Election Assistance Commission
Voting System Certification Testing

Certification Test Plan

Document Number 07-V-ESS-043-CTP-01, Rev 1.0
March 28, 2008

Prepared for:

Vendor Name	Election Systems & Software
Vendor System	ES&S AutoMARK 1.3 Voting System
EAC Application No.	ESS0703
Vendor Address	11208 John Galt Boulevard Omaha, NE 68137-2364

Prepared by:

SysTest labs®

216 16th St.
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

Revision History

Date	Description of Revision	Author	Revision No.
10/01/2007	Initial Test Plan delivered to the vendor	R. Reed/ T. Damour/ J. Garcia	Rev. 0.01
2/12/2008	Initial Test Plan (new format)– SysTest Labs	K. Swift	Rev. 0.02
2/15/2008	Updates based on vendor responses, Added Attachment I.	K. Swift, A. Backlund	Rev. 0.03
3/28/2008	Updates based on EAC Test Plan feedback. Initial submission to the EAC.	M. Hilgert	Rev. 1.0

TABLE OF CONTENTS

LIST OF TABLES

1 INTRODUCTION

This Certification Test Plan outlines the approach SysTest Labs will implement to perform Election Assistance Commission (EAC) certification testing on the ES&S AutoMARK 1.3 Voting System to the approved voting system standards (VSS), version 2002. The purpose of this document is to provide a clear understanding of the work SysTest Labs will conduct and a precise plan describing the test elements required to ensure effective Certification testing.

This test plan:

- Identifies items to be tested
- Defines the test approach
- Identifies required hardware, support software, and tools to be used for testing
- Identifies the types of tests to be performed

SysTest Labs will provide certification testing on the ES&S AutoMark 1.3 voting system based on the guidelines established for voting system certification testing as defined by the EAC. This effort includes all required levels of software, firmware, system and hardware environmental testing required to demonstrate that the ES&S AutoMark 1.3 voting system meets the requirements of the VSS, the appropriate portions of the Help America Vote Act (HAVA), and associated Vendor specific requirements. SysTest Labs' major task categories for voting system certification testing, as defined by SysTest Labs' National Voluntary Lab Accreditation Program (NVLAP) audited and approved Quality System Manual and associated SysTest Labs Procedures (SLP), include:

- Physical Configuration Audit (PCA)
    - Verification of software and hardware functional and physical configurations
    - Iterative documentation review and assessment
    - Iterative source code review
- Functional Configuration Audit (FCA)
    - Review of the ES&S AutoMark System Test & Verification Specification and all completed testing to ES&S AutoMark System Requirements Specification, as outlined in the FEC VSS Volume 1
    - Iterative hardware is environmentally testing
    - Iterative software and firmware testing to validate logic
    - Iterative testing of voting systems to validate functionality, accuracy, performance, security, and system level integration
- Management of Vendor supplied deliverables, SysTest Labs' test artifacts, and software, firmware, hardware and system test configurations
- Generation of test cases that ensure that the voting system meets all applicable VSS requirements, appropriate portions of HAVA, and associated Vendor specific requirements

- Traceability and tracking of test cases to VSS requirements, appropriate portions of HAVA, requirements established by the EAC and associated Vendor specific requirements

- Software, Firmware, System, and Hardware test execution

- Reporting of all test results

SysTest Labs' will develop and submit to the EAC a certification test report deliverable that details all test results and findings as a result of this certification test effort, as well as a recommendation to certify or not to certify based on the test results.

1.1 Certification Test Plan Attachments

The following attachments apply to this Certification Test Plan:

1. Attachment A - List of Technical Data Package (TDP) Deliverables
2. Attachment B - Supported Functionality Declaration
3. Attachment C - List of Source Code Reviewed – **PROPRIETARY**
4. Attachment D - Hardware Test Plans
5. Attachment E - ES&S AutoMark 1.3 Test Case Matrix
6. Attachment F1 - Documentation and Functional Discrepancy Report
7. Attachment F2 - Source Code Discrepancy Report – **PROPRIETARY**
8. Attachment G - Hardware Testing Results from Hardware Test Laboratories
9. Attachment H - Accredited Hardware Test Lab Certification
10. Attachment I - Trace of SysTest Labs' Test Cases to VSS, version 2002
11. Attachment J - ES&S AutoMark Certification Letter

1.2 Scope of the ES&S AutoMark 1.3 Voting System

This section provides a brief overview of the scope of the ES&S AutoMark 1.3 Voting System. In addition to the ES&S AutoMark 1.3 voting system are the ES&S Unity 3.0.1.0 & Unity 3.0.1.1 components not included in the Certification, however they are required to complete testing.

The need for this certification is due to fact that the ES&S AutoMark 1.3 component has been upgraded. ES&S and their State customers are requesting that the EAC allow for the certification of this upgrade. For further information, please refer to the ES&S AutoMark Certification EAC Notice Letter dated October 15, 2007 contained in ***Attachment J - ES&S AutoMark Certification Letter***.

This Test Plan provides a summary of the certification testing efforts for ES&S AutoMARK 1.3 voting system. The ES&S Unity 3.0.1.0 (NASED #N -2 -02 -22 -22 -008) and Unity 3.0.1.1 (NASED #N -2 -02 -22 -22 -007) voting systems have both been previously qualified under NASED, however ES&S will not be certifying these versions of voting systems under the EAC. The Unity 3.0.1.0 and Unity 3.0.1.1 voting systems will not be part of this Certification; however election data that was created at the time of 3.0.1.0 and 3.0.1.1 NASED Qualification testing will be used, enabling the test reports to demonstrate the compatibility of the systems.

The voting system consists of the AutoMARK Information Management System (AIMS), an election creation software component and two models (A100 and A200) of the Voter Assist Terminal (VAT) an optical paper ballot marking component. Elections will be created, imported and modified in AIMS and voted on the VATs. All ballots in the end to end testing will be hand counted. All ballots from the accuracy test will be counted via ES&S Model 100 and Optech III-P Eagle optical scanners. The scanners are not part of the Certification but used for tabulating purposes only.

Please note that each of the items listed in Table 1 - Summary of ES&S AutoMark 1.3 Voting System Components are explicitly defined in Tables 3, 4 and 5. The list of software, firmware, and hardware components, their model numbers and versions, and their configurations included in this certification testing effort are defined in the TDP items delivered to both SysTest Labs and the EAC.

Table 1 - Summary of ES&S AutoMark 1.3 Voting System Components

Software/Firmware	Hardware
ES&S AutoMARK Information Management System (AIMS)	ES&S AutoMARK Voter Assist Terminals (VAT) Models A100, A200

1.3 Applicable Standards

1.3.1 Applicable Voting System Standards

All testing will determine whether or not the ES&S AutoMark 1.3 voting system meets the requirements from the following voting system Standards:

1. VSS, version 2002[1]

2. Help America Vote Act (HAVA) – Section 301

1.3.2 Applicable Testing Standards

All testing will be conducted based on the following testing standards and guidelines[2]:

1. NIST NVLAP Handbook 150: 2006

2. NIST NVLAP Handbook and 150-22: 2005[3]

3. EAC Testing and Certification Program Manual, United States Election Assistance Commission, 2006

4. DRAFT – VSTL Accreditation Program Manual DRAFT

1.4 References

1. SysTest Labs Quality System Manual, Revision 1.1, February 18, 2008.

[1] Please note that in addition to the VSS, version 2002 requirements, SysTest Labs must interpret and apply similar requirements from the VSS, version 2002 for Voter Verifiable Paper Audit Trail capabilities, Ballot Marking Devices, and Bar Code Readers.

[2] Where conflicts in the testing standards exist, the EAC Guidelines take precedence.

[3] SysTest Labs was accredited as a VSTL under the 150-22: 2005 NIST Handbook but the EAC has requested that where conflicts exist, testing adhere to the guidelines defined in the 150-22: 2007 NIST Handbook.

1.5 Terms, Abbreviations and Definitions

Table 2 - Matrix of Terms & Abbreviations provided by the vendor

Term	Abbreviation	Definition
AutoMARK Information Management System	AIMS	AIMS is a Windows™-based PC application program that assists election officials or their designees in preparing the flash memory card (FMC) required by the AutoMARK Voter Assist Terminal (VAT) for use in an election.
AutoMARK Voter Assist Terminal	VAT	The AutoMARK Voter Assist Terminal comprises a touch screen monitor and an integral ballot printer. It is an optical paper ballot marking device that can be used for disabled voters and alternative languages.
Flash Memory Card	FMC	The FMC supplies ballot content information to the VAT.
Unity Release	N/A	The system configuration(s) of ES&S hardware and software voting system(s).

2 PRE-CERTIFICATION TESTS

2.1 Pre-Certification Test Activity

SysTest Labs has completed an assessment of all initial deliveries of the Technical Data Package, including 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 the ES&S AutoMark 1.3 voting system. For a complete list of all items included in the TDP, please refer to ***Attachment A - List of Technical Data Package (TDP) Deliverables***. Any subsequent re-deliveries of the TDP items will be solely the result of fixes to discrepancies identified in the FCA, PCA, or test execution activities.

SysTest Labs designs and executes procedures to test a voting system based on the requirements as outlined in VSS Volume 1, Section 2 pertaining to Overall system capabilities, Pre-voting, Voting, Post-voting, System maintenance, and Transportation and storage. The procedures, as well as the prerequisite conditions, are performed in logical configuration to fully test the proper functioning of the integrated components of the voting system as defined by the vendor, and are detailed in **Appendix A – Test Cases**.

The scope of the testing process that SysTest incorporates into voting system testing seeks to ensure the voting system is in compliance as will be verified in the end-to-end system-level test cases created and executed by SysTest, while addressing the requirements as outlined in VSS Volume 2, Section 6.

While one of the pre-certification tasks performed is a functional configuration audit (FCA) of the vendor's test cases, these test cases are reviewed to ensure the vendor is performing due diligence in compliance with testing their system.

Additionally, as detailed in ***Attachment I - Trace of SysTest Labs' Test Cases to VSS, version 2002***, SysTest performs testing to meet the requirements of VSS Volume 1 as they pertain to the system-specific functional capabilities, specific technologies, and design configurations as employed by the vendor.

SysTest Labs will also conduct an assessment of any additional voting system functionality as defined by the vendor, or requested by the vendor for inclusion in testing. This additional system functionality will be identified and included either in the test cases developed by SysTest Labs or executed as part of our sampling guidelines.

2.1.1 Physical Configuration Audit

2.1.1.1 Document Review

SysTest Labs conducted a PCA review of all vendor traced documents submitted for review in the initial delivery of the ES&S AutoMark 1.3 TDP. These included:

- System configuration overview
- System functionality description
- System hardware specifications
- Software design and specifications
- System test and verification specifications
- System security specifications
- User/system operations procedures
- System maintenance procedures
- Personnel deployment and training requirements
- Configuration management plan
- Quality assurance program
- *System change notes – N/A (first time certification)*

Each document included in the initial delivery of the ES&S AutoMark 1.3 voting system TDP was reviewed for compliance to the 2002 VSS, Volume 2, Sections 2.2 through 2.13 and Volume 2, Section 6.6. Any subsequent re-reviews of TDP items will be the result of fixes to discrepancies identified in the PCA Document Review activity.

2.1.1.2 Source Code Review

The ES&S certification campaign for the ES&S AutoMark 1.3 voting system includes only the ES&S AutoMark VAT 1.3 and AIMS 1.3 products. SysTest Labs has conducted a source code review of all source code submitted in the initial delivery of the ES&S AutoMark 1.3 voting system TDP. The coding languages include the following:

- C
- C++
- VBA
- VB.net
- C#
- Assembly

Source Code Review Tools utilized by SysTest Labs include

- Practiline Line Counter: a commercial application used to determine the counts of executable and comment lines;
- Module Finder: a SysTest Labs proprietary application used to parse module names from C/C++ and VB code and populate the identified module names into the review documents;
- ExamDiff Pro: a commercial application used to compare revised code to previously reviewed code; and
- KEdit: a commercial text editor application running a SysTest Labs proprietary macro used to parse module names from Cobol code and populate the identified module names into the review document.

Each source code module included in the initial delivery of the ES&S AutoMark 1.3 voting system TDP was reviewed for compliance to the VSS, version 2002, Volume 2, Section 6.6.

Any subsequent re-reviews of source code will be the result of fixes to discrepancies identified in the PCA Source Code Review activity. Please refer to ***Attachment C – List of Source Code Files Reviewed–PROPRIETARY*** for a listing of source code submitted for review as of this writing.

2.1.1.3 Trusted Build

The Trusted Builds will be conducted prior to SysTest Labs' testing efforts and will be completed on site at SysTest Labs' facility or a secure lab at the vendor's facility approved by SysTest. SysTest Labs will use its approved standard lab procedure that details the processes for controlling, managing, and conducting the Trusted Build. This process includes the following:

- Interviews – Key vendor staff are interviewed to evaluate processes and process conformance in the areas of configuration management and quality assurance.

- Preparation for the Trusted Build - Obtaining and reviewing EAC Testing & Certification Program Manual as well as ES&S's procedure for constructing the build platform, verifying the target build platform, and acquiring and verifying the necessary materials.
- Execution of the Trusted Build – SysTest Labs will perform the Trusted Build by using our step-by-step build procedure. SysTest Labs records and ascertains the following items throughout the build process:
    - Build environment images at various key points
    - Build environment and file hashes at various key points
    - Build environment hardware characteristics
    - Build results from code compilation
    - Final software install files

- Deliverables to Vendor and Testing – Upon completion of the Trusted Build, certain items are sent to the vendor and SysTest Labs test group. The final result will be a compact disk containing the following:
    - Final software install files
    - Hash values to validate install files
    - Images
    - Build Products

- Final Record Keeping And Archiving Procedures – At the conclusion of the Trusted Build process, SysTest Labs completes all final record keeping and archiving procedures at SysTest Labs' facility. This record keeping includes any unique identifiers, results of the build with version numbers and dates and descriptions of all hashes and images in the repository. In addition, at this time, we will generate the final product that is submitted to the EAC's approved software repository.

- 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 or witnessed by SysTest Labs staff. For the Trusted Build environment, the operating system is installed by SysTest Labs staff.

2.1.2 Functional Configuration Audit

2.1.2.1 Review of Vendor's Completed Test Cases and Results

SysTest Labs conducted an FCA review of the ES&S AutoMark 1.3 test cases delivered as part of the initial delivery of the ES&S AutoMark 1.3 voting system TDP. These test cases are designed and executed by ES&S AutoMark for QA and testing of the ES&S AutoMark 1.3 voting system. The ES&S AutoMark 1.3 test cases were reviewed to determine the scope of testing and conformance to the VSS, version 2002, Volume 1, Sections 2, 3, 4, 5 & 6 and Volume 2, Section 6.7.

The results of these audit reviews, as well as the discrepancies generated, will be included in the Certification Report.

2.1.2.2 Review of Ohio and Colorado Voting System Reviews

SysTest Labs will conduct an FCA review of the Ohio and Colorado Voting System Reviews as directed in the EAC memorandum to the VSTLs dated December 19, 2007 (please refer to item 1, in Section 1.3.2). The directive specifically states that "…any VSTL currently testing a system from one of the manufacturers listed in these reports to review the State reports to see what, if any, items might require a closer look during Federal certification testing". SysTest Labs will review the findings against the VSS, version 2002 requirements, appropriate portions of HAVA, and associated Vendor specific requirements.

2.1.3 Hardware Environmental Testing Assessment

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

- The configuration of the equipment being presented for testing is substantially identical to the equipment that was previously tested and certified and that all changes made to the hardware configuration of the equipment being presented for testing, from the hardware that was previously tested and certified were confirmed to be de minimis changes
- The standards and associated requirements under which the previous testing and certification 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 certification meets the EAC's requirements for accreditation as defined in NIST HANDBOOK 150-22: 2005.

2.2 Pre-Certification Assessment Results

2.2.1 Physical Configuration Audit

2.2.1.1 Document Review

SysTest Labs is in the process of completing the PCA Documentation Review to ensure that the ES&S AutoMark 1.3 TDP documentation is in compliance with the VSS, version 2002, Volume 2, Sections 2.2 through 2.13. All discrepancies that were encountered during the PCA Document Review to date were provided to ES&S in a series of iterative discrepancy reports for resolution. All PCA Document Review discrepancies must be corrected by ES&S and re-reviewed to ensure that each was fixed per the requirements of the VSS, version 2002, Volume 2, Sections 2.2 through 2.13.

All discrepancies generated to date are included in ***Attachment F1 - Functional and Documentation Discrepancy Report*** as a part of this Certification Test Plan. In addition, all detailed results from the Document Review and all discrepancies will be included in the Certification Test Report.

2.2.1.2 Source Code Review

Source Code Review for the ES&S AutoMark 1.3 certification began in July 2007, and was completed in December of 2007. All discrepancies that were encountered during the PCA Source Code Review to date were provided to ES&S in a series of iterative discrepancy reports for resolution. All PCA Source Code Review discrepancies must be corrected by ES&S and re-reviewed to ensure that each was fixed per the requirements of the VSS, version 2002

All discrepancies generated to date are included in ***Attachment F2 - Source Code Discrepancy Report – PROPRIETARY*** as a part of this Certification Test Plan. In addition, all detailed results from the source code review and all discrepancies will be included in the Certification Test Report.

If errors are encountered during Functional Testing, then additional source code submissions would be expected, and additional source code review would be necessary, as well as closure of any new discrepancies which may result in those reviews.

2.2.1.3 Trusted Build

Trusted Builds were performed at the SysTest Labs office in Denver and ES&S's office in Omaha, NE. The first Trusted Build for the VAT and AIMS was completed September 26, 2007, and it resulted in the Trusted Build platform PC, which was used for Trusted Builds of ES&S AutoMark products, as described under Section 2.1.1 above, on the respective build platforms PCs in order to provide the compiled software and firmware installation packages to be used in the certification testing.

The VAT encountered problems, and a second trusted build was performed on December 14, 2007, on the respective build platform PC.

2.2.1.4 Review of Vendor's Completed Test Cases and Results

SysTest Labs has determined that the initial delivery of the ES&S AutoMark 1.3 voting system TDP test cases and subsequent test results are consistent with the VSS, version 2002. All discrepancies in the test cases and test results that were encountered during the FCA were provided to ES&S in a series of iterative discrepancy reports for resolution. All discrepancies must be corrected by ES&S and re-reviewed to ensure that each was fixed per the requirements of the VSS, version 2002.

For all requirements that were identified as not tested or insufficiently tested, SysTest Labs will extract the election data from ES&S Unity 3.0.1.0, or design and develop tests cases, test data, and test procedures and will add these to SysTest Labs' list of VSTL Test Cases for ES&S AutoMark 1.3 certification test execution.

As determined by the FCA, the following tests will be executed, as part of this Certification Test Plan:

- Operational Status Check
- Readiness Test
- Sampling of ES&S AutoMark 1.3 test cases as described below in Section 4 under Sampling Methodology
- SysTest Labs' GEN01 - General Election test case
- SysTest Labs' GEN02 –Rotation and Straight party test case
- SysTest Labs' GEN02 PA – Pennsylvania Straight Party with Cross Party Endorsement test case
- SysTest Labs' GEN03 – Usability and Accessibility test case
- SysTest Labs' PRI01 - Open Primary test case
- SysTest Labs' PRI01 - Open Primary with Pick a Party/Party Preference test case
- SysTest Labs' PRI02 - Closed Primary test case
- SysTest Labs' Security test case
- SysTest Labs' Accuracy test case

Please see Tables 5, 6 and 7, and **Appendix A – Test Cases** for additional detail on the SysTest Labs test cases.

All discrepancies generated are included in ***Attachment F*** as a part of this Certification Test Plan. In addition, all detailed results from the review of the vendor completed test cases and results and all discrepancies will be included in the Certification Test Report.

2.2.2.2 Review of Ohio and Colorado Voting System Reviews

SysTest Labs will complete an FCA review of the Ohio and Colorado Voting System Reviews. SysTest Labs' FCA review of the Ohio and Colorado Voting System Reviews will result in an addendum to the Certification Test Report that will include the following:

- A summary of the state findings for each system
- How SysTest Labs incorporated (if appropriate) these findings into the test campaign for the ES&S AutoMark 1.3 voting system
- The outcome of any additional testing deemed necessary

2.2.2 Hardware Environmental Analysis of Testing Results

Test reports from previous hardware testing performed by accredited NVLAP or A2LA laboratories were analyzed to determine if the results could be accepted for certification. If the testing met the criteria as defined in 2.1.3 above, it was considered to satisfy the requirements. The equipment is then exempted from specific tests as reflected in the testing matrix in the EMC and Environmental test plans attached to this document.

3 MATERIALS REQUIRED FOR TESTING

3.1 Software/Firmware

Items identified in the table reflect all software and firmware used to perform hardware, software, security, and integrated system tests. Not all items listed below are required to run the ES&S AutoMark 1.3 voting system. However, all items listed were part of the certification test effort. Should a software version modification become necessary, an amended test plan would be produced with the new version under test listed according to ES&S revised Certification Application, which will be submitted by ES&S as appropriate.

Table 3 - Matrix of Required Software/Firmware

Application(s)	Manufacturer	Version	Description
AutoMARK Information Management System (AIMS)	ES&S	1.3.57	The AutoMARK Information Management System (AIMS) is software that manages all of the information required by the AutoMARK Voter Assist Terminal (VAT) for an election. The AIMS process starts with a printed optical scan ballot. In addition to the printed ballot, files produced by ES&S Unity Systems may be imported into AIMS, for ease in loading data into the AutoMARK election database. In lieu of the import procedure, election specific data may be manually entered into AIMS. AIMS writes the election database to a compact flash memory card (FMC). This FMC supplies ballot content information to the VAT.
AutoMARK Voter Assist Terminal (VAT)	ES&S	1.3.2904	The AutoMARK Voter Assist Terminal is ballot marking device utilizing touch screen technology to mark ballots. It is designed to help voters mark their optical scanned ballots when they are visually impaired, physically disabled, or more comfortable reading or hearing instructions and choices in an alternative language. The AutoMARK does not store, count, or tabulate votes.

Table 4 - Matrix of Required COTS Software/Firmware

COTS Application(s)	Manufacturer	Version	Description
Required COTS software for the ES&S 1.3 voting system			
Microsoft Windows	Microsoft Corporation	Windows XP, SP2	COTS software for AIMS
Microsoft Windows	Microsoft Corporation	Windows CE 5.00.16 *Note: pending final approval of applicable RFI, additional versions may apply*	COTS software for VAT
Java2 Runtime Environment SE	Sun Microsystems	1.4.2_03	COTS software for AIMS
Microsoft .NET Compact Framework	Microsoft Corporation	1.03	COTS software for VAT
Scansoft Eloquence Speech Engine	Scansoft	6.1	COTS software for AIMS and VAT
Microsoft .NET Framework	Microsoft Corporation	1.1	COTS software for AIMS
Microsoft Access 2002 Runtime	Microsoft Corporation	10.0.2627.01	COTS software for AIMS
Microsoft SQL Server Desktop Engine (AIMS-SQLS)	Microsoft Corporation	8.00.761	COTS software for AIMS
ALPS TouchPad Driver	ALPS Electric Company	No Vers.	COTS software for AIMS
SQLXML 3.0 SP3	Microsoft Corporation	3.30.3457.0	COTS software for AIMS
SigmaTel AC97 Audio Drivers	SigmaTel	4092	COTS software for AIMS
ATI Display Driver	ATI	7.91.2-030729a-0104C-Dell	COTS Software on the Laptop PC
ATI Software Uninstall Utility	ATI	6.14.10.1005	COTS Software on the Laptop PC
ATI Control Panel	ATI	6.14.10.5028	COTS Software on the Laptop PC
Broadcom Gigabit Integrated Controller	Broadcom	3.61	COTS Software on the Laptop PC
Conexant D480MDC	Conexant	9x modem	COTS Software on the Laptop PC
02Micro Smartcard Driver	02Micro Electronics	2.20.0000	COTS Software on the Laptop PC
Non required COTS software for the ES&S 1.3 voting system			
Dell ResourceCD	Dell	No Vers.	COTS Software on the Laptop PC
Modem Helper	BVRP Software	2.20	COTS Software on the Laptop PC
Quickset	Dell	No Vers.	COTS Software on the Laptop PC

3.2 Equipment (Hardware)

Equipment identified in the table reflects all hardware used to perform hardware, software, security and integrated system tests. Not all items listed below are required to run the ES&S AutoMark 1.3 voting system. However, all items listed were part of this certification test effort. All equipment was provided by ES&S. SysTest Labs staff uploaded all executables and installs on the equipment, while the equipment and Trusted Build executable and installs were under the control of SysTest Labs.

Table 5 - Matrix of Required Hardware

Item	Manufacturer	Model #	Version/Rev	Description
AutoMARK Voter Assist Terminal (VAT) **8 Received (4 each model)**	ES&S	A100 & A200	Hardware v. 1.0 Firmware v. 1.3.2904	AutoMARK Voter Assist Terminal (VAT) is an electronic ballot marking device that allows voters to electronically mark a ballot, by using the touch screen, Braille keypad, or an AT (Assistive Technology) Sip and Puff device and paddles
Dell D600 – Laptop PC	Dell	PP05L	Windows XP Professional 2002, SP2	Used for functional testing of AIMS. Processor 1.60 GHz, 221 MHz, 1.00 GB of RAM
SanDisk ImageMate CF Reader/Writer **2 Received**	SanDisk	SDDR-92	N/A	Used to read/write data to a SanDisk.
Headphones **2 Received**	AVID	FV-060	N/A	A pair of listening devices joined by a band across the top of the head and worn over the ears
VAT ballot trays **6 Received**	ES&S	N/A	N/A	6.3/4", 8.1/2" & 9.3/4"
AT Paddles **2 Received**	M-Wave	N/A	N/A	Assistive Technology device, providing Yes/No paddles for use with physically disabled voters
Sip n Puff **1 Received**	Origin Instruments Corp.	N/A	N/A	Device used by physically disabled voters

Item	Manufacturer	Model #	Version/Rev	Description
Hardware used for Accuracy testing but not part of this certification				
Model 100 scanner **2 Received**	ES&S	M100	HW revision: 1.3.0 FW revision: 5.2.1.0	Optical scanner
Optech III-P Eagle scanner **2 Received**	ES&S	N/A	HW Rev. Level B.03 Firmware v. 128.950825.1229/ 1.50.950906.1000	Optical scanner
Ballot Box **2 Received**	ES&S	N/A	N/A	Used with the M100 and Optech 111P Eagle scanners
Dell Latitude D600 Laptop	Dell	PP05L	Windows XP Professional 2002, SP2	Used for Accuracy testing. Processor 1700 MHz, 592 MHz, 1.00 GB of RAM
Memory Pack – Receiver Programmer **1 Received**	Business Records Corp.	N/A	HW revision: D	Used to read/write media for the Optech scanners.
Eagle Memory Pack	BRC	N/A	HW revision: 1.50	Used for Accuracy test with definition loaded (Optech)
Omni Drive Professional USB **2 Received**	Omni	D707-94	Rev. C1	Used for Accuracy test with definition loaded (M100)

3.3 Test Materials

Items identified in the table reflect all test materials required to perform hardware, software, security and integrated system tests not identified in section 3.1 or 3.2 above. The items noted in this section are primarily consumables required for the testing effort. Some of these may be reused for other testing after being properly prepared, for example, compact flash memory devices that have been erased and/or formatted prior to each use.

Table 6 - Matrix of Test Materials

Item	Provided by	Manufacturer	Details
PCMCIA Cards (with definition loaded)	ES&S	Vikant	PC Cards M100 program media
Eagle Printer Ribbon	ES&S	General Ribbon	Optech III-P scanners
SanDisk CF cards	ES&S	San Disk	256MB
Blank blue paper ballot stock	ES&S	ES&S	15 x 9 3/4 inches
Election Ballots (ovals, arrows, all fill)	ES&S	ES&S	Inches/ballot positions: 11x36, 14x36, 14x48, 17x41, 17x45, 17x60, 19x51, 19x68, 15", 17", 22"
Printer paper rolls	ES&S	M100: NCR Optech III-P: NCR	Optech III-P scanners, M100
Ink Cartridges	ES&S	Hewlett Packard	VAT (inkjet and infrared)
Diapers	ES&S	B&P	VAT

3.4 Deliverable Materials

In addition to the hardware, software and materials identified in sections 3.1, 3.2, and 3.3, ES&S delivered the Technical Data Package documents as part of the ES&S AutoMark 1.3 voting system. Please see ***Attachment A - List of Technical Data Package (TDP) Deliverables*** for a list of these documents.

3.5 Proprietary Data

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

4 TEST SPECIFICATIONS

Testing for compliance to the VSS 2002 will be conducted as listed below. The Test Methods for all tests are provided in **Appendix A – Test Cases**.

4.1 Hardware Configuration and Design

The vendor established the baseline hardware configuration required for testing the ES&S AutoMark 1.3 Voting System. This baseline is shown in Table 5 – Required Hardware and Table 6 – Test Materials. 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 VSS, version 2002 and HAVA.

4.2 Software System Functions

The scope of the tests in the software certification (Vol. 2, Sect. 5) and system-level tests (Vol. 2, Sect. 6) as defined in the VSS, version 2002 include:

- Pre-Certification Test Assessment (Vol. 2, Section A.2), reflecting the Technical Data Package (Vol. 2, Sect. 2) document examination portions of the Physical Configuration Audit and the Functional Configuration Audit

- Physical Configuration Audit (Vol. 2, Sect. 6.6)

    - Establish the software/hardware configuration baseline used in testing
    - Perform a full Source Code Review (Vol.2 Sect. 5.4)
    - Review vendor's functional specification for adequacy or discrepancy
    - Conduct Trusted Build and comparison to the code tested

- Functional Configuration Audit (Vol. 2, Sect. 6.7)

    - Create and issue a Certification Test Plan (Vol. 2, Section A)
    - Review, evaluate, create, and execute Functional Tests (Vol.2. Section A)
    - Initiate System-Level Integration Tests (Vol. 2, Sect. 6)

4.3 Test Case Design

4.3.1 Hardware Qualitative Examination Design

Hardware environmental certification testing is performed to verify conformance to Vol. 1. Section 3 of the FEC VSS April 2002. Specific test plans and test reports from the subcontractor labs are included as Attachments to this document.

The hardware testing will be performed at three subcontract laboratories:

- Emissions Testing will be performed at Criterion Laboratories in Rollinsville, Colorado
- Environmental Testing will be done at Advanced Product Testing (APT) Laboratories in Longmont, Colorado

- Safety Testing will be performed at Compliance Integrity Services (CIS) Laboratories in Longmont, Colorado.

SysTest Labs reviewed the results provided in test reports from the previous testing for overall system capabilities of pre-voting, voting and post-voting functions. The ES&S AutoMark 1.3 voting system hardware is incorporated into the standard set of system-level test cases with the augmentation of validation steps specific to each function (*Vol. 2, Section A.4.3.1*).

Maintainability testing, Accessibility, and Human Engineering Evaluation testing will be performed at SysTest Labs in Denver.

4.3.2 Hardware Environmental Test Case Design

Hardware testing requirements as specified in Vol. 1 Section 3 of the VSS, version 2002 are satisfied through a combination of testing by SysTest Labs and previous testing performed by Wyle Laboratories, (Wyle Laboratories, Inc., 7800 Highway 20 West, Huntsville, Alabama 80806) and Percept Technology Labs (Percept, 4888 Pearl East Cir #110, Boulder, CO 80302).

The previous testing performed by the aforementioned labs was accepted based upon the results documented in test reports provided. The testing by product is defined in Attachment D.

4.3.3 Software Module Test Case Design and Data

SysTest Labs reviews the test case design documents and data as provided by ES&S. 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 test case design. Discrepancies are issued to the vendor for correction, if determined necessary *(Vol. 2, Section A.4.3.3)*.

SysTest Labs designs additional module test cases, as required, to provide coverage of modules containing untested paths with potential for un-trapped errors. SysTest Labs also reviews 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 provides 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 standard relating to unbound arrays, parameter type and range validation, pointer controls, vote counter overflow, etc. The source code review also insures that all source code is in conformance with Volume 1, Section 4.2 and Volume 2, Section 5.4.

If it is determined during source code review that potential risks exist at module entry/exit points, then functional test cases are designed to test these areas, and the results of these tests will be included in the Certification Test Report. 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.

SysTest Labs will include in the Certification Test Report 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.

4.3.4 Software Functional Test Case Design

SysTest Labs has reviewed the ES&S AutoMark 1.3 test cases against the 2002 VSS requirements matrix, in conducting the FCA Document Review, and has evaluated the test cases in light of the vendor's system functionality documents. SysTest Labs has prepared Functional Test cases using the operator/user procedures.

Please see Tables 7 8, and 9, and **Appendix A – Test Cases** for additional detail on the SysTest Labs test cases.

Software Functional Testing will demonstrate that the ES&S AutoMark 1.3 voting system, comprising of the AIMS software and VAT firmware's capabilities, meet the applicable requirements for pre-voting, voting and post-voting functional areas (*Vol. 2, Appendix A.*). Since this testing effort does not include the Unity 3.0.1.0 and 3.0.1.1 voting systems, not all requirements will be met by the ES&S software/hardware components. Please see the functions as defined in Table 7 – Matrix of System Functional Testing.

Table 7 - Matrix of System Functional Testing

Function	Test Methodology
Ballot Preparation Functions	
a. Ballot preparation subsystem	Verify the election is defined for election day. Import, create, and modify election test data in AIMS to create ballot content for the VAT.
Before, During & After Processing of Ballots	
b.1. Logic Test – Interpretation of Ballot Styles & recognition of precincts	Verify in Functional Tests: Verify voting variation functionality identified by ES&S for the ES&S AutoMark 1.3 voting system (Vol. 1. Section 2.2.8.2).
b.2. Accuracy Tests- Ballot recording/reading accuracy	Verify with the processing of 1,549,703 consecutive ballot positions with no errors, or 3,126,404 with one error, on the VAT. (Vol. 2 Section 4.7.1.1).
b.3. Status Tests- Equipment statement & memory contents	Verify in Functional Tests: Equipment statement & memory contents at the corresponding intervals outlined in user documentation for the functions a. b.4, and c 1-7.
b.4. Report Generation – Produce test output data	N/A to AIMS and VAT. (audit logs only are produced.)
b.5. Report Generation- Produce audit data	Verify in Functional Tests: System audit reports voting
Polling Place Functions	
c.1. Opening the polls, accepting & counting ballots	Verify in Functional Tests: Vote ballots as specified in test case VAT accepts and marks paper ballots Alerts for over votes and under votes
c.2. Monitoring equipment status	Verify in Functional Tests: Equipment status as identified in user documentation
c.3. Equipment response to commands	Verify in Functional Tests: Equipment response to all voter and poll worker

Function	Test Methodology
	commands as identified in user documentation
c.4. Generating real-time audit messages	Verify in Functional Tests: Print VAT and AIMS audit logs Each audit message contains a timestamp. Election name, software, and firmware are listed in the audit log for the VAT Count of ballots processed Error messages Ballot ID is on the log for every ballot that is scanned on the VAT
c.5. Closing polls and disabling ballot acceptance	Verify in Functional Tests: N/A for VAT
c.6. Generating election data reports.	Verify in Functional Tests: The VAT does not generate any reports other than an audit log.
c.7. Transfer ballot count to central counting location	Verify in Functional Tests: Manual inspection of ballots to verify that the VAT marked the Voter's selection correctly. (VAT's do not store ballot content.)
c.8. Electronic transmission of election data to central count locations	N/A for VAT
Central Count Functions	
N/A for ES&S AutoMark 1.3 voting system	

4.3.5 Accuracy Test

The Accuracy Test is SysTest Labs' test case for validating a systems ability to accurately read/tally a large number of ballot positions (a minimum of 1,549,703 ballot positions, or 3,126,404 with one error, per Volume 2, Section 4.7.1.1). ES&S AutoMark 1.3 components subject to the Accuracy Test include:

- VAT models A100 and A200, with hardware v. 1.0 and firmware v. 1.3.2904.

The following steps are utilized in the execution of the Accuracy Test:

- Election/ballot definition is created in ES&S's Election Data Manager, and imported into AIMS.
- Ballot definition data is loaded onto the device being tested via a Compact Flash Card
- Report of the initialization process
- Display the function selections
- Open polls (N/A for the VAT)
- Zero Report (N/A for the VAT)
- Execute votes (if a touchscreen or VAT device is being tested), Scan ballots, and print audit logs
- Validate test results

4.3.6 Security Test

The Security Test Case is SysTest Labs' test case for verifying that a voting system will correspond correctly with security tests based on VSS Volume 1, Section 6. It incorporates systems security provisions, unauthorized access, deletion or modification of data, audit trail data, and modification or elimination of security mechanisms. The vendor documentation will be reviewed to ensure sufficient detail is present to operate the voting system in a secured implementation. Where the vendor statements assert the voting system is secured via mechanisms and seals, procedures will test the presence and effectiveness of such controls.

In its security testing SysTest identifies the specific threats that are tested for and the associated risk if a flaw or exception is identified in a voting system. The tests used by SysTest Labs are designed to insure that the voting system meets or exceeds the requirements in the VSS and any instance where an anomaly or possible security flaw is identified, the potential risk is reported and evaluated.

For additional detail, please also refer to the Security Test Case in **Appendix A – Test Cases.**

4.3.7 System Level Test Case Design

System level tests shall be performed on the ES&S AutoMark 1.3 voting system for the purpose of assessing the response of the software to a range of conditions. Paper ballots will be used in all test cases.

The customized test cases for all system level tests are listed in Tables 5, 6 and 7, and **Appendix A – Test Cases**.

In addition, other Functional Tests are used for validating functionality that does not fit well into a system level test cases, e.g., may have too many options to be adequately covered in system level test cases. Tables 8 and 9 provide information that delineates both the system level and the other software functions to be tested and how they will be tested.

Table 8 - Matrix of System Level and Other Functional Testing

Other Functional Testing	Test Methodology
Volume Test	
System's response to processing more than the expected number of ballots/voters per precinct, to processing more than the expected number of precincts, or to any other similar conditions that tend to overload the system's capacity to process, store, and report data.	Accuracy Test Case (described previously in this section)
Stress Tests	
System's responses to transient overload conditions. Subject polling place devices to ballot processing at the high volume rates, evaluate software response to hardware-generated interrupts and wait states.	Hardware is tested to limits outside the range of 'normal' but within specifications for the units.
Usability Tests	
Responses to input, text syntax, error message content, and audit message input	All System-Level Test Cases
Accessibility Test	
Exercises system capabilities of voters with disability features	System-Level Test Case GEN 03
Security Test	
Exercises systems security provisions, unauthorized access, deletion or modification of data, audit trail data, and modification or elimination of security mechanisms.	Security Test case for each component (described previously in this section)
Telecommunications Test	
Exercises telecommunications, maintaining data integrity, protection against external threats, monitoring and responding to external threats, shared operating environment, incomplete election returns, and use of public communications networks.	N/A as the VAT does not telecommunicate
Performance Tests	
Tests accuracy, processing rate, ballot format, handling capability and other performance attributes claimed by vendor.	All System-Level Test Cases
Recovery Tests	
Exercise system's ability to recover from hardware and data errors.	Security Test Case

4.3.8 Sampling Methodology

As part of the FCA Document Review, SysTest Labs reviewed the ES&S test case documents as provided in the TDP against the 2002 VSS requirements matrix. SysTest Labs took a sampling of ES&S' test cases according to the guideline below.

New System (new or never certified by the EAC):

- Review all vendor test cases and select tests from high-risk areas for sampling, such as:
    - Security
    - Audit log
    - Tabulating
    - Transmitting (telecomm, LAN, etc.)
    - Accuracy
    - Additional Voting System functionality

SysTest Labs chose the following test cases:

- Name: 6. System Security Test Cases (VAT)
- Name: R. Password Properties Edit Test Case (AIMS)

  (For more information on the sample tests, see Table 9)

4.3.9 Additional Functional Testing

SysTest Labs' deemed it necessary to execute additional functional test cases. These test cases are detailed below, along with more information on the Sampling test cases chosen. Also, see ***Attachment E - ES&S AutoMark 1.3 Test Case Matrix,*** for an outline of functionality being tested in each test case.

Table 9 - Matrix of Additional Testing

Test Case#	Test Case	Execution
N/A	Hi Capacity Ballot Test, 11X36 Oval ballot	Using an all fill ballot definition (all left and right ballot positions utilized) vote the first and last ballot position in all contests on the 11X36 ballot (6 contest w/35 candidates). Hand tally ballots.
N/A	Hi Capacity Ballot Test, 14X36 Oval ballot	Using an all fill ballot definition (all left and right ballot positions utilized) vote the first and last ballot position in all contests on the 14X36 ballot (6 contest w/35 candidates). Hand tally ballots.
N/A	Hi Capacity Ballot Test, 14X48 Oval ballot	Using an all fill ballot definition (all left and right ballot positions utilized) vote the first and last ballot position in all contests on the 14X48 ballot (6 contest w/47 candidates). Hand tally ballots.
N/A	Hi Capacity Ballot Test, 17X41 Oval ballot	Using an all fill ballot definition (all left ballot positions utilized) vote the first and last ballot position in all contests on the 17X41 ballot (6 contest w/40 candidates). Hand tally ballots.
N/A	Hi Capacity Ballot Test, 17X45 Oval ballot	Using an all fill ballot definition (all left and right ballot positions utilized) vote the first and last ballot position in all contests on the 17X45 ballot (6 contest w/44 candidates). Hand tally ballots.
N/A	Hi Capacity Ballot Test, 17X60 Oval ballot	Using an all fill ballot definition (all left and right ballot positions utilized) vote the first and last ballot position in all contests on the 17X60 ballot (6 contest w/59 candidates). Hand tally ballots.
N/A	Hi Capacity Ballot Test, 19X51 Oval ballot	Using an all fill ballot definition (all left and right ballot positions utilized) vote the first and last ballot position in all contests on the 19X51 ballot (6 contest w/50 candidates). Hand tally ballots.
N/A	Hi Capacity Ballot Test, 19X68 Oval ballot	Using an all fill ballot definition (all left and right ballot positions utilized) vote the first and last ballot position in all contests on the 19X68 ballot (6 contest w/67 candidates). Hand tally ballots.
N/A	Hi Capacity Ballot Test, 15 inch Arrow ballots	Using an all fill ballot definition (all left and right ballot positions utilized) vote the first and last ballot position in all contests on the 15inch ballots. (1 Column ballot with 2 contests: 1 w/32 candidates, 1 w/34 candidates;2 Column ballot w/4 contests: 2 w/32 candidates, 2 w/34 candidates;3 Column ballot with 6 contests: 3 w/32 candidates, 3 w/34 candidates). Hand tally ballots.
N/A	Hi Capacity Ballot Test, 17 inch Arrow ballots	Using an all fill ballot definition (only 3 column right and left ballot positions supported.) vote the first and last ballot position in all contests on the 17inch ballots. 3 Column ballot with 6 contests: 3 w/38 candidates, 3 w/40 candidates). Hand tally ballots.
N/A	Hi Capacity Ballot Test, 22 inch ballots	Using an all fill ballot definition (only 3 column right and left ballot positions supported.) vote the first and last ballot position in all contests on the 22inch ballots. (3 Column ballot with 6 contests: 3 w/ 53 candidates, 3 w/55 candidates). Hand tally ballots.
6	System Security Test Cases (VAT)	This test case verifies the compact flash memory card operations.
R	Password Properties Edit Test Case (AIMS)	This test case verifies the machine's ability to properly edit the system password.

4.4 EAC Interpretations

The test engagement described in this Certification Test Plan utilizes only standard VSTL test methods that conform to the EAC Testing and Certification Program Manual and the appropriate voting system standard. Additional EAC interpretations affect the test plan and test methodology and if used are noted below.

The Certification Test Plan and the execution of tests for the ES&S AutoMark 1.3 voting system identified in this plan do not include any EAC interpretations.

5 TEST DATA

5.1 Data Recording

The FEC Voting System Standards, Volume 2 Test Standards, will be used to measure certification-testing progress against the standards defined for all systems. SysTest Labs will create forms for the source code, TDP, and testing reviews. They will be stored in electronic format at SysTest Labs. SysTest Labs will record all activity via status report E-mails to the voting system vendor.

The testing process involves the assessment of:

- Operational accuracy in the recording and processing of voting data, as measured by the error rate articulated in Volume I, Section 3.

- Operational failure or the number of unrecoverable failures under conditions simulating the intended storage, operation, transportation, and maintenance environments for voting systems, using an actual time-based period of processing test ballots.

- System performance and function under normal and abnormal conditions.

- Completeness and accuracy of the system documentation and configuration management records to enable purchasing jurisdictions to effectively install, test, and operate the system.

5.2 Test Data Criteria

SysTest Labs evaluates test results against the documents and software provided by the vendor. These documents shall be used to customize a standard set of system level tests. Testing will be conducted as an independent verification and validation across the entire voting system. A greater depth of testing will be given to places where there are code changes and changes to documentation. In the standard system level tests, elections are customized to the functionality supported by the ES&S AutoMark 1.3 voting system as identified by the vendor. System performance shall be measured against a predicted result.

5.3 Test Data Reduction

SysTest Labs processes the test data by manually recording data in the Test Case records.

6 TEST PROCEDURE AND CONDITIONS

6.1 Facility Requirements

Testing will be performed on site at SysTest Labs in Denver, Colorado. All TDP and test documentation is stored in the secure project directory on SysTest Labs' secure Voting Server. All TDP and test documentation is stored on site at SysTest Labs' facility in a secure project directory on SysTest Labs' secure Voting server.

SysTest Labs always ensures voting room doors are kept locked at all times, unless the current activity requires that the door be opened. Vendors are never left unattended in a voting room at any time.

Environmental hardware testing for hardware components of the ES&S AutoMark 1.3 voting system will be performed at either NVLAP or A2LA accredited testing laboratories or at laboratories audited by SysTest Labs to NVLAP Handbook 150-22 requirements.

6.2 Test Setup

The ES&S AutoMark 1.3 voting system test platform will be set up, as part of the Physical Configuration Audit, in the standard configuration identified in the vendor TDP documents listed in ***Attachment A - List of Technical Data Package (TDP) Deliverables.*** The software will be installed, versions verified, and made operational. The hardware will also be set up and versions verified according to the vendor TDP documents. Once the hardware and software have been set up, SysTest Labs will proceed with testing the system.

6.3 Test Sequence

While there is no required sequence for performing voting system certification testing and audits, there are prerequisite tasks for some testing. Tasks and any applicable predecessor tasks are identified in the table below.

Table 10 - Matrix of Testing Tasks

Certification Task	Prerequisite Task
Scope Definition	Ascertain previous certification information for the voting system, if applicable
PCA – Review of Source Code and Document TDPs	Receipt of TDPs
FCA – Testing Requirements Determined	Submissions of TDPs by vendor (including QA and testing specifics)
EAC Certification Test Plan	Review of TDPs and vendor testing
FCA – Test Case Development	Documentation TDP review; mapping of test requirements to VSS and vendor testing (or identified risk areas where additional testing is needed)
PCA – System Configuration Audit	Equipment received at SysTest and documentation available

Certification Task	Prerequisite Task
Trusted Build	Completion of PCA source code review
FCA Hardware Environmental Testing	Completion of FCA test case preparation and PCA system configuration audit
FCA Accuracy Testing	Completion of FCA test case preparation, PCA system configuration audit, and environmental testing
FCA Functional Testing	Completion of FCA test case preparation and PCA system configuration audit
FCA System Level Testing	Completion of FCA test case preparation and PCA system configuration audit
FCA Security Testing	Completion of FCA test case preparation and PCA system configuration audit
Reporting Discrepancies	Completion of initial PCA source code and documentation reviews, and system level testing
Regression and Discrepancy Testing	Receipt of applicable discrepancy fix (source code, documentation, hardware, firmware) or vendor response
EAC Certification Test Report	Successful completion of all certification tasks

6.4 Test Operations Procedures

The SysTest Labs VSTL Test Team will provide step-by-step procedures for each test case to be conducted. Each step shall be assigned a test step number; this number, along with critical test data and test procedures information, shall be tabulated onto a test report form for test control and the recording of test results.

An inventory will be performed to verify the voting equipment received contains hardware and software elements as defined in the TDP prior to commencement of Functional or System Level testing.

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

Throughout the testing effort, test procedures 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 failure 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 certification 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 **Reject**, **NT**, and **NA** will include comments by the Tester explaining the reason for the result.

Issues encountered during review and testing will be documented on the Discrepancy Report. Issues that do not conform to the requirements of the VSS, version 2002 will be marked as **Documentation Discrepancies** or **Functional Discrepancies** (a discrepancy occurs when the software does not meet defined software requirements or specifications.).

The vendor must address all documentation and functional discrepancies prior to issuance of the Certification Test Report. Issues that are encountered during testing or documentation review, but are not addressed by the applicable standard will be added to the Discrepancy report and noted as **Informational**. The vendor has the option whether to address Informational issues. All responses provided by the vendor are noted in the Discrepancy Report attachment to the Certification Test Report.

6.5 Test Error Recovery

SysTest Labs verifies that the voting system can recover from a non-catastrophic failure of a device, or from any error or malfunction that is within the operator's ability to correct.

When an error occurs, the vendor’s documentation is followed to Restore, Resume and Recover from the error condition. In the case that this is not possible, a discrepancy is written and provided to the vendor.

Appendix A – Test Cases

Test Detail	Test Methodology
	(Election Core definition)
NOTE	*This Election Core definition is **always** to be used in conjunction with a specific test case. All base requirements are defined here for validating election testing. For specific testing variations, see the following test cases that incorporate this **Election Core**.* ***It is to be noted that not all of the following requirements are applicable for this Certification due to the fact that this is NOT an end-to-end Voting System.***
Scope	A system level test that uses The 2002 Voting System Standards (VSS) guidelines to validate required functionality and performance. Testing includes accuracy, ballot format handling capability, reporting, and usability of the hardware, software and procedures in the entire voting system.
Objective	*Refer to each test case for specific **Objectives**.*
Standards Documents	Voting System Standards 2002, vol. 1 Voting System Standards 2002, vol. 2 Specific standards are noted in following steps.
Variables: **Voting Variations**	The vendor's TDP documents specifically identify which Voting Variations *can* and *cannot* be supported by the system. The documents are reviewed and evaluated. The supported items are verified in one or more election test case. The following are the items specified in the VSS: (V1:2.2.8.2) • Closed primaries • Open primaries • Partisan offices • Non-partisan offices • Write-in voting • Primary presidential delegation nominations • Ballot rotation • Straight party voting • Cross-party endorsement • Split precincts • Vote for N of M • Recall issues, with options • Cumulative voting • Ranked order voting • Provisional or challenged ballots *Refer to each test case for the election specific **Voting Variations**.*

Test Detail	Test Methodology
	(Election Core definition)
Variables: Election Variations	*Refer to each test case for specific **Election Variations**.*
A description of the voting system type and the operational environment	*Refer to each test case for specific **System Types and Environments**.* Additionally, refer to the following tables for complete descriptions: ➢ Matrix of Required Software/Firmware ➢ Matrix of Required Hardware
Pre-requisites and initialization of the test case	Vendor documentation is reviewed, evaluated and used to define the election to be loaded in the Election Management System (EMS) for this test case. This definition is dependent on the supported requirements by the vendor. The EMS is used to prepare ballots and programs for use in casting and counting votes, and to consolidate, report, and display election results. The EMS is validated to ensure that it generates and maintains a database, or one or more interactive databases, that enables election officials or their designees to perform the following functions: • Define political subdivision boundaries and multiple election districts as indicated in the system documentation • Identify contests, candidates, and issues • Define ballot formats and appropriate voting options • Generate ballots and election-specific programs for vote recording and vote counting equipment • Install ballots and election-specific programs • Test that ballots and programs have been properly prepared and installed • Accumulate vote totals at multiple reporting levels as indicated in the system documentation • Generate the post-voting reports required by Section 2.5 • Process and produce audit reports of the data indicated in Section 4.5 (V1: 2.2.6) Election programming is created utilizing the standards to verify that the voting system: • Logically defines the ballot, including the definition of the number of allowable choices for each office and candidate • Logically defines political and administrative subdivisions, where the list of candidates or contests varies between polling places • Excludes of any contest on the ballot in which the voter is prohibited from casting a ballot because of place of residence, or other geographical criteria • Provides ability to select from a range of voting options to conform to the laws of the jurisdiction in which the system will be used • Generates all required master and distributed copies of the voting program, in conformance with the definition of the ballots for each voting device and polling place, and for each tabulating device (V1: 2.3.2) Validation is performed on each device that tabulates ballots ensuring that a ballot counter: • Can be set to zero before any ballots are submitted for tally

Test Detail	Test Methodology (Election Core definition)
	• Records the number of ballots cast during a particular test cycle or election • Increases the count only by the input of a ballot • Prevents or disables the resetting of the counter by any person other than authorized persons at authorized points • Is visible to designated election officials (V1: 2.2.9) Additionally, verification is done to ensure that Ballot boxes and ballot transfer boxes, which serve as secure containers for the storage and transportation of voted ballots, adhere to standards. (V1:3.2.4.2.6) For each iteration that the election is run: • All supplies necessary for testing are retrieved. • Verification is performed on the System to ensure that the correct versions of software, firmware and hardware, election and ballot is installed and set up as defined in the user documentation • A supervisory level access 'user' and password' is created or available • The Readiness Check List is completed if applicable • The date and tester(s) are documented Testers are informed that the test environment must remain static, if not, no changes shall occur without documentation in the test record and the authorization of the project manager.
Documentation: **Test Data & Test Results**	For each iteration that the election is run: • Capture all voting steps in order to maintain repeatability of the test • Record election, ballot, and vote data fields on the corresponding worksheet tabs • Save all worksheet tabs for all iterations of the test case • Record results of test run by entering 'Accept/Reject' on the Test Results Matrix • Provide comments when observing deviations, discrepancies or notable observations • Log discrepancies on the Discrepancy Report
Pre-vote: **Ballot Preparation procedures verifications**	Verification of Common standards includes the following and ensures that the system: • Enables the automatic formatting of ballots in accordance with the requirements for offices, candidates, and measures qualified to be placed on the ballot for each political subdivision and district • Collects and maintains data pertaining to offices and their associated labels and instructions, candidate names and their associated labels, and issues and measures and their associated text • Supports the maximum number of potentially active voting positions as indicated in vendor documentation • For Primary Elections, generates ballots that segregate the choices in partisan races by party affiliation • Generates ballots that contain identifying codes or marks uniquely associated with each new format • Ensures the vote response fields, selection buttons, or switches properly align with the specific candidate names and/or issues printed or displayed on the

Test Detail	Test Methodology
	(Election Core definition)
Pre-vote: **Ballot Preparation procedures verifications (cont.)**	ballot (V1: 2.3.1.1.1) Verification of Paper-Based systems ensures that the system: • Enables voters to make selections by marking a mark in areas designated for this purpose • For marksense systems, ensures that the timing marks align properly with the vote response fields (V1: 2.3.1.1.2) Verification of Ballot Production common standards ensures that: • The electronic display or paper ballot is capable of rendering an image of the ballot in any of the languages required by The Voting Rights Act of 1965, as amended, and as supported by the vendor • The electronic display or paper ballot does not show any advertising or commercial logos unless specifically provided for in State law. Electronic displays shall not provide connection to such material through a hyperlink • The ballot conforms to the vendor specifications for type of paper stock, weight, size, shape used to record votes, folding, bleed through, and ink for printing if paper ballots are used as part of the voting system (V1: 2.3.1.3, 2.3.1.3.1) For paper based recording, verification is performed to ensure the following: • A ballot can be accurately/securely defined and formatted (V1: 3.2.4.2) • A ballot can be accurately/securely programmed and installed into the appropriate media (V1:3.2.4.2.5) • The system Ignores, and extraneous perforations, smudges, and folds (V1:3.2.5.2.b) During the election definition and ballot preparation process, verification is performed to ensure that the system audits the preparation of the baseline ballot formats and modifications to them, a description of these modifications, and corresponding dates. The log is to include: • The allowable number of selections for an office or issue • The combinations of voting patterns permitted or required by the jurisdiction • The inclusion or exclusion of offices or issues as the result of multiple districting within the polling place • Any other characteristics that may be peculiar to the jurisdiction, the election, or the polling place's location • Manual data maintained by election personnel • Samples of all final ballot formats • Ballot preparation edit listings (V1: 4.4.1) Verification of Ballot Formatting ensures that the system supports: • Creation of newly defined elections • Rapid and error-free definition of elections and associated ballot layouts • Uniform allocation of space and fonts, ensuring no perception of a preferred

Test Detail	Test Methodology
	(Election Core definition)
	contest/candidate • Simultaneous display of the maximum number of choices for a contest • Retention of previously defined formats for an election • Prevention of unauthorized modification of any ballot formats • Modifications by authorized personnel of a previously defined ballot format (V1: 2.3.1.2)
Pre-vote: **Preparation - Security**	System Preparation - Security: • System username/password authentication and other access controls are set up according to system documentation guidelines for all devices being tested. • Any/all unnecessary processes are disabled and/or required process control measures noted in the documentation are followed. • All COTS and vendor subsystems used for system security are configured and active as recommended by the system documentation. This includes all connection, port, virus, and data or authorized process restriction systems. • Any other pre-election system security measures listed in the documentation are followed including setup of additional hardware or software not covered above. Please also see the Documentation section of the Security Test Case within Appendix A.
Readiness Testing and Poll Verification	Verification of Common Standards for Readiness Testing ensures that: • Voting machines or vote recording and data processing equipment, precinct and central count equipment are properly prepared for an election, and collect data that verifies equipment readiness • Status and data reports from each set of equipment can be obtained • The correct installation and interface of all system equipment • Hardware and software function correctly • Consolidated data reports at the polling place and higher jurisdictional levels can be generated • There is Segregation of test data from actual voting data, either procedurally or by hardware/software features When resident test software, external devices, and special purpose test software may be connected or installed in the voting device to simulate operator and voter functions provided the following standards are verified to ensure that: • These elements are capable of being tested separately, and shall be proven to be reliable verification tools prior to their use • These elements are incapable of altering or introducing any residual effect on the intended operation of the voting device during any succeeding test and operational phase (V1: 2.3.4, 2.3.4.1) Vendor documentation is reviewed, evaluated and used to create steps that ensure all voting systems and equipment function properly before and during an election. Verification of these steps provide a formal record of the following: (V1:2.3.5) • The election's identification data • The identification of all equipment units • The identification of the polling place • The identification of all ballot formats

Test Detail	Test Methodology
	(Election Core definition)
	• The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain only zeros) • A list of all ballot fields that can be used to invoke special voting options • Other information needed to confirm the readiness of the equipment, and to accommodate administrative reporting requirements To prepare voting devices to accept voted ballots, all voting systems are verified to ensure that they provide the capability to test each device prior to opening. This verifies that each is operating correctly. The tests include: • Confirmation that there are no hardware or software failures • Confirm that the device is ready to be activated for accepting votes • Confirmation that the test data is separate from voting data without impact to the testing Prior to Opening the polls, verification at the Central Location is performed to ensure that vote counting and vote consolidation equipment and software function properly. Any system used in a central count environment provides a printed record of the following: (V1:2.3.6) • The election's identification data • The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain all zeros) • Other information needed to ensure the readiness of the equipment and to accommodate administrative reporting requirements Verification is performed to ensure the following: • A list of all ballot fields is created (V1: 3.2.4.2.1) • The voting device is ready to accept votes (V1:3.2.4.3.1)
Voting: **Opening the Polls Verification**	Verification of the Readiness checklist is performed, ensuring that it is complete. Vendor documentation is reviewed, evaluated and used to create steps that ensure all voting systems and equipment perform voting functions properly. These steps are created using the guidelines listed in VSS volume 1, section 2.4. Verification of these steps provide a formal record of the following: • Opening the polls • Casting a ballot Additionally, verification ensures that all DRE systems support: o Activating the ballot o Augmenting the election counter o Augmenting the life-cycle counter If necessary, any issues, failures, or unexpected results and their required corrective action(s) are identified and recorded here. (V1: 2.4) Verification of Opening Polls for Precinct Count Systems (paper based) ensures: • An internal test of diagnostic capability to verify that all of the polling place

Test Detail	Test Methodology
	(Election Core definition)
Voting: **Opening the Polls Verification (cont.)**	tests specified in section 2.3.5 have been successfully completed • Automatic disabling any device that has not been tested until it has been tested. (V1:2.4.1.1) • A means of verifying that ballot marking devices are properly prepared and ready for use • A voting booth or similar facility, in which the voter may mark the ballot in secrecy • Secure receptacles for holding voted ballots (V1: 2.4.1.2.1) • Activating the ballot counting device • Verifying the device has been correctly activated and is functioning properly • Identifying device failure and corrective action needed (V1: 2.4.1.2.2) Verification of Opening Polls for Precinct Count Systems (DRE) ensures that: • A security seal, password, or a data code recognition capability to prevent the inadvertent or unauthorized actuation of the poll-opening function • A means of enforcing the execution of steps in the proper sequence • A means of verifying the system as been activated correctly • A means of identifying system failure and any corrective action needed (V1: 2.4.1.3) Verification of Activating the Ballot (DRE) ensures that the system: • Enables election officials to control the content of the ballot presented to the voter, whether presented in printed form or electronic display, such that each voter is permitted to record votes only in contests in which that voter is authorized to vote • Allows each eligible voter to cast a ballot • Prevents a voter from casting more than one ballot in the same election • Activates the casting of a ballot in a general election • Enables the selection of the ballot that is appropriate to the party affiliation declared by the voter in a primary election • Activates all portions of the ballot upon which the voter is entitled to vote • Disables all portions of the ballot upon which the voter is not entitled to vote (V1: 2.4.2) Verification of Casting a Ballot Common Standards ensures that the system: • Verifies that additional functional capabilities that enable accessibility to disabled voters as defined in Section 2.2.7 (V1: 2.4.3) • Provides text that is at least 3mm high and provide the capability to adjust or magnify the text to an apparent size of 6.3 mm • Protects the secrecy of the vote such that the system cannot reveal any information about how a particular voter voted, except as otherwise required by individual State law • Records the selection and non-selection of individual vote choices for each contest and ballot measure • Records the voter's selection of candidates whose names do not appear on the ballot, if permitted under State law, and record as many write-in votes as the number of candidates the voter is allowed to select • In the event of a failure of the main power supply external to the voting system, provides the capability for any voter who is voting at the time to complete casting a ballot, allow for the graceful shutdown of the voting system without loss or degradation of the voting and audit data, and allow voters to resume

Test Detail	Test Methodology
	(Election Core definition)
Voting: **Opening the Polls Verification (cont.)**	voting once the voting system has reverted to back-up power; and • Provides the capability for voters to continue casting ballots in the event of a failure of a telecommunications connection within the polling place or between the polling place and any other location. (V1: 2.4.3.1) Verification is performed to ensure that the system: • Allows the voter to easily identify the voting field that is associated with each candidate or ballot measure response • Allows the voter to punch or mark the ballot to register a vote • Allows either the voter or the appropriate election official to place the voted ballot into the ballot counting device (for precinct count systems) or into a secure receptacle (for central count systems) • Protects the secrecy of the vote throughout the process. (V1: 2.4.3.2.1) • Provides feedback to the voter that identifies specific contests or ballot issues for which an overvote or undervote is detected • Allows the voter, at the voter's choice, to vote a new ballot or submit the ballot 'as is' without correction • Allows an authorized election official to turn off the capabilities defined above (V1: 2.4.3.2.2) Additionally, verification is performed to ensure that all DRE systems: • Prohibit the voter from accessing or viewing any information on the display screen that has not been authorized by election officials and preprogrammed into the voting system (i.e., no potential for display of external information or linking to other information sources) • Enable the voter to easily identify the selection button or switch, or the active area of the ballot display that is associated with each candidate or ballot measure response • Allow the voter to select his or her preferences on the ballot in any legal number and combination • Indicate that a selection has been made or canceled • Indicate to the voter when no selection, or an insufficient number of selections, has been made in a contest • Prevent the voter from overvoting • Notify the voter when the selection of candidates and measures is completed • Allow the voter, before the ballot is cast, to review his or her choices and, if the voter desires, to delete or change his or her choices before the ballot is cast • For electronic image displays, prompt the voter to confirm the voter's choices before casting his or her ballot, signifying to the voter that casting the ballot is irrevocable and directing the voter to confirm the voter's intention to cast the ballot • Notify the voter after the vote has been stored successfully that the ballot has been cast • Notify the voter that the ballot has not been cast successfully if it is not stored successfully, including storage of the ballot image, and provide clear instruction as to the steps the voter should take to cast his or her ballot should this event occur

Test Detail	Test Methodology
	(Election Core definition)
	• Provide sufficient computational performance to provide responses back to each voter entry in no more than three seconds • Ensure that the votes stored accurately represent the actual votes cast • Prevent modification of the voter's vote after the ballot is cast; • Provide a capability to retrieve ballot images in a form readable by humans (in accordance with the requirements of Section 2.2.2.2 and 2.2.4.2) • Increment the proper ballot position registers or counters • Protect the secrecy of the vote throughout the voting process • Prohibit access to voted ballots until after the close of polls • Provide the ability for election officials to submit test ballots for use in verifying the end-to-end integrity of the system • Isolate test ballots such that they are accounted for accurately in vote counts and are not reflect in official vote counts for specific candidates or measures (V1: 2.4.3.3)
Voting: **Required functionality verifications**	Vendor documentation is reviewed, evaluated and used to create Vote Data or the test 'voters' for this test case. This Vote Data is created in matrix form and is used to ensure vote accuracy based on common standards listed in VSS volume 1, section 2.2.2.1. Each 'voter' in the Vote Data Matrix votes the ballot. A SysTest employee performs this manually. The different combinations of candidates selected by each voter in the Vote Data Matrix validates the system's ability to: • Record the election precincts/splits, contests, candidates, and issues exactly as defined by election officials • Record the appropriate options for ballot content, verifying the appropriate contests/issues are displayed as determined in election creation • Record the appropriate options for casting and recording votes across a range of voting options • Record each vote precisely as indicated by the voter and be able to produce an accurate report of all votes cast • Include control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) to demonstrate that the system has been designed for accuracy • Provide software that monitors the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected The process for casting a ballot is defined in detail in individual test case steps. These cases, steps, and verification criteria are created using the requirements stated in the VSS volume 1, section 2.4.3 and section 4.5. Additionally, the Vendor documentation is evaluated and used to enhance the testing procedures. The standards used for validation consist of the following sections: • Common Standards (V1:2.4.3.1) • Paper-Based Systems Standards (V1:2.4.3.2) • DRE Systems Standards (V1:2.4.3.3) • Vote Secrecy (DRE Systems) (V1:4.5)

Test Detail	Test Methodology
	(Election Core definition)
Voting: **Required functionality verifications (cont.)**	Backup files are made and hard copies printed for all DRE systems to record and retain redundant copies of the original ballot image (V1: 2.2.2.2, 2.2.4.2) System auditing and functional testing is performed in order to validate vote data, prescient counts, central counts, audit records and error logs. Verification is performed on the error logs based on the standards listed in the VSS volume 1 section 2.2.5. The test ballots are design with formats and voting patterns sufficient to verify performance of the test election programs. Ballots are cast in a number sufficient to demonstrate proper processing, error handling, and generation of audit data as specified in Volume I, Sections 2 and 4. Test case steps are performed during the Functionality Testing in Parallel with Hardware Testing for Precinct Count Systems to verify voting functions defined in Vol. 1: 2.4 and 2.5 of voting equipment and precinct counting equipment. Verification ensures that: • Preparation of the election programs: o Verify resident firmware, if any o Prepare software (including firmware) to simulate all ballot format and logic options for which the system will be used o Verify program memory device content o Obtain and design test ballots with formats and voting patterns sufficient to verify performance of the test election programs • Procedures to program precinct ballot counters: o Install program and data memory devices, or verify presence if resident o Verify operational status of hardware • Procedures to simulate opening of the polls: o Perform procedures required to prepare hardware for election operations o Obtain a zero report or other evidence that data memory has been cleared o Verify audit record of pre-election operations o Perform procedures required to open the polling place and enable ballot counting • Procedures to simulate counting ballots cast test ballots in a number sufficient to demonstrate proper processing, error handling, and generation of audit data • Procedures to simulate closing of polls: o Perform hardware operations required to disable ballot counting and close polls o Obtain data reports and verify correctness o Obtain audit log and verify correctness (V2: 3.3, 3.3.1) Test case steps are performed during the Functionality Testing in Parallel with Hardware Testing for Central Count Systems to verify voting functions defined in Vol. 1: 2.4 and 2.5. Verification ensures that: • Procedures to prepare election programs: o Verify resident firmware, if any o Prepare software (including firmware) to simulate all ballot format and logic options for which the system will be used, and to enable

Test Detail	Test Methodology
	(Election Core definition)
Voting: **Required functionality verifications (cont.)**	simulation of counting ballots from at least 10 polling places or precincts o Verify program memory device content o Procure test ballots with formats, voting patterns, and format identifications sufficient to verify performance of the test election programs • Procedures to simulate counting ballots count test ballots in a number sufficient to demonstrate proper processing, error handling and generation of audit data as specified in Vol. 1, Section 2 and 4. • Procedures to simulate election reports: o Obtain reports at polling places or precinct level o Obtain consolidated reports o Provide query access, if this is a feature of the system o Verify correctness of all reports and queries Obtain audit log and verify correctness (V2: 3.3.2) Integrity measures ensure the physical stability and function of the vote recording and counting processes. Verification is performed to ensure that both Common Standards and DRE Systems Standards are followed. (V1:2.2.4) Common Standards are used to ensure system integrity by validating that the voting system: (2.2.4.1) • Protects, by a means compatible with these Standards, against a single point of failure that would prevent further voting at the polling place • Protects against the interruption of electronic power • Protects against generated or induced electromagnetic radiation • Protects against ambient temperature and humidity fluctuations • Protects against the failure of any data input or storage device • Protects against any attempt at improper data entry or retrieval • Records and report the date and time of normal and abnormal events • Maintains a permanent record of all original audit data that cannot be modified or overridden but may be augmented by designated authorized officials in order to adjust for errors or omissions (e.g. during the canvassing process.) • Detect and record every event, including the occurrence of an error condition that the system cannot overcome, and time-dependent or programmed events that occur without the intervention of the voter or a polling place operator • Include built-in measurement, self-test, and diagnostic software and hardware for detecting and reporting the system's status and degree of operability DRE Systems Standards are used to ensure system integrity by validating that the voting system: (V1:2.2.4.2) • Maintains a record of each ballot cast using a process and storage location that differs from the main vote detection, interpretation, processing, and reporting path • Provides a capability to retrieve ballot images in a form readable by humans. Audit records are prepared for all testing phases of election operations using devices designed to be controlled by the jurisdiction or its contractors. These records rely upon

Test Detail	Test Methodology
	(Election Core definition)
Voting: **Required functionality verifications (cont.)**	automated audit data acquisition and machine-generated reports, with manual input of some information. These records address the ballot preparation and election definition phase, system readiness tests, and voting and ballot-counting operations. Individual test cases and steps contain instructions on how and when to generate and validate this information. (V1:2.2.5.2, 4.4) All voting systems are evaluated and verified to ensure that they meet the following requirements for time, sequence and preservation of Audit Records: • Except where noted, systems provide the capability to create and maintain a real-time audit record • All systems include a real-time clock as part of the system's hardware • All audit record entries include the time-and-date stamp • The audit record are active whenever the system is in an operating mode • The generation of audit record entries are not terminated or altered by program control, or by the intervention of any person • Once the system has been activated for any function, the system preserves the contents of the audit record during any interruption of power to the system until processing and data reporting have been completed • The system is capable of printing a copy of the audit record (V1:2.2.5.2.1, 3.2.7, 3.2.7.2) All voting systems are evaluated and verified to ensure that they meet the following requirements for Error Messages: • The system generates, stores, and reports to the user all error messages as they occur • All error messages requiring intervention by an operator or precinct official are displayed or printed unambiguously in easily understood language text, or by means of other suitable visual indicators • When the system uses numerical error codes for trained technician maintenance or repair, the text corresponding to the code is self-contained, or affixed inside the unit device • All error messages for which correction impacts vote recording or vote processing are written in a manner that is understandable to an election official who possesses training on system use and operation, but does not possess technical training on system servicing and repair • The message cue for all systems clearly state the action to be performed in the event that voter or operator response is required • System design ensures that erroneous responses will not lead to irreversible error • Nested error conditions are corrected in a controlled sequence such that system status shall be restored to the initial state existing before the first error occurred (V1:2.2.5.2.2) All voting systems are evaluated and verified to ensure that they meet the following requirements for Status Messages: • When the jurisdiction requires, some status and information messages are displayed and reported in real-time • Messages that do not require operator intervention may be stored in memory to be recovered after ballot processing has been completed • The system displays and reports critical status messages using unambiguous indicators or English language text • The system need not display non-critical status messages at the time of occurrence

Test Detail	Test Methodology
	(Election Core definition)
	• Systems may display non-critical status messages (i.e., those that do not require operator intervention) by means of numerical codes for subsequent interpretation and reporting as unambiguous text • Systems provide a capability for the status messages to become part of the real-time audit record • The system provides a capability for a jurisdiction to designate critical status messages (V1:2.2.5.2.3)
Voting: **Required functionality verifications (cont.)**	Exception Handling (Central Count) refers to the handling of ballots for a central count system when they are unreadable or when some condition is detected requiring that the cards be segregated from normally processed ballots for human review. In response to an unreadable ballot or a write-in vote, verification is done to ensure that all central count paper-based systems: (V1:3.2.5.1.2) • Outstack the ballot, or • Stop the ballot reader and display a message prompting the election official or designee to remove the ballot, or • Mark the ballot with an identifying mark to facilitate its later identification. Exception Handling (Precinct Count) refers to the handling of ballots for a precinct count system when they are unreadable or when some condition is detected requiring that the cards be segregated from normally processed ballots for human review. All paper based precinct count systems are validated to ensure that the following can be accomplished: (V1:3.2.5.1.3) • An unreadable or blank ballot - return the ballot and provide a message prompting the voter to examine the ballot • Ballot with a write-in vote - segregate the ballot or mark the ballot with an identifying mark to facilitate its later identification • A ballot with an overvote the system: o Provides a capability to identify an overvoted ballot o Returns the ballot o Provides an indication prompting the voter to examine the ballot; o Allows the voter to submit the ballot with the overvote o Provides a means for an authorized election official to deactivate this capability entirely and by contest • In response to a ballot with an undervote the system: o Provides a capability to identify an undervoted ballot o Returns the ballot o Provides an indication prompting the voter to examine the ballot o Allows the voter to submit the ballot with the undervote o Provides a means for an authorized election official to deactivate this capability Processing speed is verified for DRE voting systems to ensure that they: • Operate at a speed sufficient to respond to any operator and voter input without perceptible delay (no more than three seconds)

Test Detail	Test Methodology
	(Election Core definition)
	• If the consolidation of polling place data is done locally, performs this consolidation in a time not to exceed five minutes for each device in the polling place. (V1: 3.2.6.2.1)
Voting: Optional functionality verifications	The functionality listed above in "**Variables: Voting Variations"** is verified here.
Post-Vote: **Closing the Polls**	Vendor documentation is reviewed, evaluated and used to create steps that ensure that all voting systems and equipment perform voting functions properly for all Post-Voting Functions. These steps are created, using the guidelines listed in VSS volum1, section 2.5. Verification of these steps provide a formal record of the following: • All systems provide capabilities to accumulate and report results for the jurisdiction and to generate audit trails • Precinct count systems provide a means to close the polling place including generating appropriate reports • The standards for closing the polling place are specific to precinct count systems. The system provides the means for: (V1:2.5.1) o Preventing the further casting of ballots once the polling place has closed o Providing an internal test that verifies that the prescribed closing procedure has been followed, and that the device status is normal o Incorporating a visible indication of system status o Producing a diagnostic test record that verifies the sequence of events, and indicates that the extraction of voting data has been activated o Precluding the unauthorized reopening of the polls once the poll closing has been completed for that election • All systems provide a means to consolidate vote data from all polling places, and optionally from other sources such as absentee ballots, provisional ballots, and voted ballots requiring human review (e.g., write-in votes). (V1:2.5.2) • All systems are able to create reports summarizing the data on multiple levels. (V1:2.5.3) • *If applicable*, the voting systems offer the capability to make unofficial results available to external organizations such as the news media, political party officials, and others. Although this capability is not required, systems that make unofficial results available: (V1:2.5.4) o Provide only aggregated results, and not data from individual ballots o Provide no access path from unofficial electronic reports or files to the storage devices for official data o Clearly indicate on each report or file that the results it contains are unofficial
Post-Vote: **Vote Count Verification**	After all voting listed in the Vote Data Matrix is performed, the election data is examined and all counts are validated on the individual voter level, the voting machine level, the precinct level and the central count level. This verification ensures that the system is correctly tabulating all data and is accurately recording cast ballots, including provisional. (V1:2.2.8.1, 2.3.6, 2.5, 3.2.3.1, 3.2.5.2,3.2.6.2.2, 3.2.4.3.3) This tabulation sometimes includes verification of the following:

Test Detail	Test Methodology (Election Core definition)
	• Ensure undervotes are counted as cast votes • Separate accumulation of Undervotes and Paper Overvotes • Ensure Overvotes are counted on paper ballots and tally correctly
Post-Vote: **Security**	Post-Vote - Security: • System username/password authentication and other access controls are set up according to system documentation guidelines for all devices being tested. • Any/all unnecessary processes are disabled and/or required process control measures noted in the documentation are followed. • All COTS and vendor subsystems used for system security are configured and active as recommended by the system documentation. This includes all connection, port, virus, auditing capability, data or authorized process restriction systems. • Any other system security measures listed in the documentation are followed including setup of additional hardware or software not covered above. Please also see the Documentation section of the Security Test Case within Appendix A.
Post-Vote: **System Audit and Data Retention**	All applicable system reports are produced and verified at this point. The requirements listed in the VSS volume 1 are followed for verifying Data and Document Retention. These include the following: • Data and Document Retention (V1:4.3) • Audit Record Data (V1:4.4) Additionally, the guidelines listed in the VSS volume 1, section 3.2.8.2, are used to validate Data Report Generation.
Results are Observed	Review the outcome of the test(s) against the expected result(s): • **Accept**: expected results is observed • **Reject:** expected result is NOT observed • **Not Testable (NT)**: rejection of a previous test step prevents validation of this step or this was tested in another test case • **Not Applicable (NA):** not applicable to the current test scope or to the component under review • **Not Supported (NS)**: not supported in the current test scope
Record Observations and all input/outputs for each election	All information used in processing the test case is captured. This includes: inputs, outputs, deviations and any other item that may impact the validation of the test case. Any failure of the test against the EAC guidelines is reported and implies failure of the system. Failures are reported as Defect Issues in the Discrepancy Report and are provided to the manufacturer. Before the final Certification Test Report is issued, manufacturers are given the opportunity to correct all discrepancies. If the manufacturer submits corrections, retests are performed. Issues that do not impact the failure of the requirements but could be considered defects are logged as Informational Issues on the Discrepancy Report. It is the manufacturer's option to address these issues.

Test Detail	Test Methodology
Test Case Name	**GEN01 - General Election**
NOTE	*This test case is to be used in conjunction with the **Election Core definition**.*
Objective	The objective of this test case is to verify core functional and performance capabilities of the ES&S AutoMark 1.3 system, by using the vendor's manuals to import a general election from the ES&S Unity 3.0.1.0/3.0.1.1 system; vote on paper ballots with ovals in the left position, and arrows in the right position, with both types of ballots being voted on the VAT A100 and A200 models, and tally results for a General Election.
Variables: **Voting Variations**	The following are the items verified in this election. See the remaining election test cases for examples of all voting variations supported by the vendor. (V1:2.2.8.2) • 1 Precinct • Split precincts (3 splits per precinct) • Partisan contest: Grouped candidate slate (1 of *M*) (Governor/Lt. Governor) • Partisan contest: Vote for 1 of *M* with one party having no declared candidate (Secretary of State, Attorney General) • Partisan contest: Multi-member board (3 of *M*) and write-ins (City Council) • Non-Partisan contest: Vote for 1 of *M*, race with no declared candidates and write-ins (Sheriff) • Non-Partisan contest: Vote for 1 of *M*, race with single candidate and write-in (Superintendent of Schools) • Non-Partisan contest: Multi-member board (2 of *M*) (County Commissioner) • Non-Partisan contest: Proposition/Question (Proposition X) • Recall Type A: Simple Yes/No question (Recall Judge) • Recall Type B: Retain/Replace (Replace Judge)
Variables: **Election Variations**	**Governor/Lt. Governor**: 4 candidates **Secretary of State:** 3 candidates (no DEM candidate) **Attorney General**: 3 candidates (no DEM candidate) **Sheriff**: no candidate/write-in **City Council**: 7 candidates/3 write-ins **Superintendent of Schools**: 1 candidate/1 write-in **County Commissioner**: 5 candidates **Proposition X:** Yes/No **Recall Judge (District A):** Yes/No **Replace Judge (District B):** Retain = first option, Replace = second and third options
A description of the voting system type and the operational environment	**Software** • AIMS version 1.3.57 • VAT version 1.3.2904 **Hardware** • Voter Assist Terminal (A100) • Voter Assist Terminal (A200)

Test Detail	Test Methodology
Test Case Name	**GEN02 - Rotation and Straight Party**
NOTE	*This test case is to be used in conjunction with the **Election Core definition**.*
Objective	The objective of this test case is to verify core functional and performance capabilities of the ES&S AutoMark 1.3 system, by using the vendor's manuals to import a general election with rotation and straight party voting, from the ES&S Unity 3.0.1.0/3.0.1.1 system; vote on paper ballots with ovals in the left position, and arrows in the right position, and a two-page ballot with ovals, with all types of ballots being voted on the VAT A100 and A200 models, and tally results.

Variables:
 	
Voting Variations
	The following are the items verified in this election. See the remaining election test cases for examples of all voting variations supported by the vendor. (V1:2.2.8.2)
	
	• 2 Elections
	  o Single page ballot per voter
	  o Multi-page ballot per voter (Precinct 2000 with 3 splits has Sheriff contest on page 2)
	• Straight party (multi-member board)
	• Cross over voting
	
	• 7 Precincts
	• 1 Split precinct (3 splits)
	• Straight party voting contest: Democrat, Republican, Composer, & Scientist
	• Partisan contest: 1 of *M*, declared candidates, no write-ins (Secretary of State, Attorney General)
	• Partisan contest: 2 of *M*, declared candidates, write-ins (City Council, County Commissioner)
	• Partisan contest: 1 of *M*, declared candidates, no Rep candidate, write-ins (Superintendent of Schools)
	• Partisan contest: 1 of *M*, declared candidates, no Com candidate, write-ins (Judge)
	• Non-Partisan contest: 1 of *M*, declared candidates, write-ins (Sheriff)

Variables: **Election Variations**	**Secretary of State:** 4 candidates **Attorney General**: 3 candidates **City Council**: 7 candidates **County Commissioner**: 8 candidates **Sheriff**: 3 candidates **Superintendent of Schools**: 3 candidates **Judge:** 3 candidates
A description of the voting system type and the operational environment	**Software** • AIMS version 1.3.57 • VAT version 1.3.2904 **Hardware** • Voter Assist Terminal (A100) • Voter Assist Terminal (A200)

Test Detail	Test Methodology
Test Case Name	**GEN02 PA – Pennsylvania Straight Party with Cross Party Endorsement**
NOTE	*This test case is to be used in conjunction with the **Election Core definition**.*
Objective	The objective of this test case is to verify core functional and performance capabilities of the ES&S AutoMark 1.3 voting system, by using the vendor's manuals to import a general election with rotation, straight party for PA (Pennsylvania), and cross party endorsement voting, from the ES&S Unity 3.0.1.0/3.0.1.1 system; vote on paper ballots with ovals in the left position, and arrows in the left position, with both types of ballots being voted on the VAT A100 and A200 models, and tally results
Variables: **Voting Variations**	The following are the items verified in this election. See the remaining election test cases for examples of all voting variations supported by the vendor. (V1:2.2.8.2) • Single page ballot election per voter • 7 precincts with 1 split precincts (3 splits) • General PA straight party (multi-member board) and cross party endorsement election. • Straight party voting contest: Democrat, Republican, Composer, & Scientist • Partisan contest: 1 of *M*, declared candidates, no write-ins (Secretary of State) • Partisan contest: 1 of *M*, declared candidates, no SCI candidate, no write-ins (Attorney General) • Partisan contest: 2 of *M*, declared candidates, write-ins, cross-party endorsement (City Council) • Partisan contest: 2 of *M*, declared candidates, write-ins (County Commissioner) • Partisan contest: 1 of *M*, declared candidates, no Rep candidate, write-ins, cross-party endorsement (Superintendent of Schools) • Partisan contest: 1 of *M*, declared candidates, no Com candidate, write-ins, cross-party endorsement (Judge) • Non-Partisan contest: 1 of *M*, declared candidates, no write-ins (Sheriff)
Variables: **Election Variations**	**Secretary of State:** 4 candidates **Attorney General**: 3 candidates **City Council**: 6 candidates **County Commissioner**: 8 candidates **Sheriff**: 3 candidates **Superintendent of Schools**: 2 candidates **Judge:** 2 candidates
A description of the voting system type and the operational environment	**Software** • AIMS version 1.3.57 • VAT version 1.3.2904 **Hardware** • Voter Assist Terminal (A100) • Voter Assist Terminal (A200)

Test Detail	Test Methodology
Test Case Name	**GEN03 - Usability and Accessibility**
NOTE	*This test case is to be used in conjunction with the **Election Core definition**.*
Objective	The object of this test case is to verify core functionality and performance by using vendor manual(s) to create a general election; vote on paper ballots with ovals in the left position, and arrows in the right position, with both types of ballots being voted on the VAT A100 and A200 models, and tally results for a General Election while also testing Usability and Accessibility.
Variables: **Voting Variations**	The following are the items verified in this election. See the remaining election test cases for examples of all voting variations supported by the vendor. (V1:2.2.8.2) • 1 Precinct • Audio/Visual ballots with sip and puff and AT paddles • Template types: Default; Color with zoom; Black/White; Black/White with zoom • Partisan contest (multi-member board): 3 of M, declared candidates, write-ins (City Council) • Non-partisan contest: Yes/No (Proposition X) • Non-partisan contest: Vote for 1 of *M*, declared candidates, no write-ins (Sheriff) Multi-language ballots to be tested include: • English • Spanish • Chinese • Cantonese • Korean • Japanese • Vietnamese • Tagalog
Variables: **Election Variations**	**City Council**: 6 candidates, no REP candidate **Sheriff**: 3 candidates, rotation **Proposition X:** Yes/No
A description of the voting system type and the operational environment	**Software** • AIMS version 1.3.57 • VAT version 1.3.2904 **Hardware** • Voter Assist Terminal (A100) • Voter Assist Terminal (A200)
Voting: **Accessibility verifications**	The Standards provide requirements for voting systems to meet the accessibility needs of a broad range of voters with disabilities. The vendor must either configure all of the system's voting stations to meet the accessibility specifications or must design a unique station that conforms to the accessibility requirements and is part of the overall voting system configuration.

Test Detail	Test Methodology
Test Case Name	**GEN03 - Usability and Accessibility**
	Mimicking the voter with disabilities, verification is done to ensure that: • The voter can perform the complete voting experience independently and that their experience is similar to a non-disabled voter • The ballot is not visible to others • The ballot information for each voter is not available to unauthorized persons • The integrity of the ballot information is maintained similarly to non-disabled ballot information (V1: 2.2.7) To facilitate accessibility, all voting systems must meet Common Standards, as illustrated in Figures 2-1 through 2-4 listed in the VSS. (V1: 2.2.7.1) These Common Standards include: • Reach • Obstruction • Protrusion • Operable controls • ADA standards Mimicking the voter with disabilities, measurements are taken, according to the guidelines listed in the VSS, to ensure that disabled voter accessibility meets the necessary guidelines. Additionally verification of DRE voting systems ensures that they provide, as part of their configuration, the capability to provide access to voters with a broad range of disabilities. The DRE standards, listed in the VSS, are followed and used to verify each applicable voting machine. When necessary, measuring devices are used for validation. This can include pressure and dB meters, rulers and stopwatches. (V1: 2.2.7.2)
Voting: **Usability verifications**	Usability verification addresses the design of the voting system and it's ability to meet the needs of the voters, that is, to ensure that the interfaces between the voter and the system are easy to use and minimize voter errors. The following areas are focused on in this step: • Information displays, e.g., presentations of contests, candidates, propositions, and instructions • Vote input fields, e.g., the location where the voter indicates his or her selection • Navigation aids, e.g., the way that voters "move" from one part of the system to another The guidelines listed in the VSS Volume 1, Appendix C and section 3.4.9, are followed in order to verify: • General Principles (V1: Appendix C.2) • Overall Design and Layout of the Voter Workspace (V1: Appendix C.3) • Ballot Legibility and Understandability (V1: Appendix C.4) • Information Grouping (V1: Appendix C.5) • Voting Input Fields (V1: Appendix C.6) • Navigation and Manipulation of Ballots (V1: Appendix C.7) • Preventing and Minimizing Voter Errors (V1: Appendix C.8) • Help and System Failure (V1: Appendix C.9) • Voter Familiarization and Training (V1: Appendix C.10)

Test Detail	Test Methodology
Test Case Name	**PRI01- Open Primary**
NOTE	*This test case is to be used in conjunction with the **Election Core definition**.*
Objective	The object of this test case is to verify core functional and performance capabilities of the ES&S AutoMark 1.3 system, by using the vendor's manual(s) to import a standard open primary election from ES&S Unity 3.0.1.0/3.0.1.1 system; vote on paper ballots with ovals in the left position, and arrows in the right position, with both types of ballots being voted on the VAT A100 and A200 models, and tally results for an Open Primary Election.
Variables: **Voting Variations**	The following are the items verified in this election. See the remaining election test cases for examples of all voting variations supported by the vendor. (V1:2.2.8.2) • 1 precinct, 3 splits • 3 partisan (Democratic, Republican, and Scientist) contests • 6 Non-partisan contests • Partisan contest (Democratic, Republican & Scientist): 1 of M, presidential nomination, multi-member board (President) • Partisan contest: Alderman contest: 2 of M • Partisan contest: Secretary of State: 1 of M o Democratic ballot: 1 of M, write-in, no declared candidates o Republican ballot: 1 of M, write-in, declared candidates o Scientist ballot: 1 of M, write-in, declared candidates • Non-Partisan contest: 1 of M, write-in, no declared candidates. (Sheriff) • Non-Partisan contest: 1 of M, a single candidate, write-in (Superintendent of Schools) • Non-Partisan Ballot: 3 of M, declared candidates, write-in (School Board) • Non-partisan contest: Proposition/Question (Proposition X) • Recall Type A: Simple Yes/No question (Recall/Retain Judge) • Recall Type B: Retain/Replace (Retain/Replace Judge)
Variables: **Election Variations**	Primary Election: • **President**: 3 DEM candidates, 2 REP candidates, 2 Scientist candidates, • **Secretary of State**: no declared DEM candidate, 3 REP candidates, 2 Scientist candidates • **Alderman:** 3 DEM candidates, 4 REP candidates, 3 Scientist candidates Non-Partisan Primary Election: • **Sheriff**: No declared candidate • **Superintendent of Schools**: 1 candidate • **School Board**: 6 candidates • **Recall Judge (District A):** Yes/No • **Replace Judge (District B):** Retain = first option, Replace = second and third options • **Proposition X**: Yes/No

Test Detail	Test Methodology
Test Case Name	**PRI01- Open Primary**
A description of the voting system type and the operational environment	**Software** • AIMS version 1.3.57 • VAT version 1.3.2904 **Hardware** • Voter Assist Terminal (A100) • Voter Assist Terminal (A200)
Voting: **Additional - Required functionality verifications**	Party affiliation is identified on the ballots *where appropriate*.

Test Detail	Test Methodology
Test Case Name	**PRI01 - Open Primary with Pick-a-Party/Party Preference**
NOTE	*This test case is to be used in conjunction with the **Election Core definition**.*
Objective	The object of this test case is to verify core functional and performance capabilities of the ES&S AutoMark 1.3 voting system, by using the vendor's manual(s) to import a standard open primary, pick-a-party/party preference election from ES&S Unity 3.0.1.0/3.0.1.1 system; vote on paper ballots with ovals in the left position, and arrows in the right position, with both types of ballots being voted on the VAT A100 and A200 models, and tally results for an Open Primary Party Preference Election.
Variables: **Voting Variations**	The following are the items verified in this election. See the remaining election test cases for examples of all voting variations supported by the vendor. (V1:2.2.8.2) • 1 precinct, 3 splits • Partisan contest (Democratic, Republican & Scientist): 1 of M, President • Partisan contest: Alderman contest: 2 of M • Partisan contest: Secretary of State contest: 1 of M o Democratic ballot: 1 of M, write-in, no declared candidates o Republican ballot: 1 of M, write-in, declared candidates o Scientist ballot: 1 of M, write-in, declared candidates • Non-Partisan contest: 1 of M, write-in, no declared candidates. (Sheriff) • Non-Partisan contest: 1 of M, a single candidate, write-in (Superintendent of Schools) • Non-Partisan Ballot: 3 of M, declared candidates, write-in (School Board) • Non-partisan contest: Proposition/Question (Proposition X) • Recall Type A: Simple Yes/No question (Recall/Retain Judge) • Recall Type B: Retain/Replace (Retain/Replace Judge)
Variables: **Election Variations**	Primary Election: • **President**: 3 DEM candidates, 2 REP candidates, 2 Scientist candidates, • **Secretary of State**: no declared DEM candidate, 3 REP candidates, 2 Scientist candidates • **Alderman:** 3 DEM candidates, 4 REP candidates, 3 Scientist candidates Non-Partisan Primary Election: • **Sheriff**: No declared candidate • **Superintendent of Schools**: 1 candidate • **School Board**: 6 candidates • **Recall Judge (District A):** Yes/No **Replace Judge (District B):** Retain = first option, Replace = second and third options • **Proposition X**: Yes/No
A description of the voting system type and the operational environment	**Software** • AIMS version 1.3.57 • VAT version 1.3.2904

Test Detail	Test Methodology
Test Case Name	**PRI01 - Open Primary with Pick-a-Party/Party Preference**
	Hardware • Voter Assist Terminal (A100) • Voter Assist Terminal (A200)
Voting: **Additional - Required functionality verifications**	Party affiliation is identified on the ballots *where appropriate*.

Test Detail	Test Methodology
Test Case Name	**PRI02 - Closed Primary**
NOTE	*This test case is to be used in conjunction with the **Election Core definition**.*
Objective	The object of this test case is to verify core functional and performance capabilities of the ES&S AutoMark 1.3 voting system, by using the vendor's manual(s) to import a closed primary election from ES&S Unity 3.0.1.0/3.0.1.1 system; vote on paper ballots with ovals in the left position, and arrows in the right position, with both types of ballots being voted on the VAT A100 and A200 models, and tally results for a Closed Primary Election.
Variables: **Voting Variations**	The following are the items verified in this election. See the remaining election test cases for examples of all voting variations supported by the vendor. (V1:2.2.8.2) • 3 precincts, 3 splits • Partisan contest (Presidential delegate slate, display of delegates with nominees) o Democrat ballot: 1 of M, selection is a vote for the entire slate of delegates, write-in o Republican ballot: 1 of M, selection is a vote for the entire slate of delegates, write-in o Libertarian ballot: selection is a vote for the entire slate of delegates, write-in • Partisan contest: (US Senator) o Democrat Ballot: 2 of M, write-ins, no declared candidates, cross over to another partisan ballot if no declared candidate o Republican Ballot: 2 of M, write-ins, declared candidates o Libertarian ballot: 2 of M, write-ins, declared candidates • Partisan contest: (US Representative) o Democrat ballot: 1 of M, declared candidates o Republican ballot: 1 of M, declared candidates o Libertarian ballot: 1 of M, declared candidates • Partisan contest: (State Senator) o Democrat ballot: 1 of M, declared candidates o Republican ballot: 1 of M, declared candidates o Libertarian ballot: 1 of M, declared candidates • Partisan contest: (County Attorney) o Democrat ballot: 1 of M, declared candidates o Republican ballot: 1 of M, declared candidates o Libertarian ballot: 1 of M, declared candidates • Partisan contest: (Sheriff) o Democrat ballot: 1 of M, declared candidates o Republican ballot: 1 of M, declared candidates o Libertarian ballot: 1 of M, declared candidates

Test Detail	Test Methodology
Test Case Name	**PRI02 - Closed Primary**
	• Non-Partisan contest: 2 of M, declared candidates (County Commissioner) • Non-Partisan Ballot: Recall Type D: Retain/Recall Conditional contest (Judge recall) • Rotation by Precinct / Split
Variables: **Election Variations**	Primary Election: **Presidential Delegates:** 3 DEM candidates**,** 2 REP candidates, no Libertarian candidates **US Senator**: no DEM candidates, 2 REP candidates, 2 Libertarian candidates **US Representative in Congress**: 2 DEM candidates, 2 REP candidates, 2 Libertarian candidates **State Senator:** 2 DEM candidates, 2 REP candidates, 2 Libertarian candidates **County Attorney**: 2 DEM candidates, 2 REP candidates, 2 Libertarian candidates **Sheriff**: 2 DEM candidates, 2 REP candidates, 2 Libertarian candidates Non-Partisan Primary Election: • **County Commissioner**: 5 candidates • **Recall/Retain Judge (District D) (1st Contest):** Y/N • **Recall/Retain Judge (District D) (2nd Contest):** 1 option to replace with 2 candidates
A description of the voting system type and the operational environment	**Software** • AIMS version 1.3.57 • VAT version 1.3.2904 **Hardware** • Voter Assist Terminal (A100) • Voter Assist Terminal (A200)
Voting: **Additional - Required functionality verifications**	Party affiliation is identified on the ballots *where appropriate.*

Test Detail	Test Methodology
Test Case Name	**Accuracy**
NOTE	*This test case is to be used in conjunction with the **Election Core definition**.*
Scope	A functional test that uses The 2002 Voting System Standards (VSS) guidelines to validate the individual ballot positions in terms of a maximum error rate while processing a specified volume of data. (V2:4.7.1.1)
Objective	The object of this test is to verify that the voting system can accurately and reliably print ballots incorporating a minimum 1,549,703 ballot positions (including voted and non-voted positions) and that these ballots can be mechanically/electronically tabulated without error.
Variables: **Voting Variations**	*Please refer to "Calculation of Ballots to be processed" below.*
Variables: **Election Variations**	*Please refer to "Calculation of Ballots to be processed" below.*
A description of the voting system type and the operational environment	**Software** • AIMS version 1.3.57 • VAT version 1.3.2904 **Hardware** • Voter Assist Terminal (A100) • Voter Assist Terminal (A200)

Test Detail	Test Methodology
Test Case Name	**Accuracy**
Calculation of Ballots to be processed	**Terminals:** • A100: 3 machines • A200: 3 machines **Ballot Description:** • Oval ballot o 6 contests x 44 Candidates = 264 ballot positions o Moving diagonal vote pattern used o 44 ballots per batch x 264 ballot positions = 11,616 ballot positions per batch o 12 batches per machine x 11,616 = 139,392 ballot positions per machine o 6 machines x 139,392 = 836,352 ballot positions total • Arrow ballot o 6 contests x 51 Candidates = 306 ballot positions o moving diagonal vote pattern used o 51 ballots per batch x 306 ballot positions = 15,606 ballot positions o 8 batches per machine x 15,606 = 124,848 ballot positions per machine o 6 machines x 124,848 = 749,088 ballot positions total 836,352 + 749,088 = 1,585,440 >= 1549,703 (required ballot positions)
Voting: Additional - Opening the Polls Verification	Verify that all potential ballot positions are active and able to be voted (V1: 2.3.4.2)
Accuracy: **Error Rate**	Voting system accuracy addresses the accuracy of data for each of the individual ballot positions that could be selected by a voter, including the positions that are not selected. For a voting system, accuracy is defined as the ability of the system to capture, record, store, consolidate and report the specific selections and absence of selections, made by the voter for each ballot position without error. Required accuracy is defined in terms of an error rate that for testing purposes represents the maximum number of errors allowed while processing a specified volume of data. (V1:3.2.1) For all systems, the total number of ballots to be processed by each precinct counting device during these tests reflects the maximum number of active voting positions and the maximum number of ballot styles that the vendor's TDP claims the system can support. (V2:6.2.3, 3.2.6.1.1) The error rate determines the accuracy test vote position processing volume: • Reject: one error before counting 26,997 consecutive ballot positions correctly • Accept: 1,549,703 (or more) consecutive ballot positions are read correctly • If there is one error with more than 26,997 ballot positions but less than 1,549,703 correctly read, continue until another 1,576,701 consecutive ballot positions are counted without error (i.e. Accept: 3,126,404 with one error)

Test Detail	Test Methodology
Test Case Name	**Accuracy**
	The Ballot Reading Accuracy for paper-based system requirement governs the conversion of the physical ballot into electronic data. Reading accuracy for ballot conversion refers to the ability to: • Recognize vote punches or marks, or the absence thereof, for each possible selection on the ballot • Discriminate between valid punches or marks and extraneous perforations, smudges, and folds • Convert the vote punches or marks, or the absence thereof, for each possible selection on the ballot into digital signals. Verification of paper-based systems ensures that the system: (V1:3.2.5.2) • Detects punches or marks that conform to vendor specifications with an error rate not exceeding the requirement indicated in Section 3.2.1 • Rejects ballots that meet all vendor specifications at a rate not to exceed 2 percent

Test Detail	Test Methodology
Test Case Name	**Readiness Test**
Scope	A functional test that uses The 2002 Voting System Standards (VSS) guidelines to validate Readiness throughout the entire voting system. (V1:2.3.4)
Objective	The object of this test case is to verify equipment and system readiness to ensure that the voting system functions properly, to confirm that the system equipment has been properly intergraded, and to obtain equipment status reports. (V1:2.3.4)
Standards Documents	Voting System Standards 2002, vol. 1 Voting System Standards 2002, vol. 2 Specific standards are noted in following steps.
A listing of the applicable voting system machines	**Software** • AIMS version 1.3.57 • VAT version 1.3.2904 **Hardware** • Voter Assist Terminal (A100) • Voter Assist Terminal (A200) Refer to the following tables for complete descriptions: ➢ Matrix of Required Software/Firmware ➢ Matrix of Required Hardware
Pre-requisites and initialization of the test case	This testing is to be executed on initial testing and each time the system is to be shut down and restarted.
Documentation of Test Data & Test Results	For each iteration that the election is run: • Capture all voting steps in order to maintain repeatability of the test • Record election, ballot, and vote data fields on the corresponding worksheet tabs • Save all worksheet tabs for all iterations of the test case • Record results of test run by entering 'Accept/Reject' on the Test Results Matrix • Provide comments when observing deviations, discrepancies or notable observations • Log discrepancies on the Discrepancy Report
System Preparation - Security	System Preparation - Security: • System username/password authentication and other access controls are set up according to system documentation guidelines for all devices being tested. • Any/all unnecessary processes are disabled and/or required process control measures noted in the documentation are followed. • All COTS and vendor subsystems used for system security are configured and active as recommended by the system documentation. This includes all connection, port, virus, and data or authorized process restriction systems. • Any other pre-election system security measures listed in the

Test Detail	Test Methodology
Test Case Name	**Readiness Test**
	documentation are followed including setup of additional hardware or software not covered above. Please also see the Documentation section of the Security Test Case within Appendix A.
Readiness Testing Verification	Verification of Voting machines or vote recording and data processing equipment, precinct count equipment, and central count equipment are properly configured for an election, and collect data that verifies equipment readiness. This includes: • Obtain status and data reports from each set of equipment • Correct installation and interface of all system equipment • Hardware and software function correctly • Version verification
Summary of Instructions followed per Product	The following list of documentation is used to perform system readiness: • Election Officials Guide AQS-13-5001-208-R 07, Release Date: June 4, 2007 • Jurisdiction Guide AQS-13-5061-003-R 05, Release Date: June 4, 2007 • Poll Worker's Guide AQS-13-5061-002-R 06, Release Date: June 4, 2007
Readiness Audit	Produce and verify available system reports
Results are Observed	Review the outcome of the test(s) against the expected result(s): • **Accept**: expected results is observed • **Reject:** expected result is NOT observed • **Not Testable (NT)**: rejection of a previous test step prevents validation of this step or this was tested in another test case • **Not Applicable (NA):** not applicable to the current test scope or to the component under review • **Not Supported (NS)**: not supported in the current test scope
Record Observations and all input/outputs for each election	All information used in processing the test case is captured. This includes: inputs, outputs, deviations and any other item that may impact the validation of the test case. Any failure of the test against the EAC guidelines is reported and implies failure of the system. Failures are reported as Defect Issues in the Discrepancy Report and are provided to the manufacturer. Before the final Certification Test Report is issued, manufacturers are given the opportunity to correct all discrepancies. If the manufacturer submits corrections, retests are performed. Issues that do not impact the failure of the requirements but could be considered defects are logged as Informational Issues on the Discrepancy Report. It is the manufacturer's option to address these issues.

Test Detail	Test Methodology
Test Case Name	**Operational Status Check**
Scope	SysTest Labs requires the vendor to provide a comprehensive end-to-end test case(s) that they supply to their customers, such as state election officials. The Vendor may provide SysTest Labs a comprehensive checklist of test case(s) for particular states' functionality. This test may be based on the vendor's certification configuration. SysTest Labs will perform the operational status check once upon acceptance of the equipment, and once after all other testing, prior to checkout. (V2: 4.6.1.5)
Objective	The object of this test case is to verify that when all tests, inspections, repairs, and adjustments have been completed, normal operation can be verified by conducting an operational status check.
Standards Documents	Voting System Standards 2002, vol. 1 Voting System Standards 2002, vol. 2 Specific standards are noted in following steps.
A listing of the applicable voting system machines	**Software** • AIMS version 1.3.57 • VAT version 1.3.2904 **Hardware** • Voter Assist Terminal (A100) • Voter Assist Terminal (A200) Refer to the following tables for complete descriptions: ➢ Matrix of Required Software/Firmware ➢ Matrix of Required Hardware
Documentation of Test Data & Test Results	For each iteration that the election is run: • Capture all voting steps in order to maintain repeatability of the test • Record election, ballot, and vote data fields on the corresponding worksheet tabs • Save all worksheet tabs for all iterations of the test case • Record results of test run by entering 'Accept/Reject' on the Test Results Matrix • Provide comments when observing deviations, discrepancies or notable observations • Log discrepancies on the Discrepancy Report
Operational Status Check Verification	During this process, all equipment will be operated in a manner and environmental conditions that simulate election use to verify the functional status of the system. Prior to the conduct of each of the environmental hardware non-operating tests, a supplemental test will be made to determine that the operational state of the equipment is within acceptable performance limits. The following procedures will be followed to verify the equipment status: Step 1: Arrange the system for normal operation. Step 2: Turn on power, and allow the system to reach recommended operating temperature.

Test Detail	Test Methodology
Test Case Name	**Operational Status Check**
	Step 3: Perform any servicing, and make any adjustments necessary, to achieve operational status. Step 4: Operate the equipment in all modes, demonstrating all functions and features that would be used during election operations. Step 5: Verify that all system functions have been correctly executed.
Readiness Audit	Produce and verify available system reports
Results are Observed	Review the outcome of the test(s) against the expected result(s): • **Accept**: expected results is observed • **Reject:** expected result is NOT observed • **Not Testable (NT)**: rejection of a previous test step prevents validation of this step or this was tested in another test case • **Not Applicable (NA):** not applicable to the current test scope or to the component under review • **Not Supported (NS)**: not supported in the current test scope
Record Observations and all input/outputs for each election	All information used in processing the test case is captured. This includes: inputs, outputs, deviations and any other item that may impact the validation of the test case. Any failure of the test against the EAC guidelines is reported and implies failure of the system. Failures are reported as Defect Issues in the Discrepancy Report and are provided to the manufacturer. Before the final Certification Test Report is issued, manufacturers are given the opportunity to correct all discrepancies. If the manufacturer submits corrections, retests are performed. Issues that do not impact the failure of the requirements but could be considered defects are logged as Informational Issues on the Discrepancy Report. It is the manufacturer's option to address these issues.

Test Detail	Test Methodology
Test Case Name	**Security**
Scope	Security Testing Overview Security testing is related to four activities: **Documentation Review** - Documentation Review verifies that the system has documented policies and procedures that mitigate or eliminate security threats outlined in the VSS guidelines. It also describes Access controls. **Source Code Review** - Source Code Review insures source code meets VSS guidelines and provides additional protection against security flaws into the system. Potential security issues may include default passwords or backdoors in the source code, encryption keys in the source code, encryption flaws, unencrypted data transmissions, encryption algorithms that are not NIST certified, etc. **Hardware Testing** - Hardware Testing insures that equipment will stand up to environment conditions, machines are accurate, physical access to machine components is restricted, machine hardware is reliable and attempts to compromise machine security is detectable. A hardware malfunction could impact the accuracy of voting data or provide unauthorized access to secure information. Specific hardware limitations or restrictions impact the test procedures needed to validate security of the system. **System Testing** - System Testing verifies that voting systems have sufficient system and data protection mechanisms that when combined with other review processes, provide a secure voting environment. This section of the document relates to System Testing but depends on the other three activities that are covered in their own specific section.
Objective	Security testing attempts to identify flaws in voting systems where undesired or unauthorized human or machine activity may compromise an election through system failure, data manipulation, data interception or other means. Prevent and/or detect undesired system activities including: • Unauthorized access through accidental or intentional bypass or circumvention of authorization controls. • Alteration, deletion, replacement or theft of voter, election, audit and/or vote data. • Hardware and/or software tampering • Interruption of voting activities
Standards Documents	Voting System Standards 2002, vol. 1 Voting System Standards 2002, vol. 2 Specific standards are noted in following steps.
A listing of the applicable voting system machines	**Software** • AIMS version 1.3.57 • VAT version 1.3.2904 **Hardware** • Voter Assist Terminal (A100) • Voter Assist Terminal (A200) Refer to the following tables for complete descriptions: ➢ Matrix of Required Software/Firmware ➢ Matrix of Required Hardware

Test Detail	Test Methodology
Test Case Name	**Security**
Security Test Sub Type	**Description**
1. Role	SysTest Labs will validate that the vendor has implemented adequate security policies and controls to ensure that Voting Systems meet the requirements specified in the applicable FEC VSS 2002 Voting Standards. Using well-defined, repeatable testing methods and inspection processes, SysTest Labs will validate that the following required policies and controls exist and are effective: **1.1** Privileges are not allowed to be: • Exceeded (V1:6.2.1.2c) • Changed to Run Reports **1.2** Voters are inhibited from: • Accessing Equipment Before Polls Open • Running Reports **1.3** Changes to Privileges are Prohibited for IDs and Passwords Thus Preventing Unauthorized Report Printing, Results Transmission, Results Downloading and Resetting of Elections **1.4** Voter equipment access or keys are limited to ensure: • Only the User interface is accessible • Only a single vote may be cast • Closed Polls are secure • Counts are not available to voters • Unauthorized Accounts from System Functions **1.5** Fraudulent Ballots are not accepted by the system ensuring only valid ballots are counted **1.6** The vendor permits the voter to cast a ballot expeditiously, but precludes voter access to all other aspects of the vote-counting processes. (V1.6.2.1.2.c) **1.7** Password Required for Each System Software Component (V1:6.5.5.c) **1.8** Password Required for Each System Data Component **1.9** Password Required for Each System Data Component **1.10** Hardware Key Required for Each System Hardware Component **1.11** Each Type of User Account Can Only Perform Intended Functions
2. Access	SysTest Labs will validate that the vendor has implemented adequate ACCESS controls to ensure the integrity and operational security of Voting Systems, as specified by the requirements of applicable FEC VSS 2002 Voting Standards. Using well defined, repeatable testing methods and inspection processes, SysTest Labs will validate that the following required ACCESS policies and controls exist and are effective: **2.1** Access validation to the system ensures that only applicable system entry is allowed. This includes: • Seals and/or Password are Required to Open Polls (V1:2.4.1.3.a, 3.2.4.2.6.b) • Security Seal and/or Password Prevent Unauthorized Opening of Polls

Test Detail	Test Methodology
Test Case Name	**Security**
Security Test Sub Type	**Description**
	• Incorrect or Blank Password Cannot be Used to Open Polls (V1:6.2.1.1.d) • System Provides Access Controls that Limit or Detect Access to Critical System Components (V1:2.1.1.a, 6.2.1.1.d)
3. System Security	SysTest Labs will validate that the vendor has implemented adequate and effective system security policies and controls. Using well-defined, repeatable testing methods and inspection processes, SysTest Labs will validate that the following required policies and controls exist and are effective: **3.1** System security is achieved through a combination of technical capabilities and sound administrative practices. To ensure security, the system: (V1: 2.2.1) • Provides system functions that are executable only in the intended manner and order, and only under the intended conditions. • Uses the system's control logic to prevent a system function from executing if any preconditions to the function have not been met. • Provides safeguards to protect against tampering during system repair, or interventions in system operations, in response to system failure. • Provides security provisions that are compatible with the procedures and administrative tasks involved in equipment preparation, testing, and operation. • If access to a system function is to be restricted or controlled, the system incorporates a means of implementing this capability. • Provides documentation of mandatory administrative procedures for effective system security **3.2** The voting system may use a local or remote data network. Should such a network be used in a jurisdiction, all components of the network do comply with the telecommunications requirements described in Section 5 of the Standards and the Security requirements as described in Section 6. (V1: 3.2.2.15)
4. System Log	SysTest Labs will validate that the vendor's ability to capture and control system logs and log entries meet applicable requirements in the FEC VSS 2002 Voting Standards. Using well-defined, repeatable testing methods and inspection processes, SysTest Labs will validate that the following required logging capabilities and controls exist and are effective. Verification of System Log Activity is performed to ensure: **4.1** Error Activity provided by the system is complete, applicable, and appropriate (V1:4.4.3) **4.2** Voting Activity is captured correctly (V1:4.4.3.d) **4.3** Log(s) have the needed protection to validate that the information is secure (V1:4.4.3)
5. Software Security	SysTest Labs will validate that specific software/firmware security measures are in place, adequate, and effective. Using well-defined, repeatable testing methods and inspection processes, SysTest Labs will validate that the following required logging capabilities and controls exist and are effective: **5.1** Software security validation ensures that the firmware has been shown to be

Test Detail	Test Methodology
Test Case Name	**Security**
Security Test Sub Type	**Description**
	inaccessible to activation or control (V1:6.4.1.c) **5.2** Verify the Separation of Election Specific Firmware and Operating System are stored (V1:6.4.1.d)
6. Data Integrity	SysTest Labs will validate that the capabilities of the Voting System to manage and maintain data integrity in components and across the entire Voting System through the stages of the election process meet the applicable requirements in the FEC VSS 2002 Voting Standards. Using well-defined, repeatable testing methods and inspection processes, SysTest Labs will validate that the following required data integrity management and maintenance capabilities and controls exist and are effective: **6.1** The system meets the following requirements for installation of software, including hardware with imbedded firmware: (V1.6.4.1) • The system bootstrap, monitor, and device-controller software may be resident permanently as firmware, this firmware has been shown to be inaccessible to activation or control by any means other than by the authorized initiation and execution of the vote-counting program, and its associated exception handlers • The election-specific programming is installed and resident as firmware, this firmware is installed on a component other than the component on which the operating system resides **6.2** Transmission of data shall ensure that receipt of valid vote records is verified at the receiving stations (V1:6.5.2) **6.3** Transmission of Cast Ballots During Voting Error Detection, Recovery and Retransmission **6.4** Transmission of Cast Ballots During Voting Integrity Checks **6.5** Transmission Verification Checks **6.6** Verification that the ballot reader is prevented from reading more than one ballot at a time (multiple feed), and if detected, the card reader halts (V1: 3.2.5.1.4.a) **NOTE: VAT does not transmit data.**
7. Telecom & Data Transmission	SysTest Labs will validate that the capabilities of the voting system to manage and maintain secure telecommunications and data transmissions in components and across the entire Voting System meet the applicable requirements in the FEC VSS 2002 Voting Standards. Using well-defined, repeatable testing methods and inspection processes, SysTest Labs will validate that the following required capabilities and controls exist and are effective: **7.1** The system transmits data over public telecommunications networks, and as such: (V1.6.6.1) • Preserves the secrecy of a voter's ballot choices, and prevents anyone from violating ballot privacy **7.2** Encrypted Transmissions (V1:6.5.3.a) **7.3** Encryption Specification Verification **7.4** Session Hijacking

Test Detail	Test Methodology
Test Case Name	**Security**
Security Test Sub Type	**Description**
	7.5 Monitoring and Responding to External Threats (V1:6.5.4.3) **7.6** Shared Operating Environment (V1:6.5.5) **7.7** Security for Transmissions (V1:6.6) **7.8** Unauthorized Tool **7.9** Virus **7.10** Threat Reception and Storage Prevention (V1:6.5.4.2) **7.11** Remote Access Disabled **7.12** User Account Restriction From Remote Access Settings **7.13** Routers and/or Firewalls **NOTE: VAT does not transmit data.**
8. Threat Protection	SysTest Labs will validate that the capabilities of the Voting System to protect against computer security threats meet the applicable requirements in the FEC VSS 2002 Voting Standards. Using well-defined, repeatable testing methods and inspection processes, SysTest Labs will validate that the following required computer threat protection capabilities, security policies, and controls exist and are effective: **8.1** Memory Threat & Virus Scanning Mechanisms (1-6.5.4.2) **8.2** Rootkit Scanning Mechanisms
9. Audit Log	SysTest Labs will validate that the Voting System meets FEC VSS 2002 Voting Standards to securely manage and maintain audit logs in all components and across the entire Voting System. Using well-defined, repeatable testing methods and inspection processes, SysTest Labs will validate that the following required audit logging capabilities and controls exist and are effective: **9.1** Audit logs and data files cannot be altered through the use of an alternate boot sequence without detection, and the test will consist of attempting to boot the devices using alternative media during boot sequences. **9.2** Audit logs and data files cannot be altered through the use of editing tools without detection. **9.3** The test will consist of attempting to edit the audit log to confirm that the system either: • Does not allow edits of the audit log or data files, or • Detects and reports all attempts at editing the audit log or data files
10. Data Protection	SysTest Labs will validate that the Voting System meets FEC VSS 2002 Voting Standards to securely protect data used and stored in components and across the entire Voting System. Using well-defined, repeatable testing methods and inspection processes, SysTest Labs will validate that the following required data protection policies, capabilities, and controls exist and are effective: **10.1** Logical Isolation of Voting System Software & Data (V1:6.5.5.b) **10.2** Access Control Lists Preclude Data Leakage (V1:6.5.5.d) **10.3** Routers and Firewalls Preclude Data Leakage

Test Detail	Test Methodology
Test Case Name	**Security**
Security Test Sub Type	**Description**
	10.4 Electronic Policies Prevent Copy of Data **10.5** Voting System Access to Incomplete Election Returns (V1:6.5.6)
11. Documentation	Vendor documentation is reviewed and evaluated to verify that it speaks to required VSS security concerns with regard to various aspects of a voting system. If determined that an appropriate amount of information is supplied such that the requirements are adequately met, at a minimum, the requirement is passed. If it is determined that not enough information is supplied to adequately meet the requirement, the requirement is judged to have been failed. The following standards are used to ensure that: **11.1** Although the jurisdiction in which the voting system is operated is responsible for determining the access policies applying to each election, the vendor provides a description of recommended policies for: (V1:6.2.1.1) • Software access controls documentation • Hardware access controls documentation • Communications documentation • Effective password management documentation • Protection abilities of a particular operating system documentation • General characteristics of supervisory access privileges documentation • Segregation of Duties documentation • Any additional relevant characteristics **11.2** The voting system vendor: (V1:6.2.1.2) • Identifies each person, to whom access is granted, and the specific functions and data to which each person holds authorized access. • specifies whether an individual's authorization is limited to a specific time, time interval, or phase of the voting our counting operation **11.3** The vendor provides a detailed description of all system access control measures designed to permit authorized access to the system and prevent unauthorized access, as covered in the following areas: (V1:6.2.2) • Use of data and user authorization • Program unit ownership and other regional boundaries • One-end or two-end port protection devices • Security kernels • Computer-generated password keys • Special protocols • Message encryption • Controlled access security **11.4** The vendor defines and provides a detailed description of the methods used to prevent unauthorized access to the access control capabilities of the system itself. (V1:6.2.2)

Test Detail	Test Methodology
Test Case Name	**Security**
Security Test Sub Type	**Description**
	11.5 The vendor develops and provides detailed documentation, pertaining to polling place security operations, of measures to anticipate and counteract vandalism, civil disobedience, and similar occurrences of. The measures: (V1:6.3.1) • Allow the immediate detection of tampering with vote casting devices and precinct ballot counters • Control physical access to a telecommunications link if such a link is used **11.6** The Vendor develops and documents, in detail, the measures to be taken in a central counting environment. These measures include physical and procedural controls related to the: (V1:6.3.2) • Handling of ballot boxes • Preparing of ballots for counting • Counting operations • Reporting data **11.7** The system meets the following requirements for installation of software, including hardware with embedded firmware: (V1:6.4.1) • If software is resident in the system as firmware, the vendor requires and states in the system documentation that every device is to be retested to validate each ROM prior to the start of elections operations • To prevent alteration of executable code, no software is permanently installed or resident in the system unless the system documentation states that the jurisdiction must provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of the system hardware • After initiation of election day testing, no source code or compilers or assemblers are resident or accessible **11.8** The voting system deploys protection against the many forms of threats to which it may be exposed such as file and macro viruses, worms, Trojan horses, and logic bombs. The vendor has developed and documented the procedures to be followed to ensure that such protection is maintained in a current status. (V1:6.4.2) **11.9** The voting system uses telecommunications to communicate between system components and locations, and is subject to the same security requirements governing access to any other system hardware, software, and data function. (V1:6.5.1) **11.10** The voting system uses, for data integrity, electrical or optical transmission of data and, as such, ensures the receipt of valid vote records is verified at the receiving station. This includes standard transmission error detection and correction methods such as checksums and/or message digest hashes. Verification of correct transmission occurs at the voting system application level and ensures that the correct data is recorded on all relevant components consolidated within the polling place prior to the voter completing casting of his or her ballot. (V1:6.5.2) **11.11** The voting system, using telecommunications as defined in Section 5 to

Test Detail	Test Methodology
Test Case Name	**Security**
Security Test Sub Type	**Description**
	communicate between system components and locations before the poll site is officially closed does the following: (V1:6.5.3) • The vendor implements an encryption standard currently documented and validated for use by an agency of the U.S. Federal Government • Provides a means to detect the presence of an intrusive process, such as an Intrusion Detection System **11.12** The voting system uses public telecommunications networks and implements protections against external threats to which commercial products used in the system may be susceptible. (V1:6.5.4) **11.13** The voting system uses public telecommunications networks and therefore provides system documentation that clearly identifies all COTS hardware and software products and communications services used in the development and/or operation of the voting system. Such documentation identifies the name, vendor, and version used for each such component. (V1:6.5.4.1) • Operating systems • Communications routers • Modem drivers • Dial-up networking software **11.14** The voting system uses public telecommunications networks and uses protective software at the receiving-end of all communication paths to: (V1:6.5.4.2) • Detect the presence of a threat in a transmission • Remove the threat from infected files/data • Prevent against storage of the threat anywhere on the receiving device • Provide the capability to confirm that no threats are stored in system memory and in connected storage media • Provide data to the system audit log indicating the detection of a threat and the processing performed **11.15** The vendor uses multiple forms of protective software, as needed, to provide capabilities for the full range of products used by the voting system. (V1:6.5.4.2) **11.16** The vendor documents how they plan to monitor and respond to known threats to which the voting system is vulnerable. This documentation provides a detailed description, including scheduling information of the procedures the vendor uses to: (V1:6.5.4.3) • Monitor threats, such as through the review of assessments, advisories, and alerts for COTS components issued by the Computer Emergency Response Team (CERT), the National Infrastructure Protection Center (NIPC), and the Federal Computer Incident Response Capability (FedCIRC) • Evaluate the threats and, if any, proposed responses • Develop responsive updates to the system and/or corrective procedures

Test Detail	Test Methodology
Test Case Name	**Security**
Security Test Sub Type	**Description**
	• Submit the proposed response to the ITAs and appropriate states for approval, identifying the exact changes and whether or not they are temporary or permanent • After implementation of the proposed response is approved by the state, to assist clients, either directly or through detailed written procedures, how to update their systems and/or to implement the corrective procedures no later than one month before an election • Address threats emerging too late to correct the system at least one month before the election, including • Provide prompt, emergency notification to the ITA and the affected states and user jurisdictions • Assist client jurisdictions directly, or advising them through detailed written procedures, to disable the public telecommunications mode of the system • After the election, modify the system to address the threat; submitting the modified system to an ITA and appropriate state certification authority for approval, and assisting client jurisdictions directly, or advising them through detailed written procedure, to update their systems and/or to implement the corrective procedures after approval **11.17** For shared operating environments, ballot recording and vote counting can be performed in either a dedicated or non-dedicated environment. For ballot recording and vote counting operations performed in an environment that is shared with other data processing functions, both hardware and software features are present to protect the integrity of vote counting and of vote data. The system uses a shared operating environment such that it: (V1:6.5.5) • Uses security procedures and logging records to control access to system functions • Partitions or compartmentalizes voting system functions from other concurrent functions at least logically, and preferably physically as well • Controls system access by means of passwords, and restriction of account access to necessary functions only; • Has capabilities in place to control the flow of information, precluding data leakage through shared system resources **11.18** The voting system provides access to incomplete election returns and interactive inquiries before the completion of the official count, so that the system: (V1:6.5.6) • Is designed to provide external access to incomplete election returns only if that access for these purposes is authorized by the statutes and regulations of the using agency. This requirement applies as well to polling place equipment that contains a removable memory module, or that may be removed in its entirety to a central place for the consolidation of polling place returns • Uses voting system software and its security environment is designed

Test Detail	Test Methodology
Test Case Name	**Security**
Security Test Sub Type	**Description**
	such that data, which is accessible to interactive queries, resides in an external file, or database, that is created and maintained by the election software under the restrictions applying to any other output report, namely, that: o The output file or database has no provision for write-access back to the system o Persons whose only authorized access is to the file or database are denied write-access, both to the file or database, and to the system **11.19** The system transmits data over public telecommunications networks such that: (V1:6.6.1) • Digital signatures are employed for all communications between the vote server and other devices that communicate with the server over the network • At least two authorized election officials are required to activate any critical operation regarding the processing of ballots transmitted over a public communications network, i.e. the passwords or cryptographic keys of at least two employees are required to perform processing of votes
12. External Access	SysTest Labs will validate that the Voting System meets applicable FEC VSS 2002 Voting Standards to prohibit or limit access to partial or early election returns from unauthorized persons or processes. Using well-defined, repeatable testing methods and inspection processes, SysTest Labs will validate that capabilities, controls, and policies exist that are effective to limit external access to incomplete or early election returns from unauthorized persons or processes: **12.1** Blocked Central Count Environment Access to Incomplete Election Returns (V1:6.5.6.a)

Approval Signatures

SysTest Labs:

James M Nilius
VSTL Director
March 28, 2008

Client:

Sue Munguia
Director of Certification
March 28, 2008

End of Certification Test Plan