New York State Board of Elections
Voting System Verification Testing

Final Master Test Plan

Document Number SL-MTP-08-V-NYSBOE-0337, Rev 1.4
May 1, 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

Copyright © 2008 by SysTest Labs Incorporated

All products and company names are used for identification purposes only and may be trademarks of their respective owners.

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
4/28/08	Updated with Review Comments from NYSTEC and NYSBOE	J. Henry, P. Bialka	Rev 1.1
4/30/08	Updated Attachment A. Matching names in Requirements Matrix to names in the Test Cases	J. Henry, W. Ernissee	Rev 1.2
5/01/08	Updated Security to clarify Voting System Threat Assessments and updates to Proprietary Data.	J. Henry, P. Bialka	Rev 1.3
5/01/08	Included NYSTEC changes to the security section.	J. Henry	Rev 1.4

TABLE OF CONTENTS

1 INTRODUCTION 6
1.1 PROJECT OVERVIEW 6
1.2 PURPOSE 6
1.3 SCOPE OF TESTING 7
1.4 PRE-VALIDATION REVIEW 8
1.5 FINAL MASTER TEST PLAN ATTACHMENTS 9
1.6 SCOPE OF A VOTING SYSTEM 9
1.7 CHANGE CONTROL AND CONFIGURATION MANAGEMENT 10
1.8 ASSUMPTIONS 12
1.9 APPLICABLE STANDARDS AND REFERENCES 13
1.9.1 Required Voting System Standards 13
1.9.2 Applicable Test Method Standards 13
1.9.3 References 13
1.10 TERMS, ABBREVIATIONS AND DEFINITIONS 14
2 TEST ITEMS AND FEATURES 18
2.1 FEATURES TO BE TESTED 18
2.2 FEATURES NOT TO BE REVIEWED, ASSESSED AND/OR TESTED 19
2.3 TEST ITEM PASS/FAIL CRITERIA 19
2.4 TEST SUSPENSION CRITERIA AND RESUMPTION REQUIREMENTS 20
3 TEST TYPES 22
3.1 PHYSICAL CONFIGURATION AUDIT 22
3.1.1 Trusted Build 22
3.1.2 Software and Hardware Configuration Audit 22
3.2 FUNCTIONAL CONFIGURATION AUDIT 23
3.2.1 Review of Prior ITA Test Cases and Results 23
3.2.2 Review of Other State Verification Testing or Risk Analysis Results 23
3.2.3 Review of Prior Hardware Environmental Testing 23
3.2.4 Hardware Environmental Testing 23
3.2.5 Module Testing 24
3.2.6 System Testing 24
3.2.7 Accuracy Testing 25
3.2.8 Security Testing 25
3.3 NYSBOE INTERPRETATIONS 26

4 VERIFICATION TEST ARTIFACTS 28
5 TEST TASKS 33
5.1 PHYSICAL CONFIGURATION AUDIT 33
5.1.1 Trusted Build 33
5.1.2 Software and Hardware Configuration Audit 35
5.2 FUNCTIONAL CONFIGURATION AUDIT 35
5.2.1 Review of Prior ITA Test Cases and Results 35
5.2.2 Review of Other State Verification Testing or Risk Analysis Results 36
5.2.3 Review of Prior Hardware Environmental Testing 37
5.2.4 Hardware Environmental Testing 38
5.2.5 Module Testing 40
5.2.6 System Testing 40
5.2.7 Accuracy Testing 45
5.2.8 Security Testing 45
6 TEST DATA 50
6.1 TEST ELECTION DEFINITIONS 50
6.2 TEST VOTE DATA 51
6.3 DATA RECORDING 51
6.4 TEST DATA REDUCTION 51
7 MATERIALS REQUIRED FOR TESTING 53
7.1 SOFTWARE/FIRMWARE 53
7.2 EQUIPMENT/HARDWARE 53
7.3 TEST MATERIALS 53
7.4 PROPRIETARY DATA 54
8 TEST PROCEDURE AND CONDITIONS 55
8.1 FACILITY REQUIREMENTS 55
8.2 TEST SETUP 55
8.3 TEST SEQUENCE 55
8.4 TEST OPERATIONS PROCEDURES 58
8.5 TEST ERROR RECOVERY 59
APPROVAL SIGNATURES 60

List of Tables:

Table 1 - Summary of a Voting System's Components 9

Table 2 - Terms, Abbreviations and Definitions 14

Table 3 - Test Suspension Criteria and Resumption Requirements 20

Table 4 - Verification Testing Deliverables 29

Table 5 - 2005 VVSG Hardware Environmental Test Sections and Descriptions 39

Table 6 - Types of System Testing 41

Table 7 - Types of Security Testing 47

Table 8 - Test Materials 53

Table 9 - High-Level Verification Milestones in Sequence 56

List of Figures:

Figure 1 - Verification Testing Artifacts 28

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 voting-system oriented 2005 VVSG, Volume 2 standards and include more detailed and specific guidelines for general Test Plan format and content. 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 through Attachment A and Attachment C.
- Serves as a foundation for the development of Vendor-specific Test Plans and Test Cases.
- Defines the process for recording and reporting test results.
- Defines the process for regression testing and closure of discrepancies.

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 testing of each voting system against all 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 is tested against all security related requirements as well as assessing the effectiveness of a voting system's security controls.
    - Verification of every system function and combination of functions cited in the vendor's documentation.
- 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 is tested against 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**.
- 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). The details of what is included in Final Voting System Specific Test Report is defined in Table 4 - *Verification Testing Deliverables.* An initial draft of the Final Voting System Specific Test Report will be created using the standards within IEEE Std 829-1998 and 2005 VVSG, Vol 2, Appendix B - National Certification Test Report, and will be submitted to NYSBOE for inspection and approval prior to the delivery of the final version.

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 any previous testing performed by the Vendor, EAC (Election Assistance Commission) accredited VSTLs (Voting System Test Labs), previous NYSBOE ITAs, and SysTest Labs' own test efforts. This is defined as a component of **Deliverable 5: Review of Technical Data Packages (TDP's)**.

- SysTest Labs will evaluate system testing completed by NYSBOE ITAs in order to identify any known vulnerabilities and incorporate them into SysTest Labs Test Cases that are repeatable and detailed enough to satisfy the Testing Expectations document.

- SysTest Labs will evaluate the quality and coverage of prior hardware verification testing in addition to prior hardware environmental testing completed by previous EAC accredited VSTLs, NYSBOE ITAs, and SysTest Labs on the same voting hardware components and/or software components. For more information, see Section 3.2.1 *Review of Prior ITA Test Cases and* Results, and Section 3.2.3 *Review of Prior Hardware Environmental Testing*.

- SysTest Labs will complete an FCA review of other state certification reports, voting system test or risk assessment final reports in order to determine whether or not issues and vulnerabilities found in other States will be present in the voting systems submitted for NYSBOE verification. For more information, see Section 3.2.2 *Review of Other State Verification Testing or Risk Analysis Results* .

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*
Attachment C – *NYSBOE Lot 1 Test Cases*

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	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	Election Management System Hardware	Personal Computer (PC) and peripherals (keyboard, monitor, mouse, printer, etc.) on which the Election Management System software is installed.
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.

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 Change Control and Configuration Management

The SysTest Labs project team follows a standard Change Control and Configuration Management (CM) process. This specifies the methods used by SysTest Labs to ensure changes are managed and controlled effectively and efficiently and defines the process for receipt, check-in, storage and disposition of Vendor hardware, source code, TDP and non-TDP Documents.

It specifies the processes and procedures used by SysTest Labs to identify, monitor, and control versions of all of the stated NYSBOE project deliverables, ensuring that the items are constantly and reliably managed throughout the entire duration of the engagement to ensure changes are managed and will not result in invalidated or wasted testing efforts.

A summary of these tasks includes:

- Receive TDP code:

- Delivery department will perform a code check-in on the server. Code is placed in the vendor specific project folder with the delivery date and documentation of what was delivered.
- Delivery department notifies Project Manager (PM), Source Code Manager (SCM), and Test Manager (TM) of delivery via email.
- SCM will notify the Source Code Lead via email the code is ready for review.
- TM will review the documentation of what was delivered to determine possible testing impacts. TM may suspend associated testing until a new Trusted Build is delivered.
- Source Code Lead updates status of delivered code as received, what code to compare it to (if this is not new code), where code has been placed, and who will do the review of the code.
- The code is checked out by the person who is responsible for the code review.
- When the code review is complete, the code is checked back in and the Source Code Lead is notified.
- A peer review is done on the review and all written discrepancies are verified and an official Discrepancy Report is sent.
- If the Source Code Review Team determines the code is acceptable from their perspective, the Source Code Lead will review code impacts with the Test Lead.
- Test Lead determines if code is ready for a Trusted Build. If it is, they notify the TM who sends approval for a Trusted Build to the SCR PM. Test Lead may suspend associated testing until a new Trusted Build is provided.

- Receive TDP documents:
  - Delivery department will perform a check-in of the documents on the server. Documents are placed in the vendor specific project folder with the delivery date.
  - Delivery department notifies Project Manager (PM) and Project Lead of delivery via email.
  - The PM updates the delivery status to 'received' and notifies the Test Manager (TM) the documents are ready for review.
  - TM or the Test Lead assigns a person to perform the documentation review.
  - A peer review is done on the review and all written discrepancies are verified and an official Discrepancy Report is sent.

- Receive Hardware
  - The HW manager checks in equipment that is sent by the vendor and will be going to the Hardware labs.
  - When the equipment comes back from the hardware lab testing, the PM or Project Lead checks in the equipment and verifies it's the same hardware that was sent to the lab and compares it against the vendor documentation for confirmation.

    - The equipment is stored in a secure room with controlled access.
- Trusted Build:
    - Once code review discrepancies are complete the SCR PM assigns an SCR team member to review the vendors Trusted Build procedures and perform the build.
    - SCR team member follows build procedures exactly as written. (For details, see Section 3.1.1 - *Trusted Build*)
    - SCR team member pulls the source code from the vendor specific folder where it was checked in.
    - Once build is complete the SCR team member provides the completed build to the SysTest Labs Delivery Team to be checked in.
    - SCR team member notifies the TM and Test Lead that the install/exe is checked in.
    - TM assigns a Test Lead and a tester to load the install/exe and start their testing.
    - The Test Lead checks out the install/exe, loads it, and begins testing.

1.8 Assumptions

The development of a comprehensive test plan requires that any assumptions regarding the test effort be explicitly stated. For this test effort, the assumptions are:

- There will not be any witness builds; all builds will be Trusted Builds performed without Vendor Assistance.
- 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 except those found during the Run For Record. 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]. Fixes provided for SysTest Labs identified discrepancies that are not provided by the Vendor to SysTest Labs prior to the beginning of the 'Run For Record Test Pass' task date will not be implemented and will not be included in the Final Trusted Build used for the 'Run For Record' test.

[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

- 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.

1.9 Applicable Standards and References

1.9.1 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)

1.9.2 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
3. 2005 VVSG Volume 2, Sections 3 through 7

1.9.3 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

1.10 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.

Term	Abbreviation	Definition
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.
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.
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.

Term	Abbreviation	Definition
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. The CaliberRM tool stores the following (defined as **Deliverable 3: Testing Requirements Confirmation Matrix**):

- Requirements Matrix containing:
  - 2005 VVSG, Volume 1
  - 2005 VVSG, Volume 2
  - NYS 2007 Election Law
  - NYS 6209 Regulations
  - NYS BMD Requirements
  - Source Code Review Criteria
  - Documentation Review Criteria
- Traceability from Requirements to TDP review and assessment activities
- Traceability from Requirements to Test Cases and from Test Cases to Requirements
- Test Cases

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).

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

- Prior SysTest Labs Test Methods and Results.
- Prior Hardware Environmental Test Methods and Results.

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 the hardware reviews may be used in the verification testing efforts and therefore, not require duplicate testing as long as the hardware contains only di minimus changes. SysTest Labs will forward to the NYSBOE for review and approval those items it deems as sufficient to satisfy stated requirements. SysTest Labs will analyze the other testing results for known vulnerabilities so the test cases can be updated to validate they have been addressed.

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 as defined by the Requirements Matrix. 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.

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 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

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. NYSBOE will be notified of any Test Suspension and subsequent Resumption via the Daily Status Report. 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
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	• 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.

Suspension Item	Criteria	Criteria for Resumption
	and/or documentation	
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.
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' functional 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, without assistance by the Vendor and includes:

- 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

SysTest Labs will evaluate the prior verification testing completed by previous NYSBOE ITAs. This activity will identify any vendor specific system vulnerabilities that will need to be tested for by the SysTest Labs' effort. The outcome of these reviews may result in additional requirements, test cases and/or test steps being added to either the Requirements Matrix or the Vendor Specific Test Cases. 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

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). This activity will review the reports for any prior known or identified vulnerabilities. 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

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, however only de minimus changes to the hardware will be permitted and are subject to review and approval by the NYSBOE. 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 (based on the NYSBOE Certified Voting System Escrow Requirements – Final) 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*.

The initial set of system test cases designed for voting system verification testing for the NYSBOE are listed in Attachment C – NYSBOE Lot 1 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 source code reviews, document reviews, and selective retesting of the 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

As part of the system testing, SysTest Labs will perform a final test of the fully integrated voting systems using the Final Trusted Build. This Final Trusted Build will be created as detailed in Section 5.1.1 Trusted Build. Once the Final Trusted Build is complete, no Vendor changes will be permitted and any discrepancies found are considered part of the final tested product. This test is referred to as a "Run For Record Test". This will include all Test Cases with the exception of hardware environmental Test Cases. 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

NYSBOE's specific expectations for security testing includes both the process of validating that a voting system is fully tested against 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.

In security testing, SysTest Labs will identify and provide to the NYSBOE, for review and approval, specific threat and vulnerability 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 testing methodology as defined in Section 1.9, *Applicable Standards and References*. 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 it is an ambiguity.

---

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

[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

The illustration of the documentation and deliverables that will be developed and submitted as a part of the NYSBOE verification testing effort is 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.
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

Item	Description
	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 will include: • Test Procedures • Inputs • Expected results • Actual results • Anomalies • Date and time • Procedure step • Environment • 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

Item	Description
	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. • 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 time and date that each test was performed, and the initials of the tester(s) and observer(s). • All test procedures, test cases, and the results that are mapped from the requirements matrix. • All supporting log files, pictures, tester notes etc.

Item	Description
	• All information, or links to it necessary for a 3rd party to reach the same result as SysTest upon review of the materials. • The results from review and validation of the TDP documentation listing all resolved discrepancies 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, 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 and a listing of all prior testing that was approved by the NYSBOE to not be run because it was duplication of prior work. • A final assessment and evaluation of the voting system's ability to comply with the Requirements Matrix.

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 Attachment C – NYSBOE Lot 1 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.

Access to the archived testing artifacts by NYSBOE is by request to SysTest Labs. SysTest Labs will upload requested items to SharePoint or send them to NYSBOE by e-mail or regular mail.

5.1 Physical Configuration Audit

5.1.1 Trusted Build

Trusted builds are initiated upon completion of each cycle of the PCA source code review activity and throughout the functional testing, as detailed in the Master TDP Review Plan, and there are no open or outstanding source code related discrepancies from the TDP source code review or regression review and assessment.

During functional testing, discrepancies identified may require that Vendor source code be modified. Upon receipt from the Vendor, all code modifications will be re-reviewed and upon completion of this a new Trusted Build will be created. Regression reviews are accomplished as defined in the Master TDP Review Plan – Section 5.2.2 Regression Reviews and Assessments.

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.

- Interviews:
  - Key Vendor staff is 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.

- Ensure that all compilers are COTS (as defined in Certified voting System Software and Source Code Escrow Requirements[5]) compilers and not Vendor provided compilers. If compilers or build scripts are vendor-provided, they will be subject to the full Source Code Review process.
- 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.
      - 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 Final Trusted Build. SysTest Labs will ensure that all appropriate provisions of 2005 VVSG, Sections 7.4.4 and 7.4.5 are adhered to.
    - 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.

---

[5] *Certified Voting System Software and Source Code Escrow Requirements for New York State Board*, New York State Technology Enterprise Corporation, January 21, 2008

    - 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 Final Trusted Build process:
  - Upon completion of the Run for Record testing, SysTest Labs will complete all final record keeping and archiving procedures for the Final Trusted Build at SysTest Labs' facility.
  - 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 configuration conforms to vendor specifications of the system under test, including TDP documentation (can include hardware and software specifications, approved parts list, etc.).
- Verify that the system configuration is consistent with the configuration assessed in any previous ITA reports.
- Verify that the system configuration is consistent with the system used in hardware environmental tests for the current ITA test campaign.
- Perform an operational status check.

5.2 Functional Configuration Audit

5.2.1 Review of Prior ITA Test Cases and Results

SysTest Labs will evaluate the prior verification testing completed by previous NYSBOE ITAs. This activity will identify any vendor specific system vulnerabilities that will need to be tested for by the SysTest Labs' effort. The outcome of these reviews may result in additional requirements, test cases and/or test steps being added to either the Requirements Matrix or the Vendor Specific Test Cases.

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 there were any Vendor specific vulnerabilities identified and these will be added to the testing and reflected as such in the Requirements Matrix specified for the voting system.

Tasks required for this review:

- Identify any functional, security or operational issues identified within prior ITA reports, voting system tests or risk assessment final reports, and other comparable examinations performed by independent testing organizations, such as the Everest Report. Refer to Sub-section 6209.G of the NYS 6209 Regulations for examples of types of code-related issues that should be investigated.
- 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.

The results from this activity are part of **Deliverable 4: Evaluation of Prior Work.**

5.2.2 Review of Other State Verification Testing or Risk Analysis Results

SysTest Labs will conduct reviews of other state certification reports, voting system test or risk assessment final reports and independent testing organization examinations. These reviews will be performed in order to determine if functional, security or operational issues encountered or vulnerabilities identified 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 resolved 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. Refer to Sub-section 6209.G of the NYS 6209 Regulations for examples of types of code-related issues that should be investigated.
- 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.

The results from this activity are part of **Deliverable 4: Evaluation of Prior Work.**

5.2.3 Review of Prior Hardware Environmental Testing

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 identical, or has di minimus changes, 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. These changes to the hardware are subject to review and approval by the NYSBOE
- 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

Test Type	2005 VVSG Section	Test Description
	4.8	Electrical Fast Transient
	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.

Testing will be conducted in a secure testing room at SysTest Lab's facility, utilizing a minimum of one tester and one observer. Wherever possible, the person running the test (the observer), will not be the person who wrote the test case.

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 is tested against all elements specified in the Requirements Matrix.
• Failure Injection	This is an extension of Functional Testing where the tests are executed using either erroneous initial conditions or invalid data elements.	Failure Injection testing extends Nominal testing. In these tests, all boundary conditions are exercised.
• Data Driven	This is testing that is based on the data that is used throughout the voting system. For example, if 'x' is input in a field, it would branch to a different part of the application than if 'y' was entered. The goal is to ensure that all branches get tested.	The tests verify that each unique data element can be accessed and used according to the voting system's user documentation. These test cases are based on the election data or vote data used and not the functional flow or work flow of the voting system.
• 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.

Type of Testing	Description	Benefit
• 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.
• Run For Record	Final Validation 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.

Type of Testing	Description	Benefit
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 is tested against 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.
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:

- Evaluate the discrepancy that was fixed and the extent of the fix within the source code through Source Code Review, 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. This is performed using the Regression Review and Assessment process as defined in the Master TDP Review Plan, Section 5.2.2*, Regression Reviews and Assessments.*
- 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:
    - Depending on the extent of the source code changes, evaluate what other areas of the functionality are impacted and determine which test cases were invalidated or need to be re-run.

- 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.

5.2.6.2 Run For Record Testing

As part of system testing, after SysTest Labs has performed the final Trusted Build, (Reference Section 5.1.1 *Trusted Build*) SysTest Labs will perform the official Run For Record tests which include the functional, accuracy, and volume and stress test cases. This is the final functional test of the system to ensure that all vendor modifications are fixed.

The Final Trusted Build created for the Run For Record Testing will freeze the code, and no changes of or updates to the VSUT hardware will be permitted. Any anomalies identified during the Run For Record Testing will be noted; however, they will not be reported as formal discrepancies to the Vendor and will be considered part of the final tested product. The Run For Record Testing is the final run of the functional test cases before SysTest Labs creates the Final Voting System Specific Test Report.

The Final Trusted Build will be placed into escrow in accordance with the NYSBOE Certified Voting System Software and Source Code Escrow Requirements.[6]

5.2.6.3 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 requirement in the Requirements Matrix and SysTest Labs has confirmed through re-review and/or re-testing that the requirement has been met. The Run For Record Test will retest all discrepancies that were closed during prior regression testing.

- 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.

---

[6] *Certified Voting System Software and Source Code Escrow Requirements For New York State Board of Elections*, New York State Technology Enterprise Corporation (NYSTEC), January 21, 2008

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

NYSBOE's specific expectations for security testing includes both the process of validating that a voting system is fully tested against all security related requirements defined specifically in the Requirements Matrix as well as assessing the effectiveness of a voting system's security controls[7]. 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:

---

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

- 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).
- Where the Vendor's statements assert the voting system is secured via processes, physical mechanisms and physical seals, the test procedures will verify the presence and effectiveness of such controls.
- Negative testing will be performed to identify vulnerabilities that could be used to circumvent controls or compromise the system.

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.

Security testing is related to four main testing activities.

- **Source Code Testing –** Source Code Testing, both before and during functional testing, ensures that each source code module will be reviewed, and re-reviewed as needed, for compliance with coding requirements and best practices as defined in the 2005 VVSG and within the Requirements Matrix. This includes a review to ensure protection against all known vulnerabilities that have been identified with prior assessments and within the public sector.
- **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 tests, source code review, 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.
- **Voting System Threat Analysis –** SysTest Labs has scrutinized the lifecycle of a voting system and the classifications of voting system threats and vulnerabilities within the lifecycle of a voting machine that are likely to occur. These are:
    - Manufacturing mode – When voting systems are created. This includes software development, testing and construction of the voting system from a variety of parts suppliers. This mode begins in the early design stages for a system and ends when the machine is ready to be shipped to a customer.
    - Storage Mode – This includes the distribution of new systems and systems that are being shipped or in storage while not in use. Storage mode includes inter-election

maintenance activities performed on the systems. Storage mode begins when the machine leaves the vendor facility to be shipped and ends when a system is turned on to be used for an election or testing.

- Pre-Vote Mode – This begins when machines are pulled from storage and prepared for an election. This mode includes any programming or configuration of elections to be conducted on the system.
- Voting Mode – This begins when the machine is switched into "vote mode" and ends when the machine is switched out of "vote mode".
- Post Election Mode – This is the phase after the polls have closed and votes are being tabulated.

SysTest Labs Security Analysts have examined and evaluated voting system testing related reports from states including, but not limited to Maryland, Ohio, Connecticut, Florida and California within which threats and vulnerabilities have been identified. SysTest Labs will categorize and summarize these identified vulnerabilities into one or more of the above described voting system threat classifications.

Review and analysis of these types of threats and vulnerabilities by SysTest Labs Security and Testing experts will identify and clarify which of them can and will be addressed in the SysTest testing effort for NYSBOE and drive enhancements, updates, and additions to Voting System Specific Test Cases.

Table 7 - *Types of Security Testing* provides a high level description of the types of security testing that will be run against the voting system to determine if the system meets 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 transmission, results downloading and resetting of elections. Voter equipment access or keys are limited to ensure:

Type of Testing	Description
	• 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.
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

Type of Testing	Description
	Verify the election specific firmware and operating system are stored separately 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 results will be documented and so noted if they differ from expected results.

All data relevant to the testing of a requirement will be made available to NYSBOE via the appropriate Final Voting System Specific Test Report, and will contain references to supporting data as needed to provide independent third party reviewers the information necessary to reach the same results and 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

In accordance with the contract between SysTest Labs and the NYSBOE, the determination of proprietary information will be made at the discretion of the NYSBOE.

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 ensures access to secure voting rooms is controlled 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, Vendor 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. Vendor representatives are never left unattended in a voting test lab. Vendor representatives are 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.
FCA – Hardware Environmental Testing	Completion of FCA test case preparation and PCA system configuration audit. Initiation of hardware and performance testing, including discrepancy reporting.

Verification Task	Prerequisite Task
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. These procedures will be mapped to the Requirements Matrix. Each step shall be assigned a test step number; this number, along with critical test data and test procedure information, shall be tabulated onto the appropriate Test Case for test control and the recording of test results. These test cases contain sufficient detail to allow for consistent and repeatable test execution and will be included as part of the Final Voting System Specific Test Report.

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 and Observer names
- Type of test (*system, security, accuracy*, *hardware*)
- Test case and test steps
- Applicable requirement(s)
- Vendor 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 Final Voting System Specific Test Report along with all test cases and test procedures

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.

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