Pre-vote: **Ballot Preparation procedures verifications**	Verification of Common standards includes the following and ensures that the system: • Enables 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 district • Collects and maintains data pertaining to offices and their associated labels and instructions, candidate names and their associated labels, and issues and measures and their associated text • Supports the maximum number of potentially active voting positions as indicated in vendor documentation • For Primary Elections, generates ballots that segregate the choices in partisan races by party affiliation • Generates ballots that contain identifying codes or marks uniquely associated with each new format • Ensures the vote response fields, selection buttons, or switches properly align with the specific candidate names and/or issues printed or displayed on the ballot (V1:2.2.1.1) Verification of Paper-Based systems ensures that the system: • Enables voters to make selections by marking a mark in areas designated for this purpose • For marksense systems, ensures that the timing marks align properly with the vote response fields (V1:2.2.1.1) Verification of Ballot Production common standards ensures that:

Test Detail Test Case Name	Test Methodology (Election Core definition)
	• The electronic display or paper 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, and as supported by the vendor • The electronic display or paper ballot does not show any advertising or commercial logos unless specifically provided for in State law. Electronic displays shall not provide connection to such material through a hyperlink • The ballot conforms to the vendor specifications for type of paper stock, weight, size, shape, size and location used to record votes, folding, bleed through, and ink for printing if paper ballots are used as part of the voting system (V1:2.2.1.3) For paper based recording, verification is performed to ensure the following: • A ballot can be accurately/securely defined and formatted (V1:4.1.4.2) • A ballot can be accurately/securely programmed and installed into the appropriate media (V1:4.1.4.2.c) • The system Ignores, and extraneous perforations, smudges, and folds (V1:4.1.5.2.e) During the election definition and ballot preparation process, verification is performed to ensure that the system audits the preparation of the baseline ballot formats and modifications to them, a description of these modifications, and corresponding dates. The log is to include: • The allowable number of selections for an office or issue • The combinations of voting patterns permitted or required by the jurisdiction • The inclusion or exclusion of offices or issues as the result of multiple districting within the polling place • Any other characteristics that may be peculiar to the jurisdiction, the election, or the polling place's location • Manual data maintained by election personnel • Samples of all final ballot formats • Ballot preparation edit listings (V1:5.4.1) Verification of Ballot Formatting ensures that the system supports: • Creation of newly defined elections • Rapid and error-free definition of elections and associated ballot layouts • Uniform allocation of space and fonts, ensuring no perception of a preferred contest/candidate • Simultaneous display of the maximum number of choices for a contest • Retention of previously defined formats for an election • Prevention of unauthorized modification of any ballot formats • Modifications by authorized personnel of a previously defined ballot format (V1:2.2.1.2)
Pre-vote:	System Preparation - Security:

Test Detail Test Case Name	Test Methodology (Election Core definition)
Preparation - Security	• System username/password authentication and other access controls are set up according to system documentation guidelines for all devices being tested. • Any/all unnecessary processes are disabled and/or required process control measures noted in the documentation are followed. • All COTS and vendor subsystems used for system security are configured and active as recommended by the system documentation. This includes all connection, port, virus, and data or authorized process restriction systems. • Any other pre-election system security measures listed in the documentation are followed including setup of additional hardware or software not covered above. Please also see the Documentation section of the Security Test Case within Appendix A.
Readiness Testing and Poll Verification	Verification of Common Standards for Readiness Testing ensures that: • Voting machines or vote recording and data processing equipment, precinct and central count equipment are properly prepared for an election, and collect data that verifies equipment readiness • Status and data reports from each set of equipment can be obtained • The correct installation and interface of all system equipment • Hardware and software function correctly • Consolidated data reports at the polling place and higher jurisdictional levels can be generated • There is Segregation of test data from actual voting data, either procedurally or by hardware/software features (V1:2.2.4) When resident test software, external devices, and special purpose test software may be connected or installed in the voting device to simulate operator and voter functions provided the following standards are verified to ensure that: • These elements are capable of being tested separately, and shall be proven to be reliable verification tools prior to their use • These elements are incapable of altering or introducing any residual effect on the intended operation of the voting device during any succeeding test and operational phase (V1:2.2.4) Vendor documentation is reviewed, evaluated and used to create steps that ensure all voting systems and equipment function properly before and during an election. Verification of these steps provide a formal record of the following: (V1:2.2.5) • The election's identification data • The identification of all equipment units • The identification of the polling place • The identification of all ballot formats

Comment [rz51]: To be clear this should state that system documentation related to process controls should be followed. If the vendor documentation does not state to disable a process the tester should not disable it.

Test Detail Test Case Name	Test Methodology (Election Core definition)
	• The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain only zeros) • A list of all ballot fields that can be used to invoke special voting options • Other information needed to confirm the readiness of the equipment, and to accommodate administrative reporting requirements (V1:2.2.5) To prepare voting devices to accept voted ballots, all voting systems are verified to ensure that they provide the capability to test each device prior to opening. This verifies that each is operating correctly. The tests include: • Confirmation that there are no hardware or software failures (V1:2.2.5) • Confirm that the device is ready to be activated for accepting votes (V1:2.2.5) • Confirmation that the test data is separate from voting data without impact to the testing (V1:2.2.4.f) Prior to Opening the polls, verification at the Central Location is performed to ensure that vote counting and vote consolidation equipment and software function properly. Any system used in a central count environment provides a printed record of the following: (V1:2.2.6) • The election's identification data • The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain all zeros) • Other information needed to ensure the readiness of the equipment and to accommodate administrative reporting requirements (V1:2.2.6) Verification is performed to ensure the following: • A list of all ballot fields is created (V1:4.1.4.2) • The voting device is ready to accept votes (V1:4.1.4.3)
Voting: Opening the Polls Verification	Verification of the Readiness checklist is performed, ensuring that it is complete. Vendor documentation is reviewed, evaluated and used to create steps that ensure all voting systems and equipment perform voting functions properly. These steps are created, using the guidelines listed in volume 1, section 2.3. Verification of these steps provide a formal record of the following: • Opening the polls • Casting a ballot

Comment [rz52]: Requirements in the matrix should map to steps within each test case. Mapping the test case to requirements as is done here and throughout the test cases is fine for linking back to requirements however the mapping from the matrix to tests cases and steps within test cases is what is required.

Test Detail Test Case Name	Test Methodology (Election Core definition)
	Additionally, verification ensures that all DRE systems support: o Activating the ballot o Augmenting the election counter o Augmenting the life-cycle counter (V1:2.3) If necessary, any issues, failures, or unexpected results and their required corrective action(s) are identified and recorded here. (V1: 2.3.1) Verification of Opening Polls for Precinct Count Systems (paper based) ensures: • An internal test of diagnostic capability to verify that all of the polling place tests specified in section 1, 2.2.5 have been successfully completed • Automatic disabling any device that has not been tested until it has been tested. (V1: 2.3.1.1) Verification of Paper-based Systems ensures: • A means of verifying that ballot marking devices are properly prepared and ready for use • A voting booth or similar facility, in which the voter may mark the ballot in secrecy • Secure receptacles for holding voted ballots • Activating the ballot counting device • Verifying the device has been correctly activated and is functioning properly • Identifying device failure and corrective action needed (V1:2.3.1.2) Verification of Opening Polls for Precinct Count Systems (DRE) ensures that: • A security seal, password, or a data code recognition capability to prevent the inadvertent or unauthorized actuation of the poll-opening function • A means of enforcing the execution of steps in the proper sequence • A means of verifying the system has been activated correctly • A means of identifying system failure and any corrective action needed (V1:2.3.1.3) Verification of Activating the Ballot (DRE) ensures that the system: • Enables election officials to control the content of the ballot presented to the voter, whether presented in printed form or electronic display, such that each voter is permitted to record votes only in contests in which that voter is authorized to vote • Allows each eligible voter to cast a ballot • Prevents a voter from casting more than one ballot in the same election • Activates the casting of a ballot in a general election • Enables the selection of the ballot that is appropriate to the party affiliation declared by the voter in a primary election • Activates all portions of the ballot upon which the voter is entitled to vote • Disables all portions of the ballot upon which the voter is not entitled to vote

Test Detail Test Case Name	Test Methodology (Election Core definition)
	(V1:2.3.2) Verification of Casting a Ballot Common Standards ensures that the system: • Verifies that additional functional capabilities that enable accessibility to disabled voters as defined in volume 1, section 3.2 (V1:2.3.3) • Provides text that is at least 3mm high and provide the capability to adjust or magnify the text to an apparent size of 6.3 mm • Protects the secrecy of the vote such that the system cannot reveal any information about how a particular voter voted, except as otherwise required by individual State law • Records the selection and non-selection of individual vote choices for each contest and ballot measure • Records the voter's selection of candidates whose names do not appear on the ballot, if permitted under State law, and record as many write-in votes as the number of candidates the voter is allowed to select • In the event of a failure of the main power supply external to the voting system, provides the capability for any voter who is voting at the time to complete casting a ballot, allow for the graceful shutdown of the voting system without loss or degradation of the voting and audit data, and allow voters to resume voting once the voting system has reverted to back-up power; and • Provides the capability for voters to continue casting ballots in the event of a failure of a telecommunications connection within the polling place or between the polling place and any other location. (V1:2.3.3.1) Verification is performed to ensure that the system: • Allows the voter to easily identify the voting field that is associated with each candidate or ballot measure response • Allows the voter to punch or mark the ballot to register a vote • Allows either the voter or the appropriate election official to place the voted ballot into the ballot counting device (for precinct count systems) or into a secure receptacle (for central count systems) • Protects the secrecy of the vote throughout the process. • Provides feedback to the voter that identifies specific contests or ballot issues for which an overvote or undervote is detected • Allows the voter, at the voter's choice, to vote a new ballot or submit the ballot 'as is' without correction • Allows an authorized election official to turn off the capabilities defined above (V1:2.3.3.2) Additionally, verification is performed to ensure that all DRE systems: • Prohibit the voter from accessing or viewing any information on the display screen that has not been authorized by election officials and preprogrammed into the voting system (i.e., no potential for display of external information or linking to other information sources) • Enable the voter to easily identify the selection button or switch, or the active area of the ballot display that is associated with each candidate or ballot measure

Test Detail Test Case Name	Test Methodology (Election Core definition)
	response • Allow the voter to select his or her preferences on the ballot in any legal number and combination • Indicate that a selection has been made or canceled • Indicate to the voter when no selection, or an insufficient number of selections, has been made in a contest • Prevent the voter from overvoting • Notify the voter when the selection of candidates and measures is completed • Allow the voter, before the ballot is cast, to review his or her choices and, if the voter desires, to delete or change his or her choices before the ballot is cast • For electronic image displays, prompt the voter to confirm the voter's choices before casting his or her ballot, signifying to the voter that casting the ballot is irrevocable and directing the voter to confirm the voter's intention to cast the ballot • Notify the voter after the vote has been stored successfully that the ballot has been cast • Notify the voter that the ballot has not been cast successfully if it is not stored successfully, including storage of the ballot image, and provide clear instruction as to the steps the voter should take to cast his or her ballot should this event occur • Provide sufficient computational performance to provide responses back to each voter entry in no more than three seconds • Ensure that the votes stored accurately represent the actual votes cast; • Prevent modification of the voter's vote after the ballot is cast; • Provide a capability to retrieve ballot images in a form readable by humans [in accordance with the requirements of volume 1, sections 2.1.2 (f) and 2.1.4 (k) and (l)] • Increment the proper ballot position registers or counters • Protect the secrecy of the vote throughout the voting process • Prohibit access to voted ballots until after the close of polls • Provide the ability for election officials to submit test ballots for use in verifying the end-to-end integrity of the system • Isolate test ballots such that they are accounted for accurately in vote counts and are not reflect in official vote counts for specific candidates or measures (V1:2.3.3.3)
Voting: **Required functionality verifications**	Vendor documentation is reviewed, evaluated and used to create Vote Data or the test 'voters' for this test case. This Vote Data is created in matrix form and is used to ensure vote accuracy based on common standards listed in volume 1, section 2.1.2. Each 'voter' in the Vote Data Matrix votes the ballot. A SysTest employee performs this manually. The different combinations of candidates selected by each voter in the Vote Data Matrix validates the system's ability to: • Record the election precincts/splits, contests, candidates, and issues exactly as defined by election officials • Record the appropriate options for ballot content, verifying the appropriate contests/issues are displayed as determined in election creation • Record the appropriate options for casting and recording votes across a range of voting options • Record each vote precisely as indicated by the voter and be able to produce an accurate report of all votes cast

Test Detail Test Case Name	Test Methodology (Election Core definition)
	• 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 • 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 (V1:2.1.2) The process for casting a ballot is defined in detail in individual test case steps. These cases, steps, and verification criteria are created using the requirements stated in volume 1, section 2.3.3 and section 5.5. Additionally, the Vendor documentation is evaluated and used to enhance the testing procedures. The standards used for validation consist of the following sections: • Common Standards (V1:2.3.3.1) • Paper-Based Systems Standards (V1:2.3.3.2) • DRE Systems Standards (V1:2.3.3.3) • Vote Secrecy (DRE Systems) (V1:5.5) Backup files are made and hard copies printed for all DRE systems to record and retain redundant copies of the original ballot image (V1:2.1.2.f) System auditing and functional testing is performed in order to validate vote data, precinct counts, central counts, audit records and error logs. Verification is performed on the error logs based on the standards listed in volume 1, section:2.1.5 The test ballots are designed with formats and voting patterns sufficient to verify performance of the test election programs. Ballots are cast in a number sufficient to demonstrate proper processing, error handling, and generation of audit data as specified in volume 1, sections 2 and 4. Test case steps are performed during the Functionality Testing in Parallel with Hardware Testing for Precinct Count Systems to verify voting functions defined in volume 1, sections 2.3 and 2.4 of voting equipment and precinct counting equipment. Verification ensures that: • Preparation of the election programs: o Verify resident firmware, if any o Prepare software (including firmware) to simulate all ballot format and logic options for which the system will be used o Verify program memory device content o Obtain and design test ballots with formats and voting patterns sufficient to verify performance of the test election programs • Procedures to program precinct ballot counters: o Install program and data memory devices, or verify presence if resident o Verify operational status of hardware • Procedures to simulate opening of the polls: o Perform procedures required to prepare hardware for election operations

Test Detail	Test Methodology
Test Case Name	(Election Core definition)
	o Obtain a zero report or other evidence that data memory has been cleared o Verify audit record of pre-election operations o Perform procedures required to open the polling place and enable ballot counting • Procedures to simulate counting ballots cast test ballots in a number sufficient to demonstrate proper processing, error handling, and generation of audit data • Procedures to simulate closing of polls: o Perform hardware operations required to disable ballot counting and close polls o Obtain data reports and verify correctness o Obtain audit log and verify correctness (V2:3.3, 3.3.1) Test case steps are performed during the Functionality Testing in Parallel with Hardware Testing for Central Count Systems to verify voting functions defined in volume 1, 2.3 and 2.4. Verification ensures that: • Procedures to prepare election programs: o Verify resident firmware, if any o Prepare software (including firmware) to simulate all ballot format and logic options for which the system will be used, and to enable simulation of counting ballots from at least 10 polling places or precincts o Verify program memory device content o Procure test ballots with formats, voting patterns, and format identifications sufficient to verify performance of the test election programs • Procedures to simulate counting ballots count test ballots in a number sufficient to demonstrate proper processing, error handling and generation of audit data as specified in volume 1, sections 2 and 4. • Procedures to simulate election reports: o Obtain reports at polling places or precinct level o Obtain consolidated reports o Provide query access, if this is a feature of the system o Verify correctness of all reports and queries Obtain audit log and verify correctness (V2: 3.3.2) Integrity measures ensure the physical stability and function of the vote recording and counting processes. Verification is performed to ensure that both Common Standards and DRE Systems Standards are followed. (V1:2.1.4) Common Standards are used to ensure system integrity by validating that the voting system: • Protects, by a means compatible with these Standards, against a single point of failure that would prevent further voting at the polling place • Protects against the interruption of electronic power • Protects against generated or induced electromagnetic radiation • Protects against ambient temperature and humidity fluctuations • Protects against the failure of any data input or storage device • Protects against any attempt at improper data entry or retrieval • Records and report the date and time of normal and abnormal events

Test Detail	Test Methodology
Test Case Name	(Election Core definition)
	• Maintains a permanent record of all 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.) • 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 • Include built-in measurement, self-test, and diagnostic software and hardware for detecting and reporting the system's status and degree of operability (V1:2.1.4) DRE Systems Standards are used to ensure system integrity by validating that the voting system: • Maintains a record of each ballot cast using a process and storage location that differs from the main vote detection, interpretation, processing, and reporting path • Provides a capability to retrieve ballot images in a form readable by humans. (V1:2.1.4) Audit records are prepared for all testing phases of election operations using devices designed to be controlled by the jurisdiction or its contractors. These records rely upon automated audit data acquisition and machine-generated reports, with manual input of some information. These records address the ballot preparation and election definition phase, system readiness tests, and voting and ballot-counting operations. Individual test cases and steps contain instructions on how and when to generate and validate this information. (V1:2.1.5.1, 5.4) All voting systems are evaluated and verified to ensure that they meet the following requirements for time, sequence and preservation of Audit Records: • Except where noted, systems provide the capability to create and maintain a real-time audit record • All systems include a real-time clock as part of the system's hardware • All audit record entries include the time-and-date stamp • The audit record are active whenever the system is in an operating mode • The generation of audit record entries are not terminated or altered by program control, or by the intervention of any person • Once the system has been activated for any function, the system preserves the contents of the audit record during any interruption of power to the system until processing and data reporting have been completed • The system is capable of printing a copy of the audit record (V1:2.1.5.1.a, 4.1.7, 4.1.7.2) All voting systems are evaluated and verified to ensure that they meet the following requirements for Error Messages: • The system generates, stores, and reports to the user all error messages as they occur • All error messages requiring intervention by an operator or precinct official are displayed or printed unambiguously in easily understood language text, or by

Test Detail	Test Methodology
Test Case Name	(Election Core definition)
	means of other suitable visual indicators • When the system uses numerical error codes for trained technician maintenance or repair, the text corresponding to the code is self-contained, or affixed inside the unit device • All error messages for which correction impacts vote recording or vote processing are 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 • The message cue for all systems clearly state the action to be performed in the event that voter or operator response is required • System design ensures that erroneous responses will not lead to irreversible error • Nested error conditions are corrected in a controlled sequence such that system status shall be restored to the initial state existing before the first error occurred (V1:2.1.5.1.b) All voting systems are evaluated and verified to ensure that they meet the following requirements for Status Messages: • When the jurisdiction requires, some status and information messages are displayed and reported in real-time • Messages that do not require operator intervention may be stored in memory to be recovered after ballot processing has been completed • The system displays and reports critical status messages using unambiguous indicators or English language text • The system need not display non-critical status messages at the time of occurrence • 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 • Systems provide a capability for the status messages to become part of the real-time audit record • The system provides a capability for a jurisdiction to designate critical status messages (V1:2.1.5.1.c) Exception Handling (Central Count) 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, verification is done to ensure that all central count paper-based systems: • Outstack the ballot, or • Stop the ballot reader and display a message prompting the election official or designee to remove the ballot, or • Mark the ballot with an identifying mark to facilitate its later identification. (V1:4.1.5.1.b) Exception Handling (Precinct Count) refers to the handling of ballots for a precinct count system when they are unreadable or when some condition is detected requiring that the

Test Detail Test Case Name	Test Methodology (Election Core definition)
	cards be segregated from normally processed ballots for human review. All paper based precinct count systems are validated to ensure that the following can be accomplished: • An unreadable or blank ballot - return the ballot and provide a message prompting the voter to examine the ballot • Ballot with a write-in vote - segregate the ballot or mark the ballot with an identifying mark to facilitate its later identification • A ballot with an overvote the system: o Provides a capability to identify an overvoted ballot o Returns the ballot o Provides an indication prompting the voter to examine the ballot; o Allows the voter to submit the ballot with the overvote o Provides a means for an authorized election official to deactivate this capability entirely and by contest • In response to a ballot with an undervote the system: o Provides a capability to identify an undervoted ballot o Returns the ballot o Provides an indication prompting the voter to examine the ballot o Allows the voter to submit the ballot with the undervote o Provides a means for an authorized election official to deactivate this capability (V1:4.1.5.1.d) Processing speed is verified for DRE voting systems to ensure that they: • Operate at a speed sufficient to respond to any operator and voter input without perceptible delay (no more than three seconds) • If the consolidation of polling place data is done locally, performs this consolidation in a time not to exceed five minutes for each device in the polling place. (V1:4.1.6.2.a)
Voting: **Optional functionality verifications**	The functionality listed above in "**Variables: Voting Variations"** is verified here.
Post-Vote: **Closing the Polls**	Vendor documentation is reviewed, evaluated and used to create steps that ensure that all voting systems and equipment perform voting functions properly for all Post-Voting Functions. These steps are created, using the guidelines listed in volume 1, section 2.4. Verification of these steps provide a formal record of the following: • All systems provide capabilities to accumulate and report results for the jurisdiction and to generate audit trails (V1:2.4) • Precinct count systems provide a means to close the polling place including generating appropriate reports (V1:2.4) • The standards for closing the polling place are specific to precinct count systems. The system provides the means for: o Preventing the further casting of ballots once the polling place has closed o Providing an internal test that verifies that the prescribed closing procedure has been followed, and that the device status is normal o Incorporating a visible indication of system status o Producing a diagnostic test record that verifies the sequence of events, and

Test Detail Test Case Name	Test Methodology (Election Core definition)
	indicates that the extraction of voting data has been activated o Precluding the unauthorized reopening of the polls once the poll closing has been completed for that election (V1:2.4.1) • All systems provide a means to consolidate vote data from all polling places, and optionally from other sources such as absentee ballots, provisional ballots, and voted ballots requiring human review (e.g., write-in votes). (V1:2.4.2) • All systems are able to create reports summarizing the data on multiple levels (V1:2.4.3) • *If applicable*, the 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: o Provide only aggregated results, and not data from individual ballots o Provide no access path from unofficial electronic reports or files to the storage devices for official data o Clearly indicate on each report or file that the results it contains are unofficial (V1:2.4.4)
Post-Vote: **Vote Count Verification**	After all voting listed in the Vote Data Matrix is performed, the election data is examined and all counts are validated on the individual voter level, the voting machine level, the precinct level and the central count level. This verification ensures that the system is correctly tabulating all data and is accurately recording cast ballots, including provisional. (V1:2.1.7.1, 2.2.6, 2.4, 4.1.3.1, 4.1.5.2, 4.1.6.2.b, 4.1.4.3.c) This tabulation sometimes includes verification of the following: • Ensure undervotes are counted as cast votes • Separate accumulation of Undervotes and Paper Overvotes • Ensure Overvotes are counted on paper ballots and tally correctly
Post-Vote: **Security**	Post-Vote - Security: • System username/password authentication and other access controls are set up according to system documentation guidelines for all devices being tested. • Any/all unnecessary processes are disabled and/or required process control measures noted in the documentation are followed. • All COTS and vendor subsystems used for system security are configured and active as recommended by the system documentation. This includes all connection, port, virus, auditing capability, data or authorized process restriction systems. • Any other system security measures listed in the documentation are followed including setup of additional hardware or software not covered above. Please also see the Documentation section of the Security Test Case within Appendix A.
Post-Vote:	All applicable system reports are produced and verified at this point. The requirements listed in volume 1 are followed for verifying Data and Document Retention. These include the following:

Comment [rz53]: It looks like the pre-vote security steps and post-vote security stesps are identical How can this be?

Test Detail Test Case Name	Test Methodology (Election Core definition)
System Audit and Data Retention	• Data and Document Retention (V1:5.3) • Audit Record Data (V1:5.4) Additionally, the guidelines listed in volume 1, section 4.1.8.2, are used to validate Data Report Generation.
Results are Observed	Review the outcome of the test(s) against the expected result(s): • **Accept**: expected results is observed • **Reject:** expected result is NOT observed • **Not Testable (NT)**: rejection of a previous test step prevents validation of this step or this was tested in another test case • **Not Applicable (NA):** not applicable to the current test scope or to the component under review • **Not Supported (NS)**: not supported in the current test scope
Record Observations and all input/outputs for each election	All information used in processing the test case is captured. This includes: inputs, outputs, deviations and any other item that may impact the validation of the test case. Any failure of the test against the EAC guidelines is reported and implies failure of the system. Failures are reported as Defect Issues in the Discrepancy Report and are provided to the manufacturer. Before the final Certification Test Report is issued, manufacturers are given the opportunity to correct all discrepancies. If the manufacturer submits corrections, retests are performed. Issues that do not impact the failure of the requirements but could be considered defects are logged as Informational Issues on the Discrepancy Report. It is the manufacturer's option to address these issues.

Table 11 - General_Election_01

Test Detail	Test Methodology
Test Case Name	**GEN01**
NOTE	*This test case is to be used in conjunction with the **Election Core definition**.*
Objective	The object of this test case is to verify core functionality and performance by using vendor manual(s) to create election ballots, vote, and tally, for a General Election.
Variables: **Voting Variations**	The following are the items verified in this election: (V1:2.1.7.2) • 2 Precincts • Split Precincts (3 splits per precinct) **Partisan contests:** • "Vote for 1" race with a single candidate and a write-in (Superintendent of Schools) • "Vote for 1" race with a single candidate and a write-in (Sheriff) • "Vote for 1" race with a single candidate and a write-in (Attorney General) • "Vote for 1" race with two candidates and write-ins (County Treasurer) • "Vote N of M" on Multi-member board (County Commissioner) • "Vote N of M" on Multi-member board which includes declared candidates with write-in voting (City Council) • "Vote for 1" race where one party does not declare candidates (Secretary of State) • Slate / Group voting: one selection votes the slate (Governor/Lt. Governor) • Rotation = Standard (Rotates with every new Precinct) (Governor/Lt. Governor) **Propositions/Questions:** • Proposition/Question (Proposition X)
Variables: **Election Variations**	**Governor/Lt. Governor**: 4 candidates **Sheriff**: 1 candidate/write-in **Superintendent of Schools**: 1 candidate/1 write-in **County Commissioner**: 4 candidates **Proposition X:** Y/N **Secretary of State**: 3 candidates (no DEM candidate) **City Council**: 6 candidates/write-in **Attorney General**: 1 candidate/write-in **County Treasurer:** 2 candidates/write-in

Test Detail	Test Methodology
Test Case Name	**GEN01**
A description of the voting system type and the operational environment	*List of all DRE, BMD and any other hardware or software that is used in the voting environment for this test case.* **Software** • ***FILL IN per Vendor*** **Hardware** • ***FILL IN per Vendor***

Table 12 - General_Election_02

Test Detail	Test Methodology
Test Case Name	**GEN02**
NOTE	*This test case is to be used in conjunction with the **Election Core definition**.*
Objective	The object of this test case is to verify core functionality and performance by using vendor manual(s) to create election ballots, vote, and tally, for a General Election: Straight Party.
Variables: **Voting Variations**	The following are the items verified in this election: (V1:2.1.7.2) • Single page ballot election per voter • 7 precincts and no split precincts • Cross-over voting **Partisan contests:** • "Vote for 1" race with a single candidate and a write-in (Superintendent of Schools) • "Vote for 1" race with a single candidate and write-ins (Sheriff) • "Vote N of M" on Multi-member board (County Commissioner) • "Vote for 1" race with a single candidate and a write-in (Attorney General) • "Vote for 1" race with two candidates and write-ins (County Treasurer) • "Vote N of M" on Multi-member board which includes declared candidates with write-in voting (City Council) • "Vote for 1" race where one party does not declare candidates (Secretary of State) • Slate & Group voting: one selection votes the slate (Governor/Lt. Governor) **Propositions/Questions:** • Proposition/Question (Proposition X)
Variables: **Election Variations**	**Governor/Lt. Governor**: 4 candidates **Sheriff**: 1 candidate/write-in **Superintendent of Schools**: 1 candidate/1 write-in **County Commissioner**: 4 candidates **Proposition X:** Y/N **Secretary of State**: 3 candidates (no DEM candidate) **City Council**: 6 candidates/write-in **Attorney General**: 1 candidate/write-in **County Treasurer:** 2 candidates/write-in

Test Detail	Test Methodology
Test Case Name	**GEN02**
A description of the voting system type and the operational environment	*List of all DRE, BMD and any other hardware or software that is used in the voting environment for this test case.* **Software** • ***FILL IN per Vendor*** **Hardware** • ***FILL IN per Vendor***

Table 13 - General_Election_03 (Usability and Accessibility)

Test Detail	Test Methodology
Test Case Name	**GEN03 - Usability and Accessibility**
NOTE	*This test case is to be used in conjunction with the **Election Core definition**.*
Scope	A system level test case that uses the 2005 Voluntary Voting System Guidelines (VVSG) to validate required functionality and performance as guidance in order to met 2002 HAVA requirements. Testing includes ballot marking accuracy, General Accessibility, Vision, Dexterity, Mobility, Hearing, Speech, Language Proficiency, and Cognition requirements.
Objective	The object of this test case is to verify that usability, accessibility and all supported multi-lingual elections can be created for use on BMDs. All voters have the ability to vote privately and independently including using accessibility hardware; i.e. visual displays, Sip-n-Puffs, audio, or foot paddles/rockers. Additionally, ballots are marked correctly and that the voter can independently verify the ballot before it is cast and counted.
Variables: **Voting Variations**	The following are the items verified in this election: (V1: 2.1.7.2) • 1 precinct **Partisan contests:** • "Vote for 1" race with a single candidate and write-ins (Sheriff) • "Vote N of M" on Multi-member board (City Council) **Propositions/Questions:** • Proposition/Question (Proposition X) **Audio ballots** **Multi-language ballots to be tested include:** o ***(List supported languages here)*** o *English* o *Lang 2* o *Lang 3, etc.*
Variables: **Election Variations**	**Sheriff**: 3 candidates/rotate by candidate **Proposition X:** Y/N **City Council**: 6 candidates/write-in
A description of the voting system type and the operational environment	*List of all DRE, BMD and any other hardware or software that is used in the voting environment for this test case.* **Software** • ***FILL IN per Vendor*** **Hardware**

Test Detail	Test Methodology
Test Case Name	**GEN03 - Usability and Accessibility**
	• ***FILL IN per Vendor*** **ATI** – Audio-Tactile Interface/Accessibility hardware: • ***FILL THIS IN per Vendor*** • *Key pad* • *Hand buttons* • *Foot pedal/rockers* • *Sip and Puff* • *Braille*
Additional – Standards Documents	HAVA 2002 Requirements
Voting: **Usability verifications**	Usability verification addresses the design of the voting system and its ability to meet the needs of the voters, that is, to ensure that the interfaces between the voter and the system are easy to use and minimize voter errors. Using both the vendor's documentation and the applicable Standards Documents as guidelines, verification is performed to ensure that the voting system meets the following requirements: **Functional Capabilities** (V1: 3.1.2) • Notification to a voter identifying the contest, issues, undervotes and overvotes.(V1: 3.1.2 a, b & e) • Notification to a voter prior casting, allowing changes to the ballot, and after the ballot has been marked (V1:3.1.2 c &d) **Alternative Languages** (V1: 3.1.3) • Allow ballot selection, review and instructions in any language required by the state. (V1: 3.1.3) • For voters who lack proficiency in reading English, or whose primary language is unwritten, provide spoken instructions and ballots in the preferred language of the voter, consistent with state and federal law (V1: 3.2.7) **Cognitive Issues** (V1: 3.1.4) • Minimize cognitive difficulties to the voter providing clear instructions/warnings and assistance. (V1: 3.1.4 a, b, c & d) • Clearly indicate maximum number of candidates for a single contest and ensure a consistent relationship between candidate name and mechanism used to vote for that candidate (V1: 3.1.4 cii, ciii) • Electronic image displays shall provide synchronized audio output to convey same information as is displayed on the screen (V1: 3.2.2.1 f) **Perceptual Issues** (V1: 3.1.5) • Adjustable aspects of voting machines, shall have a mechanism to reset to the default value or shall automatically reset to standard default value upon completion voter's session (V1: 3.1.5 b & c) • Electronic voting machines shall provide minimum font size of 3.0 (measured as the height of a capital letter) and all text intended for the voter should be

Test Detail	Test Methodology
Test Case Name	**GEN03 - Usability and Accessibility**
	presented in a sans serif font.(V1: 3.1.5 d & h) • All voting machines using paper ballots should make provisions for voters with poor reading vision (V1: 3.1.5 e) • Color coding shall not be used as the sole means of conveying information (V1: 3.1.5 g) **Interaction Issues** (V1: 3.1.6) • Voting machines with electronic image displays shall not require page scrolling (V1: 3.1.6 a) • Voting machines shall provide unambiguous feedback of voter's selections, be designed to minimize accidental activation, and no key shall have a repetitive effect as a result of being continually pressed (V1:3.1.6 b, d & dii) • If a response from the voter is required within a specific time, the voting machine will issue an alert at least 20 seconds before this time has expired (V1: 3.1.6 c) **Privacy** (V1:3.1.7) • Preclude anyone else from determining the content of a voter's ballot without the voter's cooperation. Ballot and any input controls shall only be visible to the voter, the audio interface shall only be audible to the voter, and the voting system shall notify the voter of an attempted overvote in a way that preserves the privacy of the voter (V1: 3.1.7; 3.1.7.1 a, b & c)
Voting: **Accessibility verifications**	The Standards provide requirements for voting systems to meet the accessibility needs of a broad range of voters with disabilities. The vendor must either configure all of the system's voting stations to meet the accessibility specifications or must design a unique station that conforms to the accessibility requirements and is part of the overall voting system configuration. Mimicking the voter with disabilities, testing and verification is done to ensure that the voting system meets the following requirements: **General Accessibility Requirements** (V1: 3.2.1) **Vision** (V1:3.2.2) • Accessible to voters with visual disabilities or voters with partial vision (V1: 3.2.2. 3.2.2.1) • Accessible to voters who are blind and provide an audio-tactile interface (ATI) that supports the full functionality of the visual ballot interface and allows the voter to control the rate of speech. (V1: 3.2.2.2, 3.2.2.2 b & cix) • Font size of 3.0-4.0 mm and 6.3 –9.0 mm, allow high contrast and allow adjustable color for partial vision (V1: 3.2.2.1 b, c & d) • Buttons and controls shall be distinguishable by both shape and color, all mechanically operated controls or keys shall be tactilely discernible without activating these controls and keys, and status of all locking or toggle controls or keys shall be visually discernable and also through touch and sound (V1: 3.2.2.1 e, 3.2.2.2 f &g)

Test Detail	Test Methodology
Test Case Name	GEN03 - Usability and Accessibility
	Dexterity (V1: 3.2.3) • Shall be accessible to voters who lack fine motor control or use of their hands and all controls should be operable with one hand without requiring tight grasping, pinching or twisting of the wrist. Force to activate keys or controls shall be no greater than 5 lbs. If normal procedure is for voters to submit their own ballots, the station shall provide features to these voters to enable them to perform this submission (V1: 3.2.3 a, b & e) • Controls shall not require direct bodily contact or for the body to be part of any electrical circuit (V1: 3.2.3 c) • Shall provide mechanism to enable non-manual input, equivalent to tactile input (V1: 3.2.3 d) **Mobility** (V1: 3.2.4) • Accessible to voters who use mobility aids, including wheel chairs. All controls, keys, jacks, and any other part of the voting station shall be within reach as specified, and all labels, displays, controls, keys, jacks, etc. shall be legible to a voter in a wheelchair with normal eyesight, who is in an appropriate position and orientation with respect to the voting station. (V1: 3.2.4, b & c) • Voting station shall be within the clearance, obstruction and reach limits specified (3.2.4 a, bi, bii, biii, biv, bv, & bvi) **Hearing** (V1: 3.2.5) • Voting station shall incorporate features under 3.2.2.2c to provide accessibility to voters with hearing disabilities, and if it provides sound cues to alert the voter, the tone shall be accompanied with a visual cue unless the station is in audio-only mode. (V1: 3.2.5 a & b) • Electronic image displays shall provide synchronized audio output to convey same information as is displayed on the screen (3.2.2.1 f) **Speech** (V1: 3.2.6) • Voting process shall be accessible to voters with speech disabilities. No voting equipment shall require voter speech for operation (V1: 3.2.6 & 3.2.6a) **English Proficiency** (V1:3.2.7) **Cognition** (V1: 3.2.8) To facilitate accessibility, all voting systems must meet Common Standards pertaining to Mobility, as illustrated in Figures 1-4 listed in the volume 1, section 3.2.4. The DRE standards, listed in the VVSG, are followed and used to verify each applicable voting machine. When necessary, measuring devices are used for validation. This can

Test Detail	Test Methodology
Test Case Name	

Table 14 - PRI01 (Closed Primary)

Test Detail	Test Methodology
Test Case Name	**PRI01 Closed Primary**
NOTE	*This test case is to be used in conjunction with the **Election Core definition**.*
Objective	The object of this test case is to verify core functionality and performance by using vendor manual(s) to create election ballots, vote, and tally, for an Closed Primary Election.
Variables: **Voting Variations**	The following are the items verified in this election: (V1: 2.1.7.2) • 1 precinct **Partisan contest:** • "Vote for 1" Primary Presidential Nominations List the nominees, not the delegates • "Vote for 1" race with write-ins (Secretary of State) • "Vote N of M" on Multi-member board which includes declared candidates (Alderman) • "Vote for 1" race with a single candidate and a write-in (Superintendent of Schools) • "Vote for 1" race with a single candidates and write-ins (Sheriff) • "Vote N of M" on Multi-member board which includes declared candidates with write-in voting (School Board)
Variables: **Election Variations**	**Presidential Nominee:** 3 candidates (DEM) **Presidential Nominee:** 2 candidates (REP) **Presidential Nominee:** 2 candidates (SCI) **Secretary of State:** 1 candidate (DEM) **Secretary of State:** 3 candidates (REP) **Secretary of State:** 2 candidates (SCI) **Alderman:** 3 candidates (DEM) **Alderman:** 4 candidates (REP) **Alderman:** 3 candidates (SCI) **Sheriff:** 1 candidate (DEM) **Sheriff:** 1 candidate (REP) **Sheriff:** no candidate (SCI) **Superintendent of Schools:** 1 candidate (DEM) **Superintendent of Schools:** 2 candidates (REP) **Superintendent of Schools:** 3 candidates (SCI) **School Board:** 6 candidates (DEM) **School Board:** 4 candidates (REP) **School Board:** 5 candidates (SCI)
A description of the voting system type and the operational environment	*List of all DRE, BMD and any other hardware or software that is used in the voting environment for this test case.* **Software** • ***FILL IN per Vendor*** **Hardware** • ***FILL IN per Vendor***.

Table 15 - PRI02 (Closed Primary)

Test Detail	Test Methodology
Test Case Name	**PRI02 Closed Primary**
NOTE	*This test case is to be used in conjunction with the **Election Core definition**.*
Objective	The object of this test case is to verify core functionality and performance using the vendor's manuals for a Closed Primary election.
Variables: **Voting Variations**	The following are the items verified in this election: (V1: 2.1.7.2) • 7 precincts **Partisan contests:** • "Vote for 1" Primary Presidential Delegates: a delegate slate, display of delegates with nominees • "Vote for 1" race with write-ins (Secretary of State) • "Vote N of M" on Multi-member board which includes declared candidates (Alderman) • "Vote for 1" race with a single candidate and a write-in (Superintendent of Schools) • "Vote for 1" race with a single candidates and write-ins (Sheriff) • "Vote N of M" on Multi-member board which includes declared candidates with write-in voting (School Board) • Rotation: District by Registered Voters (Rotates Alderman and School Board "by Party" based on each party's registered voters)
Variables: **Election Variations**	**Presidential Delegates:** 3 sets of candidates (DEM) **Presidential Delegates:** 2 sets of candidates (REP) **Presidential Delegates:** 2 sets of candidates (SCI) **Secretary of State:** 1 declared candidate/1 write-in (DEM) **Secretary of State:** 3 candidates (REP) **Secretary of State:** 2 candidates (SCI) **Alderman:** 2 candidates (DEM) **Alderman:** 4 candidates (REP) **Alderman:** 3 candidates (SCI) **Sheriff:** 1 candidate (DEM) **Sheriff:** 1 candidate (REP) **Sheriff:** no candidate (SCI) **Superintendent of Schools:** 1 candidate (DEM) **Superintendent of Schools:** 2 candidates (REP) **Superintendent of Schools:** 3 candidates (SCI) **School Board:** 6 candidates (DEM) **School Board:** 4 candidates (REP) **School Board:** 5 candidates (SCI)

Test Detail	Test Methodology
Test Case Name	**PRI02 Closed Primary**
A description of the voting system type and the operational environment	*List of all DRE, BMD and any other hardware or software that is used in the voting environment for this test case.* **Software** • ***FILL IN per Vendor*** **Hardware** • ***FILL IN per Vendor***

Table 16 – Readiness Test

Test Detail	Test Methodology
Test Case Name	**Readiness Test**
Scope	A functional test that uses The 2005 Voluntary Voting System Guidelines (VVSG) to validate Readiness throughout the entire voting system. (V1: 2.2.4)
Objective	The object of this test case is to verify equipment and system readiness to ensure that the voting system functions properly, to confirm that the system equipment has been properly intergraded, and to obtain equipment status reports. (V1: 2.2.4)
Standards Documents	Voluntary Voting system guidelines 2005, vol. 1 Voluntary Voting system guidelines 2005, vol. 2 Specific standards are noted in following steps.
A listing of the applicable voting system machines	*List of all DRE, BMD and any other hardware or software that is used in the voting environment for this test case.* **Software** • ***FILL IN per Vendor*** **Hardware** • ***FILL IN per Vendor*** Refer to the following tables for complete descriptions: ➢ Matrix of Required Software/Firmware ➢ Matrix of Required Hardware
Pre-requisites and initialization of the test case	This testing is to be executed on initial testing and each time the system is to be shut down and restarted.
Documentation of Test Data & Test Results	For each iteration that the election is run: • Capture all voting steps in order to maintain repeatability of the test • Record election, ballot, and vote data fields on the corresponding worksheet tabs • Save all worksheet tabs for all iterations of the test case • Record results of test run by entering 'Accept/Reject' on the Test Results Matrix • Provide comments when observing deviations, discrepancies or notable observations • Log discrepancies on the Discrepancy Report
System Preparation - Security	System Preparation - Security: • System username/password authentication and other access controls are set up according to system documentation guidelines for all devices being tested. • Any/all unnecessary processes are disabled and/or required process control measures noted in the documentation are followed. • All COTS and vendor subsystems used for system security are configured and active as recommended by the system documentation. This includes all connection, port, virus, and data or authorized process restriction systems. • Any other pre-election system security measures listed in the documentation are followed including setup of additional hardware or software not covered above.

Test Detail	Test Methodology
Test Case Name	**Readiness Test**
	Please also see the Documentation section of the Security Test Case within Appendix A.
READINESS TESTING VERIFICATION	Verification of Voting machines or vote recording and data processing equipment, precinct count equipment, and central count equipment are properly configured for an election, and collect data that verifies equipment readiness. This includes: • Obtain status and data reports from each set of equipment • Correct installation and interface of all system equipment • Hardware and software function correctly • Version verification
Summary of Instructions followed per Product	The following list of documentation is used to perform system readiness: • ***FILL IN per Vendor***
Readiness Audit	Produce and verify available system reports
Results are Observed	Review the outcome of the test(s) against the expected result(s): • **Accept**: expected results is observed • **Reject:** expected result is NOT observed • **Not Testable (NT)**: rejection of a previous test step prevents validation of this step or this was tested in another test case • **Not Applicable (NA):** not applicable to the current test scope or to the component under review • **Not Supported (NS)**: not supported in the current test scope
Record Observations and all input/outputs for each election	All information used in processing the test case is captured. This includes: inputs, outputs, deviations and any other item that may impact the validation of the test case. Any failure of the test against the EAC guidelines is reported and implies failure of the system. Failures are reported as Defect Issues in the Discrepancy Report and are provided to the manufacturer. Before the final Certification Test Report is issued, manufacturers are given the opportunity to correct all discrepancies. If the manufacturer submits corrections, retests are performed. Issues that do not impact the failure of the requirements but could be considered defects are logged as Informational Issues on the Discrepancy Report. It is the manufacturer's option to address these issues.

Table 17 – Operational Status Test

Test Detail	Test Methodology
Test Case Name	**Operational Status Check**
Scope	SysTest Labs requires the vendor to provide a comprehensive end-to-end test case(s) that they supply to their customers, such as state election officials. The Vendor may provide SysTest Labs a comprehensive checklist of test case(s) for particular states' functionality. This test may be based on the vendor's certification configuration. SysTest Labs will perform the operational status check once upon acceptance of the equipment, and once after all other testing, prior to checkout. (V2: 4.6.1.5)
Objective	The object of this test case is to verify that when all tests, inspections, repairs, and adjustments have been completed, normal operation can be verified by conducting an operational status check.
Standards Documents	Voluntary Voting system guidelines 2005, vol. 1 Voluntary Voting system guidelines 2005, vol. 2 Specific standards are noted in following steps.
A listing of the applicable voting system machines	*List of all DRE, BMD and any other hardware or software that is used in the voting environment for this test case.* **Software** • ***FILL IN per Vendor*** **Hardware** • ***FILL IN per Vendor*** Refer to the following tables for complete descriptions: ➢ Matrix of Required Software/Firmware ➢ Matrix of Required Hardware
Documentation of Test Data & Test Results	For each iteration that the election is run: • Capture all voting steps in order to maintain repeatability of the test • Record election, ballot, and vote data fields on the corresponding worksheet tabs • Save all worksheet tabs for all iterations of the test case • Record results of test run by entering 'Accept/Reject' on the Test Results Matrix • Provide comments when observing deviations, discrepancies or notable observations • Log discrepancies on the Discrepancy Report
Operational Status Check Verification	During this process, all equipment will be operated in a manner and environmental conditions that simulate election use to verify the functional status of the system. Prior to the conduct of each of the environmental hardware non-operating tests, a supplemental test will be made to determine that the operational state of the equipment is within acceptable performance limits. The following procedures will be followed to verify the equipment status: • Step 1: Arrange the system for normal operation. • Step 2: Turn on power, and allow the system to reach recommended operating temperature. • Step 3: Perform any servicing, and make any adjustments necessary, to achieve operational status. • Step 4: Operate the equipment in all modes, demonstrating all functions and features that would be used during election operations. • Step 5: Verify that all system functions have been correctly executed.

Test Detail	Test Methodology
Test Case Name	**Operational Status Check**
Readiness Audit	Produce and verify available system reports
Results are Observed	Review the outcome of the test(s) against the expected result(s): • **Accept**: expected results is observed • **Reject:** expected result is NOT observed • **Not Testable (NT)**: rejection of a previous test step prevents validation of this step or this was tested in another test case • **Not Applicable (NA):** not applicable to the current test scope or to the component under review • **Not Supported (NS)**: not supported in the current test scope
Record Observations and all input/outputs for each election	All information used in processing the test case is captured. This includes: inputs, outputs, deviations and any other item that may impact the validation of the test case. Any failure of the test against the EAC guidelines is reported and implies failure of the system. Failures are reported as Defect Issues in the Discrepancy Report and are provided to the manufacturer. Before the final Certification Test Report is issued, manufacturers are given the opportunity to correct all discrepancies. If the manufacturer submits corrections, retests are performed. Issues that do not impact the failure of the requirements but could be considered defects are logged as Informational Issues on the Discrepancy Report. It is the manufacturer's option to address these issues.

Table 18 – Volume and Stress Test

<table>
<tr><th>Test Detail</th><th>Test Methodology</th></tr>
<tr><td>Test Case Name</td><td>Volume and Stress</td></tr>
<tr><td>NOTE</td><td>This test case is to be used in conjunction with the Election Core definition.</td></tr>
<tr><td>Scope</td><td>A functional test that uses The 2005 Voluntary Voting System Guidelines (VVSG) to validate the system's response to a range of both normal and abnormal conditions initiated in an attempt to compromise the system. (V2:6.1)</td></tr>
<tr><td>Objective</td><td>The objective of this test case is to evaluate the voting system's responses to processing volume and stress.</td></tr>
<tr><td>Variables:
Voting Variations</td><td>Please refer to “Calculation of Ballots to be processed” below.</td></tr>
<tr><td>Variables:
Election Variations</td><td>Please refer to “Calculation of Ballots to be processed” below.</td></tr>
<tr><td>A description of the voting system type and the operational environment</td><td>List of all DRE, BMD and any other hardware or software that is used in the voting environment for this test case.

Software

• FILL IN per Vendor

Hardware

• FILL IN per Vendor</td></tr>
<tr><td>Calculation of Ballots to be processed</td><td>For all systems, the total number of ballots to be processed by each precinct counting device during these tests reflect the maximum number of active voting positions and the maximum number of ballot styles that the TDP claims the system can support. (V2:6.2.3)

(Contests and Candidates are Individualized per vendor)
<table>
<tr><th>Voter</th><th>Con1</th><th>Con2</th><th>Con3</th><th>…</th><th>…</th><th>…</th><th>ConX</th></tr>
<tr><td>1</td><td>Can1</td><td>Can1</td><td>Can1</td><td>Can1</td><td>Can1</td><td>Can1</td><td>Can1</td></tr>
<tr><td>2</td><td>Can2</td><td>Can2</td><td>Can2</td><td>Can2</td><td>Can2</td><td>Can2</td><td>Can2</td></tr>
<tr><td>3</td><td>Can3</td><td>Can3</td><td>Can3</td><td>Can3</td><td>Can3</td><td>Can3</td><td>Can3</td></tr>
<tr><td>4</td><td>Can4</td><td>Can4</td><td>Can4</td><td>Can4</td><td>Can4</td><td>Can4</td><td>Can4</td></tr>
<tr><td>5</td><td>Can5</td><td>Can5</td><td>Can5</td><td>Can5</td><td>Can5</td><td>Can5</td><td>Can5</td></tr>
<tr><td>6</td><td>Can6</td><td>Can6</td><td>Can6</td><td>Can6</td><td>Can6</td><td>Can6</td><td>Can6</td></tr>
<tr><td>…</td><td>…</td><td>…</td><td>…</td><td>…</td><td>…</td><td>…</td><td>…</td></tr>
<tr><td>X</td><td>CanX</td><td>CanX</td><td>CanX</td><td>CanX</td><td>CanX</td><td>CanX</td><td>CanX</td></tr>
</table></td></tr>
<tr><td>Voting: Additional - Opening the Polls Verification</td><td>Verify that all potential ballot positions are active and able to be voted (V1: 2.2.4.i)</td></tr>
</table>

Test Detail	Test Methodology
Test Case Name	**Volume and Stress**
Voting: **Stress and Volume Verifications**	Verification is performed to ensure that the voting system is able to process and appropriately handle the following: **Volume testing (**V2:A.4.3.5) • More than the expected number of ballots/voters per precinct • More than the expected number of precincts • Any other similar conditions that tend to overload the system's capacity to process, store, and report data Additionally, evaluation is performed to verify that the voting system is able to process and appropriately respond the following: **Stress testing (**V2:A.4.3.5) • Transient overload conditions • Ballot processing at the high volume rates • Software response to hardware-generated interrupts and wait states • *When applicable, Central counting systems can be subjected to similar overloads, including, for systems that support more than one card reader, continuous processing through all readers simultaneously*

Table 19 – Accuracy Test

Test Detail Test Case Name	Test Methodology Accuracy
NOTE	*This test case is to be used in conjunction with the **Election Core definition**.*
Scope	A functional test that uses The 2005 Voluntary Voting System Guidelines (VVSG) to validate the individual ballot positions in terms of a maximum error rate while processing a specified volume of data. (V2:4.7.1.1)
Objective	The object of this test is to verify that the voting system can accurately and reliably print ballots incorporating a minimum 1,549,703 ballot positions (including voted and non-voted positions) and that these ballots can be mechanically/electronically tabulated without error.
Variables: **Voting Variations**	*Please refer to "Calculation of Ballots to be processed" below.*
Variables: **Election Variations**	*Please refer to "Calculation of Ballots to be processed" below.*
A description of the voting system type and the operational environment	List of all DRE, BMD and any other hardware or software that is used in the voting environment for this test case. **Software** • ***FILL IN per Vendor*** **Hardware** • ***FILL IN per Vendor***

Calculation of Ballots to be processed	***(Individualized per vendor)***
	
	Terminals:
	• *Type: # of machines*
	
	Ballot Description:
	• *Type of ballot*
	  • # Contests x # Candidates = # ballot positions
	  • *Type of vote pattern used*
	  • *# Ballots per batch x #* ballot positions = *# total ballot positions per batch*
	  • *# Batches per machine x # total ballot positions per batch = total ballot positions per machine*
	  • *# Machines x total ballot positions per machine = grand total ballot positions*
	  • *Grand total ballot positions* >= 1549,703 (required ballot positions)

Voting: **Additional - Opening the Polls Verification**	Verify that all potential ballot positions are active and able to be voted (V1: 2.2.4.i)

Test Detail Test Case Name	Test Methodology Accuracy
Accuracy: **Error Rate**	Voting system accuracy addresses the accuracy of data for each of the individual ballot positions that could be selected by a voter, including the positions that are not selected. For a voting system, accuracy is defined as the ability of the system to capture, record, store, consolidate and report the specific selections and absence of selections, made by the voter for each ballot position without error. Required accuracy is defined in terms of an error rate that for testing purposes represents the maximum number of errors allowed while processing a specified volume of data. (V1:4.1.1) For all systems, the total number of ballots to be processed by each precinct counting device during these tests reflects the maximum number of active voting positions and the maximum number of ballot styles that the vendor's TDP claims the system can support. (V2:6.2.3, V1:4.1.6.1.a.i) The error rate determines the accuracy test vote position processing volume: • Reject: one error before counting 26,997 consecutive ballot positions correctly • Accept: 1,549,703 (or more) consecutive ballot positions are read correctly • If there is one error with more than 26,997 ballot positions but less than 1,549,703 correctly read, continue until another 1,576,701 consecutive ballot positions are counted without error (i.e. Accept: 3,126,404 with one error) The Ballot Reading Accuracy for paper-based system requirement governs the conversion of the physical ballot into electronic data. Reading accuracy for ballot conversion refers to the ability to: • Recognize vote punches or marks, or the absence thereof, for each possible selection on the ballot • Discriminate between valid punches or marks and extraneous perforations, smudges, and folds • Convert the vote punches or marks, or the absence thereof, for each possible selection on the ballot into digital signals. Verification of paper-based systems ensures that the system: (V1:4.1.5.2) • Detects punches or marks that conform to vendor specifications with an error rate not exceeding the requirement indicated in Section 4.1.1 • Rejects ballots that meet all vendor specifications at a rate not to exceed 2 percent

Table 20 – Security - General

Test Detail	Test Methodology
Test Case Name	**Security – General**
Scope	Security Testing Overview Security testing is related to four activities: **Documentation Review** - Documentation Review verifies that the system has documented policies and procedures that mitigate or eliminate security threats outlined in the VSS guidelines. It also describes Access controls. **Source Code Review** - Source Code Review insures source code meets VSS guidelines and provides additional protection against security flaws into the system. Potential security issues may include default passwords or backdoors in the source code, encryption keys in the source code, encryption flaws, unencrypted data transmissions, encryption algorithms that are not NIST certified, etc. **Hardware Testing** - Hardware Testing insures that equipment will stand up to environment conditions, machines are accurate, physical access to machine components is restricted, machine hardware is reliable and attempts to compromise machine security is detectable. A hardware malfunction could impact the accuracy of voting data or provide unauthorized access to secure information. Specific hardware limitations or restrictions impact the test procedures needed to validate security of the system. **System Testing** - System Testing verifies that voting systems have sufficient system and data protection mechanisms that when combined with other review processes, provide a secure voting environment. This section of the document relates to System Testing but depends on the other three activities that are covered in their own specific section.
Objective	Security testing attempts to identify flaws in voting systems where undesired or unauthorized human or machine activity may compromise an election through system failure, data manipulation, data interception or other means. Prevent and/or detect undesired system activities including: • Unauthorized access through accidental or intentional bypass or circumvention of authorization controls. • Alteration, deletion, replacement or theft of voter, election, audit and/or vote data. • Hardware and/or software tampering • Interruption of voting activities
Standards Documents	Voluntary Voting system guidelines 2005, vol. 1 Voluntary Voting system guidelines 2005, vol. 2 Specific standards are noted in following steps.
A listing of the applicable voting system machines	*List of all DRE, BMD and any other hardware or software that is used in the voting environment for this test case.* **Software** • ***FILL IN per Vendor*** **Hardware** • ***FILL IN per Vendor*** Refer to the following tables for complete descriptions: ➢ Matrix of Required Software/Firmware ➢ Matrix of Required Hardware

Comment [rz54]: This test case appears to be yet another listing of what will be tested. The test case should describe how a requirement will be tested. The matrix already covers what will be tested.

Comment [rz55]: Missing NYS requirements.

Test Detail	Test Methodology
Test Case Name	**Security – General**
Security Test Sub Type	**Description**
Role	SysTest Labs will validate that the vendor has implemented adequate security policies and controls to ensure that Voting Systems meet the requirements specified in the applicable VVSG 2005 Voting Standards. Using well-defined, repeatable testing methods and inspection processes, SysTest Labs will validate that the following required policies and controls exist and are effective: **1.1** Privileges are not allowed to be: • Exceeded (V1: 7.2.1.1.c) • Changed to Run Reports **1.2** Voters are inhibited from: • Accessing Equipment Before Polls Open • Running Reports **1.3** Changes to Privileges are Prohibited for IDs and Passwords Thus Preventing Unauthorized Report Printing, Results Transmission, Results Downloading and Resetting of Elections **1.4** Voter equipment access or keys are limited to ensure: • Only the User interface is accessible • Only a single vote may be cast • Closed Polls are secure • Counts are not available to voters • Unauthorized Accounts from System Functions **1.5** Fraudulent Ballots are not accepted by the system ensuring only valid ballots are counted **1.6** The vendor permits the voter to cast a ballot expeditiously, but precludes voter access to all other aspects of the vote-counting processes. (V1: 7.2.1.1.c) **1.7** Password Required for Each System Software Component (V1: 7.5.4.c) **1.8** Password Required for Each System Data Component **1.9** Password Required for Each System Data Component **1.10** Hardware Key Required for Each System Hardware Component **1.11** Each Type of User Account Can Only Perform Intended Functions
Access	SysTest Labs will validate that the vendor has implemented adequate ACCESS controls to ensure the integrity and operational security of Voting Systems, as specified by the requirements of applicable VVSG 2005 Voting Standards. Using well defined, repeatable testing methods and inspection processes, SysTest Labs will validate that the following required ACCESS policies and controls exist and are effective:

Test Detail	Test Methodology
Test Case Name	**Security – General**
Security Test Sub Type	**Description**
	2.1 Access validation to the system ensures that only applicable system entry is allowed. This includes: • Seals and/or Password are Required to Open Polls (V1: 2.3.1.3.a, 4.1.4.2.d.ii) • Security Seal and/or Password Prevent Unauthorized Opening of Polls • Incorrect or Blank Password Cannot be Used to Open Polls (V1: 7.2.1.d) • System Provides Access Controls that Limit or Detect Access to Critical System Components (V1: 2.1.1.a, 7.2.1.d)
System Security	SysTest Labs will validate that the vendor has implemented adequate and effective system security policies and controls. Using well-defined, repeatable testing methods and inspection processes, SysTest Labs will validate that the following required policies and controls exist and are effective: **3.1** System security is achieved through a combination of technical capabilities and sound administrative practices. To ensure security, the system: (V1: 2.1.1) • Provides system functions that are executable only in the intended manner and order, and only under the intended conditions. • Uses the system's control logic to prevent a system function from executing if any preconditions to the function have not been met. • Provides safeguards to protect against tampering during system repair, or interventions in system operations, in response to system failure. • Provides security provisions that are compatible with the procedures and administrative tasks involved in equipment preparation, testing, and operation. • If access to a system function is to be restricted or controlled, the system incorporates a means of implementing this capability. • Provides documentation of mandatory administrative procedures for effective system security **3.2** The voting system may use a local or remote data network. Should such a network be used in a jurisdiction, all components of the network do comply with the telecommunications requirements described in Section 5 of the Standards and the Security requirements as described in Section 6. (V1: 4.1.2.15)
System Log	SysTest Labs will validate that the vendor's ability to capture and control system logs and log entries meet applicable requirements in the VVSG 2005 Voting Standards. Using well-defined, repeatable testing methods and inspection processes, SysTest Labs will validate that the following required logging capabilities and controls exist and are effective. Verification of System Log Activity is performed to ensure: (V1: 5.4.3) **4.1** Error Activity provided by the system is complete, applicable, and appropriate **4.2** Voting Activity is captured correctly **4.3** Log(s) have the needed protection to validate that the information is secure

Test Detail	Test Methodology
Test Case Name	**Security – General**
Security Test Sub Type	**Description**
Software Security	SysTest Labs will validate that specific software/firmware security measures are in place, adequate, and effective. Using well-defined, repeatable testing methods and inspection processes, SysTest Labs will validate that the following required logging capabilities and controls exist and are effective: **5.1** Software security validation ensures that the firmware has been shown to be inaccessible to activation or control (V1: 7.4.1.c) **5.2** Verify the Separation of Election Specific Firmware and Operating System are stored (V1: 7.4.1.d)
Data Integrity	SysTest Labs will validate that the capabilities of the Voting System to manage and maintain data integrity in components and across the entire Voting System through the stages of the election process meet the applicable requirements in the VVSG 2005 Voting Standards. Using well-defined, repeatable testing methods and inspection processes, SysTest Labs will validate that the following required data integrity management and maintenance capabilities and controls exist and are effective: **6.1** The system meets the following requirements for installation of software, including hardware with imbedded firmware: (V1: 7.4.1) • The system bootstrap, monitor, and device-controller software may be resident permanently as firmware, 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 • The election-specific programming is installed and resident as firmware, this firmware is installed on a component other than the component on which the operating system resides **6.2** Transmission of data shall ensure that receipt of valid vote records is verified at the receiving stations (V1: 7.5.1.a) **6.3** Transmission of Cast Ballots During Voting Error Detection, Recovery and Retransmission **6.4** Transmission of Cast Ballots During Voting Integrity Checks **6.5** Transmission Verification Checks **6.6** Verification that the ballot reader is prevented from reading more than one ballot at a time (multiple feed), and if detected, the card reader halts (V1: 4.1.51.e.i)
Telecom & Data Transmission	SysTest Labs will validate that the capabilities of the voting system to manage and maintain secure telecommunications and data transmissions in components and across the entire Voting System meet the applicable requirements in the VVSG 2005 Voting Standards. Using well-defined, repeatable testing methods and inspection processes, SysTest Labs will validate that the following required capabilities and controls exist and are effective: **7.1** The system transmits data over public telecommunications networks, and as such: (V1: 7.6.1) • Preserves the secrecy of a voter's ballot choices, and prevents anyone from violating ballot privacy

Comment [rz56]: NYS requirements forbid any capability to use telecommunications. This test case has to be to ensure that no such capability exists.

Test Detail	Test Methodology
Test Case Name	**Security – General**
Security Test Sub Type	**Description**
	7.2 Encrypted Transmissions (V1:7.5.1.b.i) **7.3** Encryption Specification Verification **7.4** Session Hijacking **7.5** Monitoring and Responding to External Threats (V1: 7.5.3) **7.6** Shared Operating Environment (V1: 7.5.4) **7.7** Security for Transmissions (V1: 7.6) **7.8** Unauthorized Tool **7.9** Virus **7.10** Threat Reception and Storage Prevention (V1: 7.5.2) **7.11** Remote Access Disabled **7.12** User Account Restriction From Remote Access Settings **7.13** Routers and/or Firewalls
Threat Protection	SysTest Labs will validate that the capabilities of the Voting System to protect against computer security threats meet the applicable requirements in the VVSG 2005 Voting Standards. Using well-defined, repeatable testing methods and inspection processes, SysTest Labs will validate that the following required computer threat protection capabilities, security policies, and controls exist and are effective: **8.1** Memory Threat & Virus Scanning Mechanisms (V1: 7.5.2c) **8.2** Rootkit Scanning Mechanisms
Audit Log	SysTest Labs will validate that the Voting System meets VVSG 2005 Voting Standards to securely manage and maintain audit logs in all components and across the entire Voting System. Using well-defined, repeatable testing methods and inspection processes, SysTest Labs will validate that the following required audit logging capabilities and controls exist and are effective: **9.1** Audit logs and data files cannot be altered through the use of an alternate boot sequence without detection, and the test will consist of attempting to boot the devices using alternative media during boot sequences. **9.2** Audit logs and data files cannot be altered through the use of editing tools without detection. **9.3** The test will consist of attempting to edit the audit log to confirm that the system either: • Does not allow edits of the audit log or data files, or • Detects and reports all attempts at editing the audit log or data files
Data Protection	SysTest Labs will validate that the Voting System meets VVSG 2005 Voting Standards to securely protect data used and stored in components and across the entire Voting

Test Detail	Test Methodology
Test Case Name	**Security – General**
Security Test Sub Type	**Description**
	System. Using well-defined, repeatable testing methods and inspection processes, SysTest Labs will validate that the following required data protection policies, capabilities, and controls exist and are effective: **10.1** Logical Isolation of Voting System Software & Data (V1: 7.5.4.b) **10.2** Access Control Lists Preclude Data Leakage (V1: 7.5.4.d) **10.3** Routers and Firewalls Preclude Data Leakage **10.4** Electronic Policies Prevent Copy of Data **10.5** Voting System Access to Incomplete Election Returns (V1: 7.5.5)
Documentation	Vendor documentation is reviewed and evaluated to verify that it speaks to required VVSG security concerns with regard to various aspects of a voting system. If determined that an appropriate amount of information is supplied such that the requirements are adequately met, at a minimum, the requirement is passed. If it is determined that not enough information is supplied to adequately meet the requirement, the requirement is judged to have been failed. The following standards are used to ensure that: **11.1** Although the jurisdiction in which the voting system is operated is responsible for determining the access policies applying to each election, the vendor provides a description of recommended policies for: (V1: 7.2.1) • Software access controls documentation • Hardware access controls documentation • Communications documentation • Effective password management documentation • Protection abilities of a particular operating system documentation • General characteristics of supervisory access privileges documentation • Segregation of Duties documentation • Any additional relevant characteristics **11.2** The voting system vendor: (V1: 7.2.1.1) • Identifies each person, to whom access is granted, and the specific functions and data to which each person holds authorized access. • Specifies whether an individual's authorization is limited to a specific time, time interval, or phase of the voting our counting operation **11.3** The vendor provides a detailed description of all system access control measures designed to permit authorized access to the system and prevent unauthorized access, as covered in the following areas: (V1: 7.2.1.2) • Use of data and user authorization • Program unit ownership and other regional boundaries

Test Detail	Test Methodology
Test Case Name	**Security – General**
Security Test Sub Type	**Description**
	• One-end or two-end port protection devices • Security kernels • Computer-generated password keys • Special protocols • Message encryption • Controlled access security **11.4** The vendor defines and provides a detailed description of the methods used to prevent unauthorized access to the access control capabilities of the system itself. (V1: 7.2.1.2) **11.5** The vendor develops and provides detailed documentation, pertaining to polling place security operations, of measures to anticipate and counteract vandalism, civil disobedience, and similar occurrences of. The measures: (V1: 7.3.1) • Allow the immediate detection of tampering with vote casting devices and precinct ballot counters • Control physical access to a telecommunications link if such a link is used **11.6** The Vendor develops and documents, in detail, the measures to be taken in a central counting environment. These measures include physical and procedural controls related to the: (V1: 7.3.2) • Handling of ballot boxes • Preparing of ballots for counting • Counting operations • Reporting data **11.7** The system meets the following requirements for installation of software, including hardware with embedded firmware: (V1: 7.4.1) • If software is resident in the system as firmware, the vendor requires and states in the system documentation that every device is to be retested to validate each ROM prior to the start of elections operations • To prevent alteration of executable code, no software is permanently installed or 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 • After initiation of election day testing, no source code or compilers or assemblers are resident or accessible **11.8** The voting system deploys protection against the many forms of threats to which it may be exposed such as file and macro viruses, worms, Trojan horses, and logic bombs. The vendor has developed and documented the procedures to be followed to ensure that such protection is maintained in a current status. (V1: 7.4.2) **11.9** The voting system uses telecommunications to communicate between system components and locations, and is subject to the same security requirements governing access to any other system hardware, software, and data function. (V1: 7.5.1)

Test Detail	Test Methodology
Test Case Name	**Security – General**
Security Test Sub Type	**Description**
	11.10 The voting system uses, for data integrity, electrical or optical transmission of data and, as such, ensures the receipt of valid vote records is verified at the receiving station. This includes standard transmission error detection and correction methods such as checksums and/or message digest hashes. Verification of correct transmission occurs at the voting system application level and ensures 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. (V1: 7.5.1.a) **11.11** The voting system, using telecommunications as defined in Section 5 to communicate between system components and locations before the poll site is officially closed does the following: (V1: 7.5.1.b) • The vendor implements an encryption standard currently documented and validated for use by an agency of the U.S. Federal Government • Provides a means to detect the presence of an intrusive process, such as an Intrusion Detection System **11.12** The voting system uses public telecommunications networks and implements protections against external threats to which commercial products used in the system may be susceptible. (V1: 7.5.2.a) **11.13** The voting system uses public telecommunications networks and therefore provides 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. Such documentation identifies the name, vendor, and version used for each such component. (V1: 7.5.2.b) • Operating systems • Communications routers • Modem drivers • Dial-up networking software **11.14** The voting system uses public telecommunications networks and uses protective software at the receiving-end of all communication paths to: (V1: 7.5.2.c) • Detect the presence of a threat in a transmission • Remove the threat from infected files/data • Prevent against storage of the threat anywhere on the receiving device • Provide the capability to confirm that no threats are stored in system memory and in connected storage media • Provide data to the system audit log indicating the detection of a threat and the processing performed **11.15** The vendor uses multiple forms of protective software, as needed, to provide capabilities for the full range of products used by the voting system. (V1: 7.5.2.d) **11.16** The vendor documents how they plan to monitor and respond to known threats to which the voting system is vulnerable. This documentation provides a detailed description, including scheduling information of the procedures the vendor uses to: (V1: 7.5.3) • Monitor threats, such as through the review of assessments, advisories, and alerts for COTS components issued by the Computer Emergency Response Team (CERT), the National Infrastructure Protection Center (NIPC), and the

Test Detail	Test Methodology
Test Case Name	**Security – General**
Security Test Sub Type	**Description**
	Federal Computer Incident Response Capability (FedCIRC) • Evaluate the threats and, if any, proposed responses • Develop responsive updates to the system and/or corrective procedures • 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 • After implementation of the proposed response is approved by the state, to assist clients, either directly or through detailed written procedures, how to update their systems and/or to implement the corrective procedures no later than one month before an election • Address threats emerging too late to correct the system at least one month before the election, including • Provide prompt, emergency notification to the ITA and the affected states and user jurisdictions • Assist client jurisdictions directly, or advising them through detailed written procedures, to disable the public telecommunications mode of the system • After the election, modify the system to address the threat; submitting the modified system to an ITA and appropriate state certification authority for approval, and assisting client jurisdictions directly, or advising them through detailed written procedure, to update their systems and/or to implement the corrective procedures after approval **11.17** For shared operating environments, ballot recording and vote counting can be performed in either a dedicated or non-dedicated environment. For ballot recording and vote counting operations performed in an environment that is shared with other data processing functions, both hardware and software features are present to protect the integrity of vote counting and of vote data. The system uses a shared operating environment such that it: (V1: 7.5.4) • Uses security procedures and logging records to control access to system functions • Partitions or compartmentalizes voting system functions from other concurrent functions at least logically, and preferably physically as well • Controls system access by means of passwords, and restriction of account access to necessary functions only; • Has capabilities in place to control the flow of information, precluding data leakage through shared system resources **11.18** The voting system provides access to incomplete election returns and interactive inquiries before the completion of the official count, so that the system: (V1: 7.5.5) • Is designed to provide external access to incomplete election returns 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 • Uses voting system software and its security environment is designed such that

Test Detail	Test Methodology
Test Case Name	**Security – General**
Security Test Sub Type	**Description**
	data, which is accessible to interactive queries, resides in an external file, or database, that is created and maintained by the election software under the restrictions applying to any other output report, namely, that: o The output file or database has no provision for write-access back to the system o 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 **11.19** The system transmits data over public telecommunications networks such that: (V1: 7.6.1) • Digital signatures are employed for all communications between the vote server and other devices that communicate with the server over the network • At least two authorized election officials are required to activate any critical operation regarding the processing of ballots transmitted over a public communications network, i.e. the passwords or cryptographic keys of at least two employees are required to perform processing of votes
External Access	SysTest Labs will validate that the Voting System meets applicable VVSG 2005 Voting Standards to prohibit or limit access to partial or early election returns from unauthorized persons or processes. Using well-defined, repeatable testing methods and inspection processes, SysTest Labs will validate that capabilities, controls, and policies exist that are effective to limit external access to incomplete or early election returns from unauthorized persons or processes: **12.1** Blocked Central Count Environment Access to Incomplete Election Returns (V1: 7.5.5.a)

Table 21 - Security - Source Code Review

Comment [rz57]: All this test case is really saying is that Fortify will be used. The test case should be much more comprehensive so that all source code reviewers have a common template/work plan to follow when reviewing code initially and throughout the functional testing.

Test Detail	Test Methodology
Test Case Name	**Security – Source Code Review**
Scope	*A number of requirements in the VVSG, NYS Law and 6209 require that source code is reviewed from a security perspective.* *Security Source Code Review* testing is related to the following activities: • **Documentation for Source Code –** Review all vendor documentation related to source code and software development. • **Obtain and Validate Source Code** – Obtain all source code from vendor and ensure source code has not been altered. • **Security Source Code Review** – Security source Code Review insures security vulnerabilities are identified in system source code. Vulnerabilities in the source code will be evaluated and verified though tools to discover coding practices which may leave systems flawed and potentially become susceptible to attack. Potential security issues may also include default passwords, back doors in the source code, or encryption keys in the source code, encryption flaws, unencrypted data transmissions, encryption algorithms that are not NIST certified, etc.
Objective	Security Code Review testing attempts to identify flaws in voting systems software where undesired or unauthorized activity may compromise a machine or election through vulnerabilities, data manipulation, data interception or other means. Detect undesired system and software activities including: • Alteration, deletion, replacement affecting confidentiality, integrity, authenticity, or availability of system or voter data • Identification of software vulnerabilities that could affect system and software • Interruption of voting activities including system or data compromise Security Source Code Review will be performed using Fortify SCA. Vulnerabilities discovered will originate from the following: • Input Validation and Representation • API Abuse • Security Features – such as passwords management • Time and State – deadlock or insecure temp file • Errors • Code Quality • Encapsulation – such as trust boundary violations For a list of vulnerabilities identified by Fortify SCA, please see "Table 7 - Areas of Security Focused Source Code Review" of the "Master Technical Data Package Review Plan"
Standards Documents	Voluntary Voting system guidelines 2005, vol. 1 Voluntary Voting system guidelines 2005, vol. 2 Specific standards are noted in following steps. IISO/IEC 18045:2005 Information technology -- Security techniques -- Methodology for IT security evaluation ISO/IEC 15408 Information technology -- Security techniques -- Evaluation criteria for IT security
A listing of the applicable voting system machines	*List of all DRE, BMD and any other hardware or software that is used in the voting environment for this test case.* **Software**

Test Detail	Test Methodology
Test Case Name	**Security – Source Code Review**
	• ***FILL IN per Vendor*** **Hardware** • ***FILL IN per Vendor*** Refer to the following tables for complete descriptions: ➢ Matrix of Required Software/Firmware ➢ Matrix of Required Hardware
Documentation of Test Data & Test Results	Documentation for secure source code review • Assessment of vendor documentation for items that are applicable to Secure Source Code Review including TDP from vendor • Procedures may be altered due to information discovered in documentation. This may lead to alteration to test cases
Obtain and Validate Source Code	Code escrow and transfer procedures used to obtain all source code • Verification via documentation and other sources that additional source code does not exists • Check hash codes to ensure source code has not been altered
Verification of Secure Source Code Review implementation	• Secure code analysis of all source code to obtain a baseline of vulnerabilities • The source code review (based on the TDP, in addition to the source code) uses a combination of manual review and automated data collection using Fortify SCA and analysis methodologies to identify potential areas for exploitation • Manual source code review to follow identified vulnerabilities noted in code • Depending on what vulnerabilities are discovered, functional and hardware testing teams will be notified of items and additional tests will be created to cover applicable items • Standards and supporting languages noted for fortify SCA for unique code vulnerabilities *If the programming language for a particular voting system is not supported by Fortify SCA, other source code review tools will be used and supplemented with manual security source code review to ensure the same level of security source code review is performed.*

Comment [rz58]: Why aren't multiple tools used even when Fortify may support the language?

Table 22 - Security - Cryptography

Test Detail	Test Methodology
Test Case Name	**Security – Cryptography**
Scope	*A number of requirements in the VVSG, NYS Law and 6209 require various types of cryptography and that such cryptography meets specific requirements.* *Cryptography* testing is related to the following activities: • **Documentation Review** - Cryptography documentation review will be an assessment of implied use of cryptography through the vendor's descriptions within documentation of use, and verification of applied FIPS 140-2 requirements • **Cryptography Code Review** – Cryptography Code Review insures cryptographic modules adhere to FIPS 140-2. Security issues associated with Cryptography include weak and unsubstantial cryptographic means to protect information or communications affecting the confidentiality, and integrity of voter and system data.
Objective	Cryptography Code Review will perform a number of activities on cryptographic modules including identification, implementation, use, and verification of applied FIPS 140-2 requirements. Cryptographic modules and/or functions will be evaluated by the following: • Verify that vendor documentation on cryptography deployed is documented (approved FIPS 140 -2 cryptographic modules) • Cryptographic modules must meet FIPS 140-2 certified modules and must be identified as approved modules • Identify non-approved cryptographic modules • Verify implementation of cryptographic modules and validly of usage • Test VVSG, NYS regulations to applicable standards for cryptography, digital signatures, and hashing algorithms for FIPS 140-2 compliance. • Below are listed requirements that identify cryptography, digital signatures, and hashing: VVSG Vol 1: 7.4.5(a) VVSG Vol 1 7.4.5.1ai VVSG Vol 1 7.4.6d VVSG Vol 1 7.4.6di VVSG Vol 1 7.4.6dii VVSG Vol 1 7.6.1c VVSG Vol 1 7.7.1aiii VVSG Vol 1 7.7.1b VVSG Vol 1 7.7.3aii VVSG Vol 1 7.5.1a VVSG Vol 1 7.9.3a VVSG Vol 1 2.1.5.1avii VVSG Vol 1 5.1.1a NYS Regulation 6209.2.F.10a NYS Regulation 6209.2.F.12 NYS Regulation 6209.10C
Standards Documents	Voluntary Voting system guidelines 2005, vol. 1 Voluntary Voting system guidelines 2005, vol. 2 Cryptographic Module Validation Program (CMVP) FIPS 140-2 • NIST and FIPS documentation for supporting recommendations NIST SP 800-57 Recommendation for Key Management NIST SP 800-89 Recommendation for Obtaining Assurances for Digital Signature Applications NIST SP 800-106 Randomized Hashing Digital Signatures. NIST SP 800-107 Recommendation for Using Approved Hash Algorithms NIST 800-21-1 Guideline for Implementing Cryptography in the Federal Government NIST 800-56A Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography FIPS 180-3 Secure Hash Standard (SHS) FIPS 186-2 Digital Signature Standard (DSS)

Test Detail Test Case Name	Test Methodology Security – Cryptography
	FIPS 186-3 Digital Signature Standard (DSS) - Draft FIPS 198 The Keyed-Hash Message Authentication Code (HMAC)
A listing of the applicable voting system machines	*List of all DRE, BMD and any other hardware or software that is used in the voting environment for this test case.* **Software** • ***FILL IN per Vendor*** **Hardware** • ***FILL IN per Vendor*** Refer to the following tables for complete descriptions: ➢ Matrix of Required Software/Firmware ➢ Matrix of Required Hardware
Documentation of Test Data & Test Results	Cryptography documentation review will be an assessment of implied use of cryptography through the vendor's descriptions within documentation of use, and verification of applied FIPS 140-2 requirements. • Determine where in the voting system uses cryptography • Assessment of vendor documentation on cryptographic requirements exists • Verify results from PCA and FCA to identify any inconsistencies with documented cryptography • Verify that cryptography deployed is documented (approved FIPS 140 -2 cryptographic modules located on the CMPV website) • Verify that vendor documentation on cryptographic requirements exists
Cryptography Standards Validation	Cryptography Code Review attempts to identify cryptographic module implementation, use, and verification of applied FIPS 140-2 requirements. • Verify the cryptography on removable media and correspond to existing documentation • Cryptography deployed is documented(approved FIPS 140 -2 cryptographic modules) • Cryptographic modules meet FIPS 140-2 certified modules and are identified as approved modules • Identify non-approved cryptographic modules identified and reported
Verification of Cryptography implementation	Assess cryptography modules are verified as valid, implemented, and working to the vendors specification, • Verify implementation of cryptographic modules and validly of usage • Reference FIPS 140-2 certification and ensure that all provisions of the associated security policy have been implemented properly by the system vendor • Check to ensure that cryptography is enabled by viewing data that has been encrypted

Table 23 - Security - Intrusive Security Testing

Test Detail	Test Methodology
Test Case Name	**Security – Intrusive Security Testing**
Scope	*A number of requirements in the VVSG, NYS Law and 6209 require that intrusive security testing be completed. This testing requires involvement from many different groups.* *Intrusive Security Testing* is related to the following activities: • **Documentation of Security Controls** – Review all vendor documentation related to hardware security, software security, firmware security, other security controls, and compensating controls. • **Hardware Security Testing –** Intrusive security testing of the hardware to attempt to gain unauthorized access. • **Software Security Testing –** Intrusive security testing of the operating system, voting application, COTS, and all other applications and software to attempt to gain unauthorized access. • **Functional Security Testing –** Intrusive security testing before, during and after an election to attempt to gain unauthorized access at any point on the voting process.
Objective	Intrusive security testing is an attempt to break the security of the voting system or gain unauthorized access to the voting system. Intrusive security testing can include many domains of information security including but not limited to: • Vulnerability testing • Penetration testing • Black box testing • White box testing • Security Assessments • Automated testing • Manual testing Intrusive security testing involves the uses of trained information security professionals with the experience and expertise to perform security testing in a programmatic manner in order to bypass security controls on the system. These individuals must have: • An intimate working knowledge of each individual voting system • General domain expertise in the area of security • Experience with a wide variety of security testing tools • The ability to leverage publically available information about weaknesses in voting systems, operating systems, applications, etc. to try to bypass security controls on the system. This testing will be performed as a separate task from other testing activities because these testing activities may result in the voting system entering non-functioning or unknown state.
Documentation of Security Controls	Review all documentation related to security controls on the voting machine including, but not limited to, hardware controls, software controls, and controls in place during setup, preparation, conducting an election, or after the completion of an election.
Hardware Security Testing	Perform hardware security testing in an attempt to gain unauthorized access. This should include testing of all input and output components, physical controls and levers, security seals, etc.
Software Security Testing	Perform software security testing in an attempt to gain unauthorized access. This should include a review of the results from the security source code review to better understand security weaknesses in the code. It should also include manual and automated testing of application and OS components.

Comment [rz59]: This is a excellent test case. SysTest must map it to the appropriate requirements in the Matrix.

It may be important to state some parameters and more detail on how this test should be conducted such that the same approach and effort level is applied to each machine. An excellent reference document is: http://vote.nist.gov/meeting-08172007/OEVT.pdf

It would seem that this test case can be done in parallel with other test cases and perhaps by different staff. How to execute this test case should be discussed with NYSBOE.

Test Detail	Test Methodology
Test Case Name	**Security – Intrusive Security Testing**
Functional Security Testing	Perform functional security testing in an attempt to gain unauthorized access. This should include conducting an election and trying to gain unauthorized access at any point during the election process.

Table 24 - Telecommunications

Test Detail Test Case Name	Test Methodology Telecommunications
Scope	A functional test that uses the 2005 Voluntary Voting System Guidelines (VVSG) to validate required functionality. Testing includes Telecommunications capability of the vendor's voting system. During the FCA and PCA, all communication components of the Voting System are identified. Telecom and related Security tests are necessary for each component (DATA UNIT or DU) participating in a data interchange. Each DU (scanner, tabulator, DRE, PC) with the supported mediums of data exchange and roles of SENDER and RECEIVER creates a baseline to establish the initial scope of the required Telecommunications and Security conformance tests. The type of data and physical communication link technology employed by a DU (Serial, Dial-up, Lan, Wan, Wifi, GPRS) will necessitate a test case and will influence the overall scope of the testing, laboratory environment preparation, and required hardware and software testing toolsets.
Objective	The object of this test case is to verify that the physical, technical, and procedural (documentation) controls correspond correctly for Telecommunication features.
Standards Documents	Voluntary Voting system guidelines 2005, vol. 1 Voluntary Voting system guidelines 2005, vol. 2 Specific standards are noted in following steps.
A description of the voting system type and the operational environment	List and describe, per vender, all specific components involved in the storage, transfer and validation of election results after the polls are closed.
Test Classifications	Voting System telecommunications capabilities and associated components identified by the FCA and PCA are assigned to a predefined baseline test class, or a specialized class is created for any unique functionality or technology employed. Due to user configurable system options present in Voting Systems, each DU test component may have relevance in one or more phases of the System Level testing processes. **Telecommunication Test Case Classifications:**

Test Id	Test Class	Telecommunication Test Class Description
	Setup	
1	base test	Configure and validate basic device communication functionality, usability
	Pre Election	
2	no com	PC Election / Ballot to Device using media
3	direct com	PC Election / Ballot to Device using Serial, Parallel, USB ports
4	Land line modem	PC Election / Ballot to Device using Dialup public telephone network
5	Lan	PC Election / Ballot to Device using LAN
6	Wan	PC Election / Ballot to Device using WAN
7	RF Lan	PC Election / Ballot to Device data using wireless private LAN
8	RF Wan	PC Election / Ballot to Device using public / global wireless WAN
	Post Election	
101	no com	Device poll results using device media to PC with media readers

Comment [rz60]: This test case makes no sense for NYS as NYS law requires that no network capability exists on voting systems. The entire test case should be re-written focus on testing that the capability does not exist.

Comment [NPE61]: This test case focuses and making sure that all external communications are effective and controlled however, NYS requirement is that it NOT have any external communications.

In other words, this test case should focus on ensuring that there is no communications capabilities.

Comment [rz62]: NYS requirements are missing

Test Detail Test Case Name	Test Methodology Telecommunications

102	direct connect	Device poll results using direct cable connect to PC com ports
201	Public land line 1	Device transmit results to PC
202	Public land line 2	PC transmit consolidated device results to PC
301	Private Lan 1	Device results to PC
302	Private Lan 2	PC consolidated device results to PC
303	Private Wan 1	Device results to PC on private WAN
304	Public Wan 1	Device results to PC using public WAN / Internet
401	Private RF Lan 1	Device results to PC using private LAN (&/or WAN)
402	Public RF Lan 1	Device results to PC using Wireless Internet

Telecommunications and Security tests include coverage of the Voting System software components and the respective functionality paths for exception conditions prescribed by the EAC standards. A standard set of exception and security tests are included with the base communications test cases.

Detail steps are added to the System Level tests to address particular software and device features and functions, and to facilitate execution of the tests. These exception tests involve the inspection of the data in transit, modification of in-transit data, and interruption of a transmission in progress, and combinations of invalid senders, receivers and malicious software introduction.

The standard baseline tests for operation, exception handling and security are detailed in the table below.

Operational, Exception Handling and Security Test Case Classifications:

Test Id	Test Class	Telecommunication Test Class Description
	Operational Test	
.1a	Manual	Manual initiate transfer - Valid Receiver
.1b	Auto	Auto initiate transfer - Valid Receiver
	Negative Test	
.2a	Invalid	Initiate transfer - Invalid Receiver
.2b	No receiver	Initiate transfer - No Receiver
.2c	Cancel	Initiate transfer - Cancel Session
.2d	Interrupt	Initiate transfer - Interrupt Session
.2z	Resume	Resume transfer
	Security Test	
.3a	Intrude	Threat / Intrusion Detection
.3b	Remove	Threat Removal
.3c	Store	Threat Storage Prevention
.3d	Log	Log entries - threats or intrusions detected and resulting actions
.3e	Signed	Digital signature, encryption
.3f	Authorize	Dual authorization / cryptographic keys employed

Pre-requisites and initialization of the test case The Setup and Pre Election phases of testing may determine a Data Unit's communications behavior; thereby requiring instances of repeatable test steps in separate

Test Detail Test Case Name	Test Methodology Telecommunications
	8. Verify Confirmation of the successful or unsuccessful completion of the data transmission. To provide confirmation, the telecommunications components of a voting system shall: (V1: 6.2.7) • Notify the user of the successful or unsuccessful completion of the data transmission; and • In the event of unsuccessful transmission, notify the user of the action to be taken. 9. Verify Access Control procedures and system capabilities that detect or limit access to system components in order to guard against loss of system integrity, availability, confidentiality, and accountability (V1: 7.5.1 & V1: 7.2), Verify all system access control measures designed to permit authorized access to the system and prevent unauthorized access, such measures include: (V1: 7.2.1.2) • Use of data and user authorization; • Program unit ownership and other regional boundaries; • One-end or two-end port protection devices; • Security kernels; • Computer-generated password keys; • Special protocols; • Message encryption; and • Controlled access security. 10. Verify Data Integrity by validating that transmission of data shall ensure the receipt of valid vote records is verified at the receiving station. Verify use of standard transmission error detection and correction methods such as checksums or message digest hashes. 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. (V1: 7.5.1.a) 11. "Voting systems that use telecommunications as defined in Section 6 to communicate between system components and locations before the poll site is officially closed shall: (V1: 7.5.1.b)" • Implement an encryption standard currently documented and validated for use by an agency of the U.S. Federal Government; and • Provide a means to detect the presence of an intrusive process, such as an Intrusion Detection System. 12. Verify system for 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. Verify if requirement is satisfied by confirming the proper implementation of proven commercial security software. (V1: 7.5.2) 13. Verify that Vendor documentation provides Identification of COTS Products 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. • Such documentation shall identify the name, vendor, and version used for each such component.

Test Detail Test Case Name	Test Methodology Telecommunications
	14. Verify the Use of Protective Software at the receiving-end of all communications paths to: (V1: 7.5.2) • Detect the presence of a threat in a transmission; • Remove the threat from infected files/data; • Prevent against storage of the threat anywhere on the receiving device; • Provide the capability to confirm that no threats are stored in system memory and in connected storage media; and • Provide data to the system audit log indicating the detection of a threat and the processing performed. • Validate the use of multiple forms of protective software as needed to provide capabilities for the full range of products used by the voting system. 15. Verify Vendor documentation to ensure conformance of Monitoring and Responding to External Threats to which their voting systems are vulnerable. This documentation shall provide a detailed description, including scheduling information, of the procedures the vendor will use to: (V1: 7.5.3) • Monitor threats, such as through the review of assessments, advisories, and alerts for COTS components • Evaluate the threats and, if any, proposed responses; • Develop responsive updates to the system and/or corrective procedures; • 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; • 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 no later than one month before an election; and • 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. After the election, modifying the system to address the threat; submitting the modified system to an ITA and appropriate 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. 16. Voting Process Security for Casting Individual Ballots over a Public Telecommunications Network (V1: 7.6.2)
Documentation: **Test Data & Test Results**	For each iteration that the election is run: • Capture all voting steps in order to maintain repeatability of the test • Record election, ballot, and vote data fields on the corresponding worksheet tabs • Save all worksheet tabs for all iterations of the test case • Record results of test run by entering 'Accept/Reject' on the Test Results Matrix • Provide comments when observing deviations, discrepancies or notable observations • Log discrepancies on the Discrepancy Report

Test Detail Test Case Name	Test Methodology Telecommunications
Results are Observed	Review the outcome of the test(s) against the expected result(s): • **Accept**: expected results is observed • **Reject:** expected result is NOT observed • **Not Testable (NT)**: rejection of a previous test step prevents validation of this step or this was tested in another test case • **Not Applicable (NA):** not applicable to the current test scope or to the component under review • **Not Supported (NS)**: not supported in the current test scope
Record Observations and all input/outputs for each election	All information used in processing the test case is captured. This includes: inputs, outputs, deviations and any other item that may impact the validation of the test case. Any failure of the test against the EAC guidelines is reported and implies failure of the system. Failures are reported as Defect Issues in the Discrepancy Report and are provided to the manufacturer. Before the final Certification Test Report is issued, manufacturers are given the opportunity to correct all discrepancies. If the manufacturer submits corrections, retests are performed. Issues that do not impact the failure of the requirements but could be considered defects are logged as Informational Issues on the Discrepancy Report. It is the manufacturer's option to address these issues.

APPROVAL SIGNATURES

Signing below indicates approval of this Final Master Test Plan for the NYSBOE Voting System Examination and Certification Testing project.

Rex Reed, PMP, SysTest Labs, Senior Project Manager Test Plan Author and Program Manager	Date
Glenn Truglio, SysTest Labs, Chief Operating Officer Project Director and Project Advisory Board	Date
Robert Warren, NYSBOE, Certification Project Manager	Date
Tarry Breads, NYSBOE, Administrative Project Manager	Date
Anna Svizzero, NYSBOE, Director Of Election Operations	Date
Kim Galvin, NYSBOE Deputy Director Of Election Operations	Date

End of Final Master Test Plan