Election Assistance Commission
Voting System Certification Testing

Certification Test Plan
Document Number 07-V-ESS-035-CTP-01, Rev 10.0
December 9, 2008

Prepared for:

Vendor Name	Election Systems & Software
Vendor System	Election Systems and Software (ES&S) Unity 4.0 Voting System
EAC Application No.	ESS0702
Vendor Address	11208 John Galt Boulevard Omaha, NE 68137-2364

Prepared by:

216 16th St.
Suite 700
Denver, CO 80202

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 #
07/30/2007	Draft Initial Certification Test Plan – SysTest Labs	R. Tognetti	Rev. 00
08/02/2007	Initial submission to the EAC	T. Damour, J. Garcia	Rev. 01
12/18/2007	Updates to Rev 01 based on feedback from the EAC dated 11/26/2007	B. Phillips, J. Garcia, S. Holt, M. Hilgert, K. Swift	Rev. 02
1/22/2008	Updates based on feedback from Brian Phillips	K. Swift	Rev. 03
2/01/2008	Updates based on vendor and EAC feedback	K. Swift, A. Backlund	Rev. 04
2/7/2008	Updates based on vendor feedback	K. Swift	Rev. 05
2/15/2008	Added Accuracy TC to Appendix. Removed reference to the Electronic Poll Book from Telecommunications TC. Changed Telecommunications, Readiness, and Accuracy Test Cases to functional, not system-level. Corrected VSS references in the Security Test Case. Made minor corrections to table and attachment references. Added DS200 to Emission Testing performed by NCEE. Removed statement regarding storage of artifacts (Sec. 5.1). Moved Approval Signatures after Appendix A. Removed Attachment F.	K. Swift	Rev. 06
3/18/2008	Added Attachment I. Updates based on EAC feedback. Changes made for manufacturer of AutoMARK (ATS) products to ES&S.	K. Swift M. Hilgert	Rev. 07
5/19/2008	Updates based on EAC feedback. Added Attachment J. Added Volume Test case to Appendix A	M. Hilgert, A. Backlund, K. Swift	Rev. 8.0
10/24/08	Modified Appendix A Added SLP table to section 1.4 Added Test Cases to Appendix A Updated section 6.5 Updated Security Table in Appendix A Updated core definition in Appendix A Updated section 4.3.6 Security Testing Updated section 2.1.2.2 with Evolution of Testing Updated 3.2 Hardware Updated COTS information under 4.3.6 Added ES&S Unity 4.0 Security Functional Testing table Accepted all formatting changes	K.McGee D.Valdez K. Swift	Rev. 9.0
10/29/08	Section 4.3 updated with Volume, Stress, Performance, and Error Recovery Information	R. Thomas	Rev. 9.0
11/17/08	Table 9 updated to reflect current status of test cases Page 60 section 6.5 updated with additional requirements and additional error restoration information.	R. Thomas	Rev. 9.1

Date	Description of Revision	Author	Revision #
	Signature page updated Updated table in section 4.3.6		
12/09/08	Removed Compact Flash Multi Card Reader/Writer reference from Table 2 Removed Compact Flash Multi Card Reader/Writer (gang-burner) reference from Table 5 Updated Software and Hardware Version/Revision numbers Updated Section 1.4.1, SysTest Lab Procedures List	D. Forester	Rev. 10.0

TABLE OF CONTENTS

1 INTRODUCTION 6

1.1 CERTIFICATION TEST PLAN ATTACHMENTS 7
1.2 SCOPE OF THE ES&S UNITY 4.0 VOTING SYSTEM 8
1.3 APPLICABLE STANDARDS 11
1.3.1 Applicable Voting System Standards 11
1.3.2 Applicable Testing Standards 11
1.4 REFERENCES 11
1.4.1 All testing will be conducted following the SysTest Lab Procedures: 11
1.4.2 Applicable RFI's and NOC's listed in Appendix B 12
1.5 TERMS, ABBREVIATIONS AND DEFINITIONS 13

2 PRE-CERTIFICATION TESTS 15

2.1 PRE-CERTIFICATION TEST ACTIVITY 15
2.1.1 Physical Configuration Audit 16
2.1.2 Functional Configuration Audit 18
2.1.3 Hardware Environmental Testing Assessment 18
2.2 PRE-CERTIFICATION ASSESSMENT RESULTS 19
2.2.1 Physical Configuration Audit 19
2.2.2 Hardware Environmental Analysis of Testing Results 21

3 MATERIALS REQUIRED FOR TESTING 22

3.1 SOFTWARE/FIRMWARE 22
3.2 EQUIPMENT (HARDWARE) 26
3.3 TEST MATERIALS 32
3.4 DELIVERABLE MATERIALS 33
3.5 PROPRIETARY DATA 33

4 TEST SPECIFICATIONS 34

4.1 HARDWARE CONFIGURATION AND DESIGN 34
4.2 SOFTWARE SYSTEM FUNCTIONS 34
4.3 TEST CASE DESIGN 34
4.3.1 Hardware Environmental Test Case Design 34
4.3.2 Acceptance of Previous Hardware Test Results 35
4.3.3 Software Module Test Case Design and Data 35
4.3.4 Software Functional Test Case Design 36
4.3.5 Accuracy Test 38
4.3.6 Security Test 39
4.3.7 System Level Test Case Design 46
4.3.8 Sampling Methodology 48
4.3.9 Additional Functional Testing 48
4.3.10 Volume, Performance, Stress and Error Recovery Test Approach 50

5 TEST DATA 58

5.1 DATA RECORDING 58
5.2 TEST DATA CRITERIA 58
5.3 TEST DATA REDUCTION 58

6 TEST PROCEDURE AND CONDITIONS 59

6.1 FACILITY REQUIREMENTS 59
6.2 TEST SETUP 59
6.3 TEST SEQUENCE 59

6.4 TEST OPERATIONS PROCEDURES 60
6.5 TEST ERROR RECOVERY 61

7 APPENDIX A – TEST CASES 62

7.1 SAMPLING OF VENDOR TESTING RESULTS 62
7.2 SYSTEM LEVEL TEST RESULTS 63

8 APPENDIX B – EAC INTERPRETATIONS 123

APPROVAL SIGNATURES 124

LIST OF TABLES

Table 1 - Summary of Unity 4.0 Voting System Components 8
Table 2 - Matrix of Terms & Abbreviations provided by the vendor 13
Table 3 - Matrix of Required Software/Firmware 22
Table 4 - Matrix of COTS Software/Firmware 24
Table 5 - Matrix of Required Hardware 26
Table 6 - Matrix of Test Materials 32
Table 7 - Matrix of System Functional Testing 36
Table 8 - ES&S Unity 4.0 Security Functional Testing 41
Table 9 - Matrix of System Level and Other Functional Testing 47
Table 10 - Matrix of Additional Testing 49
Table 11 - Matrix of Testing Tasks 59

1 INTRODUCTION

This Certification Test Plan outlines the approach SysTest Labs will implement to perform Election Assistance Commission (EAC) certification testing of the Election Systems and Software (ES&S) Unity 4.0 voting system to the approved Voting System Standards (VSS), version 2002. The purpose of this document is to provide a clear and precise plan for test elements required to ensure effective Certification testing of components outlined in section 1.2 of this Certification Test Plan.

This Certification Test Plan:

- Identifies items that need 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 Unity 4.0 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 Unity 4.0 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' 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)
    - Iterative review of ES&S System Test & Verification Specification and all of ES&S's completed testing to ES&S System Requirements Specification, as outlined in the FEC VSS Volume 1, Section 2
    - Iterative hardware environmental 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, 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: Unity 4.0 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 Certifications
10. Attachment I: VSS FCA - SysTest TC Trace
11. Attachment J: EAC Requirements Matrix – **PROPRIETARY**

1.2 Scope of the ES&S Unity 4.0 Voting System

This section provides a brief overview of the scope of the ES&S Unity 4.0 voting system components.

Please note that each of the items listed in Table 1- Summary of Unity 4.0 Voting System Components and Figure 2 - Overview of the Unity 4.0 Components are explicitly defined in tables 1, 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 solely by ES&S in the TDP items delivered to both SysTest Labs and the EAC.

Table 1 - Summary of Unity 4.0 Voting System Components

Software/Firmware	Hardware
Election Management System (EMS) • Audit Manager • Election Data Manager • AutoMARK Information Management System (AIMS) • ES&S Ballot Image Manager (includes Ballot on -Demand) • iVotronic Image Manager • Hardware Programming Manager • Data Acquisition Manager • Election Reporting Manager	• Compact Flash Multi-Card Reader/Writer • Automatic Bar Code Reader • Hand held bar code scanner (Voyager) • iVotronic DRE with a 4.5-inch Real-Time Audit Log printer • iVotronic DRE with a 9-inch Real-Time Audit Log printer • iVotronic DRE without a 4.5-inch Real-Time Audit Log printer • iVotronic DRE without a 9-inch Real-Time Audit Log printer • iVotronic DRE with stand-alone printer • iVotronic DRE with the communication pack • AutoMARK Voter Assist Terminals • Model 100 precinct scanner with steel ballot box • intElect DS200 precinct/central count scanner with steel ballot box • intElect DS200 precinct/central count scanner with plastic ballot box • Model 650 central count scanners with green light optical sensor to read ovals on the left and right • Model 650 central count scanners with red light optical sensors to read ovals on the left

Figure 1 - Overview of Unity 4.0 Election Support Process

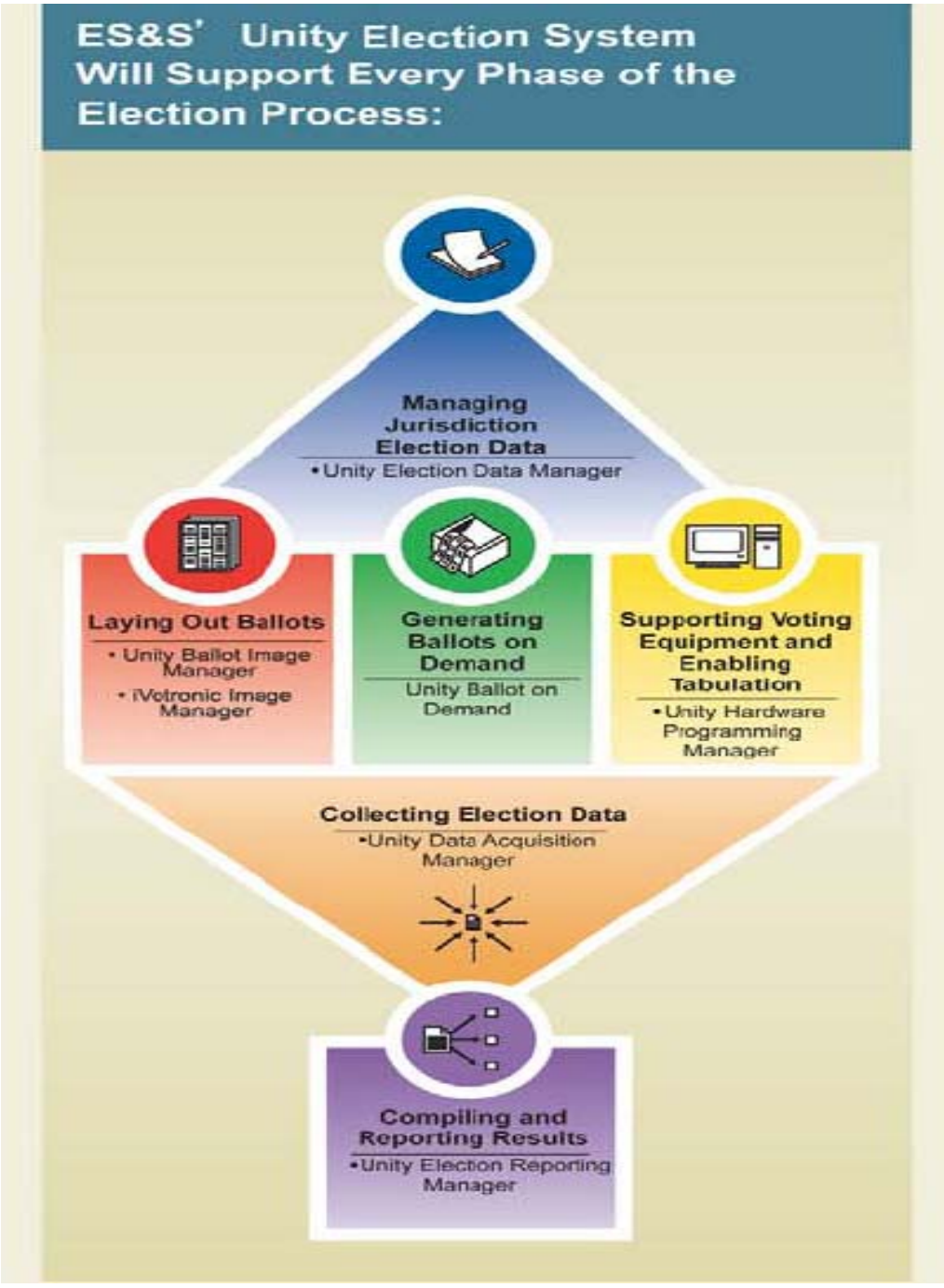
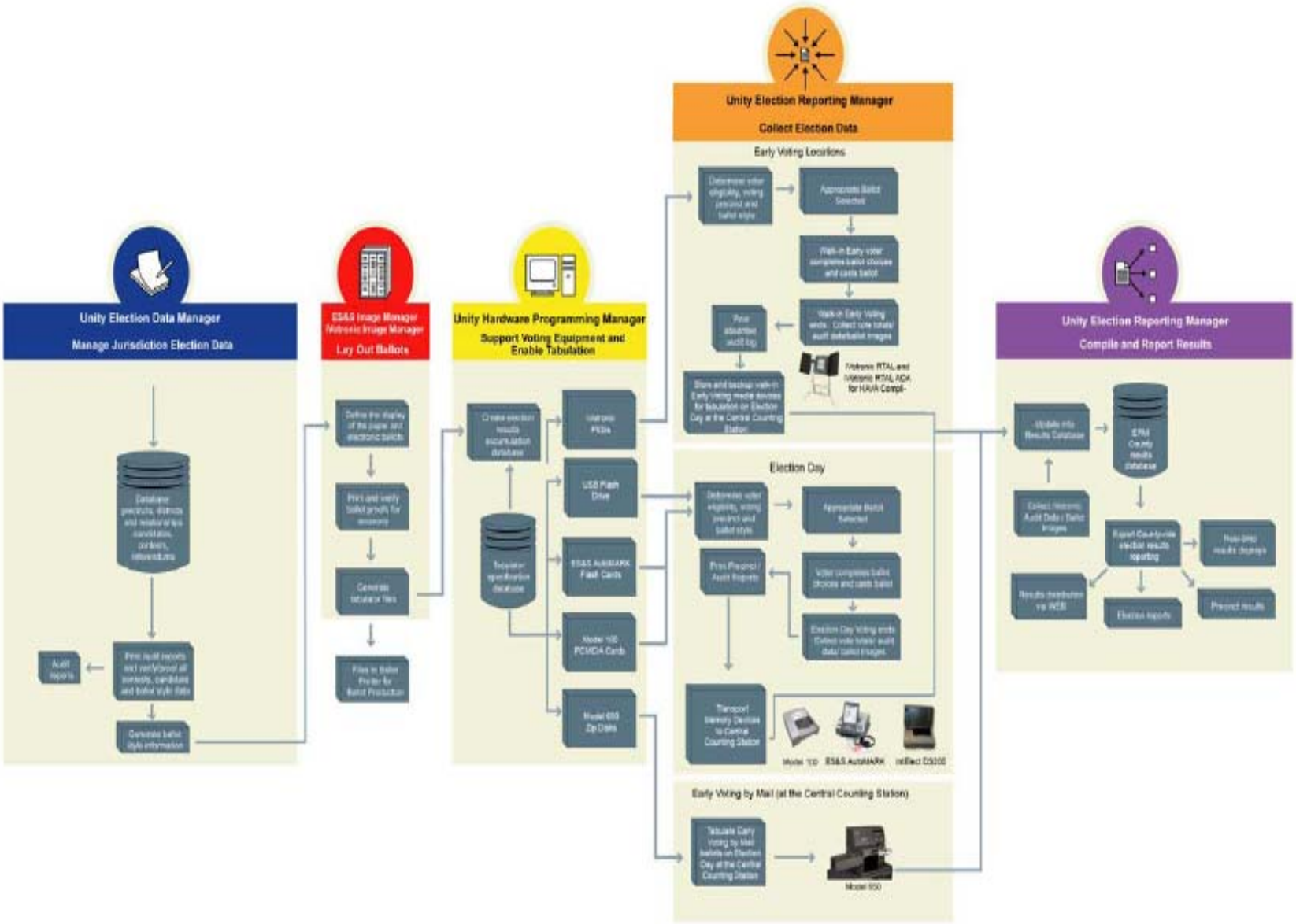


Figure 2 - Overview of the Unity 4.0 Components



1.3 Applicable Standards

1.3.1 Applicable Voting System Standards

All testing will determine whether or not the Election Systems and Software (ES&S) Unity 4.0 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 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

1.4.1 All testing will be conducted following the SysTest Lab Procedures:

- SysTest Labs VSTL Quality System Manual rev1.4
- Accuracy and Lab Policies Training rev1.0
- SLP-QS-01 rev2.2 - Quality System Document Structure Usage
- SLP-QS-02 rev2.6 - Change Control & Approvals
- SLP-QS-03 rev2.3 - Configuration Mgmt & Record Mgmt
- SLP-QS-04 rev2.4 - Quality System Audits
- SLP-QS-05 rev2.2 - Process Quality Control & Internal Audits
- SLP-QS-06 rev2.3 - Management Reviews
- SLP-QS-08 rev2.2 - Control of Nonconforming Work
- SLP-QS-09 rev2.3 - Preventive and Corrective Actions
- SLP-QS-10 rev2.4 - Supplier Agreements and Management
- SLP-QS-11 rev2.2 - Review of Requests, Tenders, and Contracts

[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.

- SLP-QS-12 rev3.1 - Service to Clients & Handling of Concerns
- SLP-TR-01 rev3.2 - Identifying Employee Training Needs
- SLP-TR-02 rev3.2 - Conducting Training
- TR Doc VC-01 rev1.0 - Voting training - Election Process
- SLP-VC-GL rev1.1 - SysTest Labs Voting Glossary
- FORM-VC-02 rev00 - Security Log.xls
- SLP-VC-02 rev2.1 - Ensuring Protection of Items and Data
- SLP-VC-03 rev1.0 - Communication with Manufacturers
- SLP-VC-05 rev2.1 - Certification Test Plan
- SLP-VC-06 rev2.2 - Deliverables Check-in
- SLP-VC-07 rev2.1 - PCA Doc Review
- SLP-VC-08 rev2.1 - FCA Vendor Test Review
- SLP-VC-09 rev2.2 - PCA Software & Hardware Configuration Audit
- SLP-VC-10 rev2.0 - Test Method Development and Validation
- SLP-VC-11a rev2.3 - PCA Source Code Review
- SLP-VC-11b rev1.3 - PCA Augmented Source Code Review
- SLP-VC-12a rev1.0 - Readiness Validation
- SLP-VC-12b rev3.0 - Preparing Test Suites
- SLP-VC-13 rev2.6 - Trusted Build
- SLP-VC-14 rev2.0 - Preparing Source Code Review for Certification Report
- SLP-VC-15 rev2.4 - FCA Test Execution—Functional, System
- SLP-VC-16 rev2.3 - Test Execution – Regression
- SLP-VC-18 rev2.3 - Discrepancy Report & Test Review Corrections
- SLP-VC-19 rev2.2 - Certification Report
- SLP-VC-20 rev2.0 - Engineering Change Evaluation Reporting
- SLP-VC-21 rev2.2 - Releasing Reports
- SLP-VC-22 rev2.1 – Archiving
- SLP-VC-23 rev2.1 - Hardware Test Management
- SLP-VC-24 rev2.0 - Subcontractor Lab Management
- SLP-VC-25 rev2.1 - Measurement & Analysis
- SLP-VC-26 rev1.0 - Test Equipment Calibration and Maintenance
- SLP-VC-29 rev1.0 - Controlling and Versioning Test Documents

1.4.2 Applicable RFI's and NOC's listed in Appendix B

1.5 Terms, Abbreviations and Definitions

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

Term	Abbrev.	Definition
Audit Manager	AM	Audit Manager is ES&S' tracking program for the Unity software suite. AM tracks user activity in AM, EDM and ESSIM.
Automatic Bar Code Reader	ABCR	The ABCR is a device that audits and recounts the printout generated by the iVotronic RTAL printer. The ABCR device interfaces with ABCR software installed on a PC to generate reports based upon the scanned barcodes from the RTAL printout.
AutoMARK Information Management System	AIMS	Software that facilitates creation of the election database, or conversion of a 3rd party election database, for installation on the VAT.
AutoMARK Voter Assist Terminal	VAT	AutoMARK's optical paper ballot marking device for disabled voters and alternative languages
Ballot On Demand	BOD	Election officials use Ballot on Demand to print test ballots, early voting ballots and ballots for polling places that run short of ballot stock on Election Day.
Binary Logic Input Device		Alternative accessible appliance that is connected to the AutoMARK Voter Assist Terminal through a stereo jack, enabling the voter to issue either a yes or no command. These devices may include foot pedals and Sip/Puff tubes.
Data Acquisition Manager	DAM	The ES&S Data Acquisition Manager software is used to transmit election results over a network connection from ES&S ballot counting equipment to a central count location.
Delkin & SanDisk USB		A USB flash drive to store the DS200 scanner's election definition, audit log and other election-specific information.
Election Data Manager	EDM	Election Data Manager is a database system that stores all of a jurisdiction's precinct, office, and candidate information. It is used in conjunction with other Unity software to format and print ballots, program ballot scanning equipment, and produce Election Day reports.
Election Reporting Manager	ERM	The Election Reporting Manager is an election results reporting program, used to generate paper and electronic reports for poll workers, candidates, and the media. ERM can display updated election totals on a monitor as ballot data is tabulated and can send result reports directly to media outlets over the Internet. ERM is designed to support a wide range of ES&S ballot scanning equipment and can produce reports for both central count systems and precinct count systems.
ES&S Ballot Image Manager	ESSIM	ES&S Ballot Image Manager is a publishing tool used to design and print ballots with the election information stored in EDM.
Flash Memory Card	FMC	The FMC supplies ballot content information to the VAT.
iVotronic		The iVotronic is a DRE (direct recording electronic) touch screen that displays ballots and records votes. The iVotronic addresses accessibility requirements through the use of voice files, font type and size, and color combinations. There are two sizes of iVotronics: 12 inch and 15 inch. There are two types of iVotronics: ADA and Non-ADA. The ADA iVotronics are manufactured with either a 3-key, 4-key, or 6-key configuration. The 6-key allows the use of the sip and puff. The Non-ADA iVotronics are manufactured without keys.

Term	Abbrev.	Definition
iVotronic Image Manager	iVIM	The iVotronic Image Manager enables the user to create and format graphic ballot screens for the iVotronic-voting device.
Hardware Programming Manager	HPM	Hardware Programming Manager enables the user to import, format, and convert the election definition files for ballot scanning equipment and DREs.
intElect DS200	DS200	The intElect DS200 precinct or central count ballot scanner is part of a jurisdiction-wide election tabulating system. Voters make selections on a ballot and then insert their ballots directly into the DS200 at the polling place. The scanner tabulates votes and sorts a ballot as soon as a voter inserts it and then feeds the ballot into the attached ballot storage bin accepting ballots inserted in any direction and reads both sides of the ballot simultaneously.
Model 100	M100	The Model 100 precinct ballot scanner is part of a jurisdiction-wide election tabulating system. Voters make selections on a ballot and then insert their ballots directly into the Model 100 at the polling place. The scanner tabulates votes and sorts a ballot as soon as a voter inserts it and then feeds the ballot into the attached ballot storage bin accepting ballots inserted in any direction and reads both sides of the ballot simultaneously.
Model 650	M650	The Model 650 is an optical scan central count counter that is used to scan ballots at a central count location. The M650 scans up to 350 ballots per minute, counts different sizes (11, 14, 17, 19 inches) of ballots and can read voting marks on the right or left of the ballot column. The M650 prints results reports and saves results to a zip disk.
PCMCIA		PCMCIA card stores the M100 election definition, as well as voter results, exactly mirroring the ballot contents and issues as defined by election officials.
Personalized Electronic Ballots	PEB	An electronic ballot that a jurisdiction defines for use with the iVotronic to open polls, load ballots and collect votes from each terminal at the end of an election day.
Real-Time Audit Log Printer	RTAL	The Real-Time Audit Log Printer records each voter's actions on a paper audit log in real time, including all selections and de-selections. The paper audit log can be viewed but not touched by the voter prior to casting a vote, as the paper is behind a clear plastic cover. Under-voted contests and a two-dimension bar code of the votes are appended to the audit entries and the paper advances out of the view window in either a 9-inch or 4.5-inch window.
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 will conduct an assessment 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, and firmware components of the ES&S Unity 4.0 voting system. For a complete list of all items included in the TDP, please refer to Attachment A.

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. The location of verification procedures for requirements not applicable to Appendix A are noted in Attachment J.

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. Where SysTest identifies insufficient testing by the vendor was performed, we include those requirements in our test cases.

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 conducted 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 is identified and included either in the test cases developed by SysTest Labs or executed as part of our sampling guidelines.

It should be noted that this Certification Testing does not include state specific issues unless specifically requested by the vendor or unless the state issue impacts any Federal election. Please refer to Attachment B for all vendor-supported functionality.

2.1.1 Physical Configuration Audit

2.1.1.1 Document Review

SysTest Labs conducted a PCA review of the documents submitted for review in the ES&S Unity 4.0 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

Each document included in the Unity 4.0 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.

2.1.1.2 Source Code Review

The ES&S Unity 4.0 test campaign is a full certification as defined by the EAC. A full certification requires that all program source code undergo a full source code review. SysTest Labs has conducted a source code review of all source code submitted as a part of the TDP. The coding languages for the Unity 4.0 voting system include the following:

- C
- C++
- JAVA
- VB
- Assembler
- COBOL

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
- 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

SysTest Labs utilizes a team approach in reviewing and managing the tasks of receiving the code to be reviewed, determining the volume of code to be reviewed, reviewing the vendor's internal coding standards and determining if there are any variances from the prescribed Standards, creating the review work documents, distributing the code to be reviewed along with the created work documents to the project code reviewers, reviewing the code, performing peer reviews, creating discrepancy reports, and receiving modified code and other vendor responses.

2.1.1.3 Trusted Build

Prior to testing, SysTest Labs will conduct a trusted build according to the detailed trusted build procedures provided by the vendor in the TDP and the EAC Testing and Certification Program Manual. The process includes interviews of key vendor staff to evaluate vendor processes and process conformance in the areas of configuration management and quality assurance. The following staff positions are interviewed: Developer and Senior Software Engineer. Preparation for the trusted build includes obtaining and reviewing the vendor-defined procedures for constructing the build platform, verifying the target build platform, and acquiring the installation material and VSTL reviewed source code.

COTS Tools:

- Acronis Software – Performs hard drive wiping and imaging.
- SLAX Linux boot CD – Performs hash values with “sha1deep” command to produce SHA1 hashes.

The source code is provided by the vendor and hash values are compared to the hash values of the code from the VSTL to assure that reviewed code is being built. The hash values are generated with the “sha1deep” command line command to produce SHA1 hashes. A build machine is erased by the VSTL in preparation for the build with a clean machine. Execution of the trusted build complies with the vendor’s detailed build procedures for constructing the build environment and only the items listed in those procedures will be placed on the machine. A hash is taken of the build environment after this process is complete (TCPM 5.6.1.3). The VSTL approved source code is placed on the machine for the build and another hash and image is obtained (TCPM 5.6.2.2 & 5.6.2.3). The next image and hash is taken after following the vendor’s build procedures to compile the source code and produce the executable code (TCPM 5.6.3.1). Additional hashes are taken of any installation CDs that are made during the build (TCPM 5.6.3.3). All hashes, images, and copies of the VSTL approved source code are kept on a VSTL archive during the entire build procedure and all build results are copied to the archive after the build is complete.

The conclusion of the trusted build consists of record-keeping and archiving procedures that occur at SysTest Labs. The report contains any unique identifiers, results of the build with version numbers and dates and descriptions of all hashes and images in the repository. VSTL

backup procedures are performed on all Trusted Build media and records to create an accessible and safe copy. A copy of the resulting media and records are submitted to the EAC-approved software repository as part of finalizing the Certification Test Report. All items in section 5.8 of the Testing and Certification Program Manual are the responsibility of the vendors to address.

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 Unity 4.0 test cases delivered as part of the initial delivery of the Unity 4.0 voting system TDP. These test cases are designed and executed by ES&S for QA and testing of the Unity 4.0 voting system. The Unity 4.0 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.

2.1.2.2 Evolution of Testing

SysTest Labs Inc. will maintain a spreadsheet/database of all known vulnerabilities or issues for all Voting Systems. These vulnerabilities or issues will be acquired through advisories from the Vendor, EAC or from State Sponsored Security Audits/tests. We will append all new reports to the list as they are received and identify the applicability of the vulnerability with respect to scope of the requirements, uniqueness and scenario under which it was identified. The Test Case for all applicable issues will be identified at this time also. When new Test engagements are being developed it will be the responsibility of the Test manager / security manager to include tests for all identified vulnerabilities in the Vendor Specific Test Steps. In this way we will ensure that a knowledge transfer between vendor takes place and any newly identified vulnerabilities are addressed.

2.1.3 Hardware Environmental Testing Assessment

The acceptance and use of previous hardware environmental testing and certification 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 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 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 Unity 4.0 certification began in April 2007, and was completed in January of 2008. 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 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 both the Omaha, NE offices of ES&S, and at the SysTest Labs office in Denver. The first Trusted Build was completed July 30, 2007 in Omaha, NE, and it resulted in the Trusted Build platform PC, which was used for Trusted Builds of ES&S products. Subsequently a separate Trusted Build platform PC will be built at the SysTest site for Trusted Builds of the AutoMARK products.

Trusted Builds were performed with ES&S, and will be performed for AutoMARK products, as described under Section 2.1.1 above, on the respective build platform PCs in order to provide the compiled software and firmware installation packages to be used in the certification testing.

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 Unity 4.0 voting system TDP test cases and subsequent test results are consistent with the VSS, version 2002.

For all requirements that were identified as not tested or insufficiently tested, SysTest Labs will design and develop tests cases, test data, and test procedures and will add these to SysTest Labs' list of VSTL Test Cases for Unity 4.0 certification test execution.

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

- Operational Status Check Test Case (Operational Test Case Status REV 00 H.xls)
- Readiness Test Case (Readiness Functional Test Execution REV H00.xls)
- Functional Test Case (High Capacity Ballot/Various Sampling) Functional Test Execution 01 Rev H01.xls
- Maintainability Test Case (Maintainbility Test Rev 01 08-19-08.xls)
- SysTest Labs' GEN01 - General Election Test Case (System - Gen01 Rev H00.xls)
- SysTest Labs' GEN02 - Straight Party Test Case (System - Gen02 - Straight Party Rev H00.xls)
- SysTest Labs' GEN02 - Pennsylvania Straight Party with Cross Party Endorsement Test Case
- SysTest Labs' GEN03 - Usability & Accessibility Test Case (System - Gen03 - Add Languages Rev H00.xls)
- SysTest Labs' PRI01 - Open Primary Test Case
- SysTest Labs' PRI01 - Open Primary with Pick a Party/Party Preference Test Case (System - Pri01 - Pick a Party Rev H00 08.13.08.xls)
- SysTest Labs' PRI02 - Closed Primary Test Case (Pri02 - Closed Primary Rev H00.xls)
- SysTest Labs' 40HTEST1 – General Straight Party (System - 40HTEST1 Rev H00 (General SP).xls)
- OhioTest – General Election w/ Party Affiliation (OhioTest - Gen01 & PRI02 Rev 00.xls)
- SysTest Labs' 40HTEST3 – Functional (40HTEST3 Rev00 General.xls)
- SysTest Labs' 40HTEST4 – Functional (40HTEST4 Rev00 General.xls)
- SysTest Labs' 40HTEST5 – Functional (40HTEST5 Rev 00.xls)
- SysTest Labs' 3000 Precincts – Functional (3000 PCTS Rev01.xls)
- SysTest Labs' Security Test Case (SEC Test Case Rev 00 Template Rev 08-11-2008.xls)
- SysTest Labs' Telecommunications Test Case
- SysTest Labs' Accuracy Test Case (Accuracy Test Case Rev00 iVo.xls, Accuracy Test Case Rev00 M100 v00.xls, Accuracy Test Case Rev00 M650 v00.xls, Accuracy Test Case Rev00 DS200 v3.xls
- SysTest Labs' Volume Test Case
- SysTest Labs' Stress Test Case
- Systest Labs' Performance Test Case
- Systest Labs' Error Recovery Test Case
- SysTest Labs' Electrical Supply Test Case (40Heavy Electrical Supply Rev00.xls)
- PCA System Configuration Checklist_HW_Unity 4 0 Traveler Rev 05 HEAVY.xls

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

2.2.2 Hardware Environmental Analysis of Testing Results

Test reports from previous hardware testing 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, telecommunications, security and integrated system tests. Not all items listed below are required to run the Unity 4.0 voting system. However, all items listed were part of the certification test effort. Should a software version modification become necessary, an amended Certification 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.

For a complete description of the minimal PC configuration required, review the section "System Requirements" in all System Operations Procedures documents for each product. These documents are contained in the vendor's TDP.

Table 3 - Matrix of Required Software/Firmware

Application(s)	Manufacturer	Version	Description
Audit Manager	ES&S	7.5.0.0	Audit Manager provides security and user tracking for itself, Election Data Manager and Ballot Image Manager. Audit Manager runs in the background of the other Unity programs and provides password security and a real-time audit log of all user inputs and system outputs. Jurisdiction Officials use Audit Manager to set Unity system passwords and track user activity.
Election Data Manager	ES&S	7.8.0.0	Election Data Manager is a single-entry database that stores all of a jurisdiction's precinct, office, and candidate information. Election Data Manager is used in conjunction with other Unity software to format and print ballots, program ballot scanning equipment, and produce Election Day reports.
ES&S Ballot Image Manager (with Ballot on Demand)	ES&S	7.7.0.0	ESSIM is a desktop publishing tool that is used to design and print ES&S paper ballots. ESSIM uses ballot style information created by Unity Election Data Manager to display the WYSIWYG ballots. Ballot On Demand (BOD) is an accessory program that you can use to print individual, Election Day ballots directly from ESSIM.
iVotronic Image Manager	ES&S	3.2.0.0	iVotronic Image Manager (iVIM) is a desktop publishing tool that is used to design and generate graphic ballots for the iVotronic precinct voting system. iVIM uses ballot style information created by Unity Election Data Manager to display the WYSIWYG ballots. iVotronic Image Manager also allows the user to view the ballot in different languages, and create multiple displays for the same ballot. Ballots generated by iVotronic Image Manager comply with ADA (Americans with Disabilities Act) requirements using voice files, specific font type and size, and color combinations.
Hardware Programming	ES&S	5.7.0.0	Hardware Programming Manager (HPM) is a complete election package that enables the user to import, format,

Application(s)	Manufacturer	Version	Description
Manager			and convert the election file; define districts; specify election contests and candidates; create election definitions for ballot scanning equipment; burn M100 PCMCIA Cards, DS200 USB memory sticks, M650 zip disks, or PEBs; and create the Data Acquisition Manager Precinct List. The Hardware Programming Manager is primarily used for converting the election IFC file for use with the Election Reporting Manager and for creating and loading election parameters; however, it may also be used for coding the election. The Unity Hardware Programming Manager seamlessly programs the ES&S election tabulation hardware with election-specific information retrieved from the Unity Election Data Manager (EDM). **NOTE: Creating an election definition from scratch in HPM is not supported in the Unity 4.0 certification.**
Data Acquisition Manager	ES&S	6.1.3.0	The Unity Data Acquisition Manager (DAM) is a client-server application that collects election data from ES&S voting systems and transmits the data directly from the polls or regional sites via modem transmission to the host election server for the purpose of results accumulation, reporting, and display. The Data Acquisition Manager allows users to transfer election results from remote polling sites to a jurisdiction's election headquarters. Data Acquisition Manager has two software configurations: Data Acquisition Manager Remote and Acquisition Manager Host. Poll workers use the remote configuration to transfer election results to the central collection location. Officials at the central site use the host configuration to receive election data from polling places. Workers at the central location load collected results into Election Reporting Manager™ to format, print, and display final election reports.
Election Reporting Manager	ES&S	7.5.2.0	Election Reporting Manager (ERM) is ES&S' election results reporting program. ERM generates paper and electronic reports for election workers, candidates, and the media. ERM can also display updated election totals on a monitor as ballot data is tabulated, and it can send results reports directly to media outlets. Election Reporting Manager is designed to support a wide range of ES&S ballot scanning equipment and can produce reports for both central-count systems and precinct-count systems.
AIMS	ES&S	1.3.57	The AutoMARK Management Information 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 AIMS election database. In lieu of the import procedure,

Application(s)	Manufacturer	Version	Description
			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.

Table 4 - Matrix of COTS Software/Firmware

COTS Application(s)	Manufacturer	Version	Description
Required COTS software for the Unity 4.0 voting system			
Windows XP Professional	Microsoft Corporation	2002 Service Pack 2	COTS software for all Applications listed above.
RM COBOL RUNTIME System	RM/COBOL	11.01	COTS software for the ERM, HPM
Adobe Type Manager (includes Adobe Type Basics and Adobe Type Manager Light)	Adobe	4.1	COTS software for ESSIM, BOD
OmniDrive USB Professional	Omni	No version	COTS software for the HPM, ERM
PEB Reader	Pivot/ES&S	1.1.0.0	COTS software for HPM, ERM
Non-required COTS software for the Unity 4.0 voting system			
Broadcom Gigabit Integrated Controller	Broadcom	9.02.06	COTS software Voyager Hand scanner, and Desktop PCs.
C-Major Audio	SigmaTel	42.xx	COTS software Voyager Hand scanner, and Desktop PCs.
Conexant D110 MDC	Unknown	92 Modem	COTS software Voyager Hand scanner
Graphics Media Accelerator Driver for Mobile	Intel	No version	COTS software Voyager Hand scanner
MS Office Professional Edition 2003 (MS Word and Excel installed in the setup)	Microsoft Corporation	11.0.7969.0	COTS software Voyager Hand scanner
O2Micro Smartcard Driver	O2Micro	2.26.0000	COTS software Voyager Hand scanner, and Desktop PCs.
ATI Display Driver	ATI	No version	COTS software for the Server
Dell OpenManage Array Manager	Dell	No version	COTS software for the Server
DirectX Hotfix – KB839643	Microsoft Corporation	No version	COTS software for the Server
HP Laser Jet 2300 Uninstaller	HP	No version	COTS software for the Server
Intel® PRO Intelligent	Intel	2.01.1000	COTS software for the Server

COTS Application(s)	Manufacturer	Version	Description
Installer Intel® PRO Network Adapters and Drivers			
Internet Explorer Q867801	Microsoft Corporation	No version	COTS software for the Server
LiveUpdate	Symantec Corporation	1.7	COTS software for the Server
Symantec AntiVirus Client	Symantec Corporation	8.0.0.374	COTS software for the Server
Outlook Express Q823353	Microsoft Corporation	No version	COTS software for the Server
Windows 2000	Microsoft Corporation	Service Pack 4	COTS software for the Server
Windows 2000 Administration Tools	Microsoft Corporation	5.0.0.0000	COTS software for the Server
Microsoft Health Monitor 2.1	Microsoft Corporation	2.10.1850.0000	COTS software for the Server
Microsoft Internet Security and Acceleration Server	Microsoft Corporation	3.0.1200	COTS software for the Server
Microsoft Shared Fax	Microsoft Corporation	1.0000	COTS software for the Server
Microsoft Small Business	Microsoft Corporation	Server 2000	COTS software for the Server
Microsoft Data Access Components KB870669	Microsoft Corporation	No version	COTS software for the Server
Microsoft.NET Framework	Microsoft Corporation	1.1.4322	COTS software for the Server
Windows 2000 Hotfix: - KB819696, - KB820888, - KB822831, - KB823182, - KB823559, - KB82410, - KB824141, - KB824146, - KB825119, - KB826232, - KB828028, - KB828035, - KB828741, - KB828749, - KB835732, - KB837001 - KB839643, - KB839645, - KB840315, - KB841872, - KB841873, - KB842526,	Microsoft Corporation	- 20030703.183130 - 20030604.152521 - 20030611.114034 - 20030618.121409 - 20030627.135515 - 20030716.151320 - 20030805.151423 - 20030823.144456 - 20030827.151123 - 20031007.160553 - 20040122.114409 - 20031023.142138 - 20040311.130332 - 20031023.124056 - 20040323.171849 - - 20040506.120130 - 0040519.160457 - 20040622.153749 - 20040520.90850 - 20040610.95344 - 20040521.202909	COTS software for the Server
Intel ProEthernet Adapter and Software	Intel	No version	COTS Software on the Desktop PCs
SeaCOM	Unknown	No version	COTS Software on the Desktop PCs
SoundMAX	Unknown	No version	COTS Software on the Desktop PCs
ATI Software Uninstall Utility	ATI	6.14.10.10.14	COTS Software on the Desktop PCs

COTS Application(s)	Manufacturer	Version	Description
ATI Control Panel	ATI	6.14.10.5173	COTS Software on the Desktop PCs
ATI Display Driver	ATI	8.20-051110A1-028793C-Dell	COTS Software on the Desktop PCs
Conexant D480mdc	Unknown	92 modem	COTS Software on the Desktop PCs

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 Unity 4.0 voting system. However, all items listed were part of this certification test effort. All equipment was provided by ES&S; SysTest Labs staff installed required COTS software, as needed, per vendor's documentation; uploaded all executables and installs on the equipment, while the equipment and Trusted Build executables and installs were under the control of SysTest Labs.

Table 5 - Matrix of Required Hardware

Item	Manufacturer	Model #	Version/Rev	Description
intElect DS200 (Scanner) (3)	ES&S	DS200	Hardware v. 1.2.0 & 1.2.1 DS200 Firmware 1.3.7.0 Power Management Firmware 1.2.0.0 Scanner Firmware 2.11.0.0	A precinct/central count ballot scanner. The scanner accepts ballots, tabulates votes, and sorts the ballots (if attached to a ballot box containing a diverter).
Steel ballot box without diverter	ES&S	N/A	N/A	A storage receptacle to store scanned ballots. (Used with M100 and DS200).
Model 100 (Scanner) –	ES&S	M100	Hardware v. 1.3.0 Firmware v. 5.4.0.0	A precinct ballot scanner. The scanner accepts ballots, tabulates votes, and sorts the ballots (if attached to a ballot box containing a diverter).
Model 100 (Scanner) –	ES&S	M100	Hardware v. 1.3.0 Firmware v. 5.4.0.0	A precinct ballot scanner. The scanner accepts ballots, tabulates votes, and sorts the ballots (if attached to a ballot box containing a diverter).
Steel ballot box	ES&S	N/A	N/A	A storage receptacle to sort and

Item	Manufacturer	Model #	Version/Rev	Description
w/ diverter)				store scanned ballots. (Used with M100 and DS200).
Plastic ballot box	ES&S	N/A	N/A	A storage receptacle to sort and store scanned ballots. (Used with M100 and DS200).
Model 650 – Red – Left (Scanner)	ES&S	M650	Hardware v. 1.2 Firmware v. 2.2.1.0	An optical scan central counter that is used to scan ballots at a central count location. The M650 prints results reports and saves results to a zip disk.
Model 650 – Green – Right (Scanner)	ES&S	M650	Hardware v. 1.1 Firmware v. 2.2.1.0	An optical scan counter that is used to scan ballots at a central count location. The M650 prints results reports and saves results to a zip disk.
Model 650 – Green – Left (Scanner)	ES&S	M650	Hardware v. 1.2 Firmware v. 2.2.1.0	An optical scan central counter that is used to scan ballots at a central count location. The M650 prints results reports and saves results to a zip disk.
12inch, 3 key iVotronic (DRE) –	ES&S	0105-096-90659	Hardware v. 1.1 Firmware v. 9.2.3.0	A DRE (direct recording electronic) touch screen that displays ballots and records votes. This is 12 inches with 3 keys ADA buttons.
12inch, Non-ADA iVotronic (DRE) –	ES&S	0105-096-90659	Hardware v. 1.1 Firmware v. 9.2.3.0	A DRE (direct recording electronic) touch screen that displays ballots and records votes. This is 12 inches with no ADA buttons.
15inch, 3 key iVotronic (DRE)	ES&S	9VDC 2770mA	Hardware v. 1.1 Firmware v. 9.2.3.0	A DRE (direct recording electronic) touch screen that displays ballots and records votes. This is 15 inches with 3 keys ADA buttons.
15inch, 4 Key iVotronic (DRE) –	ES&S	9VDC 2770mA	Hardware v. 1.1 Firmware v. 9.2.3.0	A DRE (direct recording electronic) touch screen that displays ballots and records votes. This is 15 inches with 4 keys ADA buttons.
15inch, 6 key iVotronic (DRE) –	ES&S	15” 9VDC 2770mA	Hardware v. 1.1 Firmware v. 9.2.3.0	A DRE (direct recording electronic) touch screen that displays ballots and records votes. This is a 15 inches with 6 key ADA buttons. The iVotronic 6 keys allows the use of the sip and puff.
15 inch, Non-ADA iVotronic (DRE) –	ES&S	0105-096-90659	Hardware v. 1.1 Firmware v. 9.2.3.0	A DRE (direct recording electronic) touch screen that displays ballots and records votes. This is 15 inches with no ADA buttons.

Item	Manufacturer	Model #	Version/Rev	Description
15 inch Supervisor iVotronic (RED) –	ES&S	9VDC 2770mA 0150-096-90659	Hardware v. 1.1 Firmware v. 9.2.3.0	Poll workers use supervisor equipment to open polls, load ballots onto voter PEBs or voting terminals, close the polls, and print results for the polling place.
iVotronic RTAL Booth 4.5 inch window	Booth: Pivot, Printer: Xten	N/A	Hardware v. N/A Firmware v. V012	The Real-Time Audit Log Printer records each voter's actions on a paper audit log in real time on a 4.5-inch window. This printer is attached to a private voting booth.
iVotronic RTAL Booth 9 inch window	Booth: Pivot, Printer: Xten	N/A	Hardware v. N/A Firmware v. V012	The Real-Time Audit Log Printer records each voter's actions on a paper audit log in real time on a 9-inch window. This printer is attached to a private voting booth.
ABCR (Automatic Bar Code Reader) –	JADAK	N/A	Hardware v. B Firmware v. 29	The ABCR is a device that audits and recounts the barcode printout generated by the iVotronic RTAL printer.
Supervisor PEB –	Pivot	N/A	Hardware v. N/A Firmware v. 1.7.1.0	A portable cartridge fitted with an infrared communications window and a flash memory chip. Supervisor PEBs contain specific ballot data for each election. They open the polls, load the ballot onto a voter terminal and enable the service mode for administrative functions.
Election SecurityKey PEB	ES&S	N/A	Hardware v. N/A Firmware v. 1.7.1.0	The iVotronic utilizes a "Key" PEB which requires that a key be passed to each iVotronic during set up in order to validate that the EQC (election qualification code) is correct for the election being conducted. This "Key" also requires that the correct election key be resident on each terminal before the election data is allowed to be unencrypted.
Voter Activated PEB – **3**	Pivot	N/A	Hardware v. N/A Firmware v. 1.7.1.0	The Voter Activated PEB allows the voter to activate a ballot on the terminal in complete privacy.
Communication Pack with Seiko printer	Pivot Seiko	N/A DPU 3445	Hardware v. 1.1	A case that contains special communications hardware, a serial thermal printer, and an optional modem for the iVotronic. The printer generates paper results, and the modem is used to transfer results to a central count location.
Printer	Seiko	DPU-	N/A	Standalone printer for the

Item	Manufacturer	Model #	Version/Rev	Description
(standalone for iVotronic)		3445		iVotronic.
BOD Printer	OkiData	9600		Printer used to print ballots.
Printer (M650 Red Left Printer) (2)	520 OkiData	GE5258 A	N/A	Printer for audit logs and reports for the M650.
Printer (M650 Green Right Printer) – 2	520 OkiData	GE5258 A	N/A	Printer for audit logs and reports for the M650.
Printer (M650 Green Left Printer) – 2	Epson Model # LQ-590	P363A	N/A	Printer for audit logs and reports for the M650.
LaserJet Printer	HP	2300N	N/A	Printer for reports created within Unity.
Router	Dlink	1 @ DSH-16, 1 with no identification	1 @ V. B2, 1 with no identification	Directs and controls the flow of data.
Modem	US Robotics	56K Sportster	N/A	A device that allows computer information to be sent over a telephone line.
Multi-Modem Adapters (Used in DAM PC) **(1 each)**	Equinox	N/A	N/A	4 and 8 port
Multi-Modem Adapters (Used in DAM PC)	Digi	N/A	N/A	4 and 8 Port
Multi-Modem Adapters (Used in DAM PC)	Perle	N/A	N/A	4 and 8 Port
Multi-Port Adapter (Used in DAM PC)	SeaLevel	N/A	N/A	7801 & 7803 – 8 Port 7406 – 4 Port
USB PEB Reader/Writer	Pivot	M1706	Hardware v. 1.1	A device with a USB connection used to upload election results from a PEB to a PC.
Hand Bar Code Reader	Voyager	MS9544	N/A	A device that reads the barcode printout generated by the iVotronic RTAL printer.
Omni Drive	Omni	D707-94	Rev. C1 USB 1.1	A device used to read/write data to the PCMCIA card.
Omni Drive Professional USB2	Omni	D707-94	Rev. A USB 2.0	A device used to read/write data to the PCMCIA card.
SanDisk Reader	SanDisk	SDDR-91	N/A	Used to read data off of a SanDisk.
SanDisk	SanDisk	SDDR-92	N/A	Used to read data off of a

Item	Manufacturer	Model #	Version/Rev	Description
ImageMate CF Reader				SanDisk.
Zip Disk **1 Received**	iOmega	Z250US BPCMBP	N/A	Used to store data.
Headphones	ADID -(ESS) N/A -(ES&S VAT)	N/A	N/A (ESS) AKG-K-44 (ES&S VAT)	A pair of listening devices joined by a band across the top of the head and worn in or over the ears.
External Volume Control Button	ES&S	N/A	Hardware v. N/A	Used for controlling the volume on the 12 inch 3-Key and 15 inch 3-Key iVotronics.
Serial PEB Reader	Pivot	N/A	Hardware Rev. 1.1 Software: N/A	A device with a serial connection used to upload election results from a PEB to a PC. The reader can also connect to a M100 to combine results at the polling place.
UPS	Belkin	N/A	N/A	Backup uninterrupted power source for the M650
Sip n Puff	Pivot	N/A		Device used on the iVotronic 6-key by physically disabled voters
iVotronic booth	Pivot	N/A	N/A	A booth that holds an iVotronic terminal and optionally an RTAL printer, to ensure voter privacy.
Dell Laptop D600 Latitude	Dell	N/A	Windows XP Professional, SP2 Rev A00	Intel® Pentium® M processor 1.60GHz 1.60 GHz, 1.00 GB of RAM (Laptop for Remote modeming only) Post Voting (DAM Client Regional Site remote only)
Dell PC Pentium®	Dell	N/A	Windows XP Professional, SP2	4 CPU 2.00GHz, 512MB of RAM (PC System 1) (Pre and Post Voting)
Dell PC Pentium®	Dell	N/A	Windows XP, SP2	4 CPU 2.80GHz, 2.79 GHz, 1.00 GB of RAM (PC System 2) Pre and Post Voting
Dell PC Pentium®	Dell	N/A	Windows XP Professional, SP2	4 CPU 2.80GHz, 2.79 GHz, 5.12 MB of RAM (PC System 3) (Post Voting DAM Host only)
Server (PC) PE600SC	Dell	N/A		Intel Pentium 4 CPU 1.80 GHz AT/AT compatible 523,763 KB RAM
Dell Laptop D610 Latitude	Dell	N/A	Windows XP Professional, SP2 Rev A06	Intel® Pentium® M processor 1.73GHz 795MHz, 0.99GB of RAM, (Physical Address Extension - laptop) (Hand Bar Code Reader and ABCR)
Multi Compact Flash Reader/Writer (Gang	Dell	N/A	Windows XP Professional, SP2	Pentium 4 CPU 2.80GHz, 2.79 GHz, 512 MB of RAM (Pre & Post voting)

Item	Manufacturer	Model #	Version/Rev	Description
Programmer PC)			Rev A00	
VAT	ES&S	Model # A100	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.
VAT	ES&S	Model # A200	Hardware v 1.0, and 1.1 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.

3.3 Test Materials

Items identified in the table reflect all test materials required to perform hardware, software, telecommunications, 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, various forms of flash memory such as USB or 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
Printer paper rolls	ES&S	RTAL: Future Logic & Nashua, M100 & DS200: NCR Communication Pack & Seiko Printer: Nakagawa	RTAL, Communication Pack, M100, DS200 and Seiko Printer
Zip disks	ES&S	Iomega	M650 program media
SanDisk (CF)	ES&S	SanDisk & Kingston	Compact Flash card 128, 256 & 512MB
Blank paper ballot stock	ES&S	Weyerhaeuser	Inches/ballot positions: 11x36, 14x36, 14x48, 17x45, 17x60, 19x51, 19x68
PCMCIA	ES&S	Vikant	M100 program media
USB Memory Stick	ES&S	Delkin & SanDisk	DS200
Head sets	ES&S	ADID (ES&S) N/A (ES&S VAT)	For the VAT and iVotronic

3.4 Deliverable Materials

Deliverable Materials consist of all of the documents submitted as part of the TDP supplied by the vendor.

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 Unity 4.0 voting system:

- Hardware Specifications
- Software Specifications
- Voter, operator, and hardware/software maintenance manuals
- Program listings, facsimile ballots, tapes
- Sample output report formats

Please see Attachment A for a complete list of TDP 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 system level 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 Unity 4.0 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 ES&S'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 Environmental Test Case Design

Hardware environmental certification testing is performed to verify conformance to Vol. 1. Section 3 of the FEC VSS April 2002. Certification testing is accomplished through a combination of testing performed by SysTest Labs and previous testing performed by subcontractor labs. Specific test plans and test reports from the subcontractor labs are included in Attachment D: Hardware Test Plans and Attachment G: Hardware Testing Results from Hardware Test Laboratories.

The hardware testing will be performed at four subcontract laboratories:

- Emissions Testing will be performed at Criterion Laboratories in Rollinsville, Colorado (intElect DS200)
- Environmental Testing will be done at Advanced Product Testing (APT) Laboratories in Longmont, Colorado (ABCR and intElect DS200)
- Emissions Testing will be performed at National Center for Excellence in Electronics (NCEE) in Lincoln, Nebraska. (ABCR and intElect DS200)
- Safety Testing will be performed at Compliance Integrity Services (CIS) Laboratories in Longmont, Colorado. (ABCR and intElect DS200)

4.3.2 Acceptance of Previous Hardware Test Results

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 G.

4.3.3 Software Module Test Case Design and Data

SysTest Labs reviewed 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 post-build configuration, including related hash codes.

4.3.4 Software Functional Test Case Design

SysTest Labs has reviewed the ES&S 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.

Software Functional Testing will demonstrate that the ES&S Unity 4.0 voting system overall capabilities meet the requirements for pre-voting, voting and post-voting functional areas (*Vol. 2, Appendix A.*). These include the functions 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, and one more precinct/polling place can be defined.
Ballots Before, During & After Processing	
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 Unity 4.0 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 (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, c 1-7 and d. 1-8
b.4. Report Generation – Produce test output data	Verify in Functional Tests: Clearing Election Totals Manual data entry Generating a Zero Report Testing an Election Creating Test Reports Clearing Totals for Election Day Selecting Reporting Groups Loading Scanner Totals Producing Election Reports

Function	Test Methodology
	Displaying Election Information ERM Election Results
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: Zero Reports Scan 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 commands as identified in user documentation
c.4. Generating real-time audit messages	Verify in Functional Tests: Print audit log Each audit message contains a timestamp. Election name, software, and firmware are listed at the beginning of each audit log. Count of ballots processed is included in log of uploaded results. Error messages. Precinct ID is identified for all results pertaining to insertions, additions, and deletions.
c.5: Closing polls and disabling ballot acceptance	Verify in Functional Tests: Inability to cast additional ballots Close of polls Inability to scan additional ballots
c.6. Generating election data reports.	Verify in Functional Tests: Generation of precinct reports
c.7. Transfer ballot count to central counting location	Verify in Functional Tests: Reading media into ERM (DS200 – USB, M100 – PCMCIA, iVotronic – PEB) Telecommunication
c.8. Electronic transmission of election data to central count locations	Verify in Functional Tests: Confirming transmission, receipt, and validity of data interactively and with reports
Central Count Functions	
*d.1.*Process ballot deck for > 2 precincts with 3 split precincts per precinct for a total of 6 ballot styles	Verify in Functional Tests: Process of ballot decks
d.2. Monitoring equipment status	Verify in Functional Tests: Equipment status as identified in user documentation
d.3. Equipment response to commands	Verify in Functional Tests: Equipment responds to all voter and poll worker commands as identified in user documentation (Messages generated by the equipment that require an action by the voter or poll worker before operation continues--as in blank ballots, overvotes, undervotes as defined in election setup)
.4. Integration with peripherals equipment or	See b.3

Function	Test Methodology
other data processing systems	
d.5. Generating real-time audit messages.	See b.4
d.6. Generating precinct-level election data reports	See b.3
d.7. Generating summary election data reports	See b.3
d.8. Transfer of detachable memory module to the processing equipment	See b.3
d.9. Electronic transmission of data to other processing equipment	Verify in Functional Tests: Confirming transmission, receipt, and validity of data interactively and with reports
d.10. Producing output data for interrogation by external display devices	Verify in Functional Tests: Confirming transmission, receipt, and validity of data interactively and with reports where possible

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). Unity 4.0 components subject to the Accuracy Test include:

- intElect DS200 scanners – hardware vers. 1.2.0 & 1.2.1, firmware vers. 1.3.7.0
- Model 100 scanners - hardware vers. 1.3.0, firmware vers. 5.4.0.0
- Model 650 scanners - hardware vers. 1.1 and 1.2, firmware vers. 2.2.1.0
- iVotronic DRE - hardware vers. 1.1, firmware vers. 9.2.3.0
- RTAL equipped voting booth – RTAL firmware vers. V012
- ABCR scanner – hardware vers. B, firmware vers. 29
- Voyager Hand Held Scanner
- Communication pack with Seiko printer - hardware vers. 1.1, firmware vers. N/A
- AutoMARK VAT Models A100 and A200 - hardware vers. 1.0 and 1.1, firmware vers.1.3.2904

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

- Election/ballot definition is created in EDM, and additionally imported into AIMS.
- Ballot definition data and scanner media is created and loaded onto the device being tested.
- Report of the initialization process
- Display the function selections
- Open polls

- Zero Report
- Execute votes (if a touchscreen or VAT device is being tested), Scan ballots (if an optical scanner or VAT is being tested), Close polls, Run Totals report and Audit Log
- Transfer data to ERM for reporting
- 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.

SysTest Labs will implement and configure the COTS operating system and security policy as described in the vendor's documentation. This configuration will then be reviewed against the best business practices security policy as defined by National Vulnerability Database website. We will use the security policy recommendations of National Checklist Program Repository (http://nvd.nist.gov/ncp.cfm?repository) for the implemented Operating System as guidance for the configured security policy. Specifically, we will use the baseline security policy for Windows operating systems as defined:

Windows XP Professional - Windows XP Security Guide (Checklist-ID 79)
Windows Server 2003 - Windows Server 2003 Security Checklist (Checklist-ID 221)
Windows Server 2000 - Prose Guide - Windows 2000 Security Checklist (Checklist-ID 67)

Vol 2, 6.4.1:
SysTest Labs has designed and will conduct security testing to validate the requirements defined in Volume I, Section 6 as they pertain to the component under test. These tests will include the verification of the access control mechanisms and the security features described in the vendor's documentation, as shown in the table below.

The security tests will verify and validate all of the security requirements and attempt to circumvent the security controls to gain unauthorized access to the component under test. SysTest Labs will test the known vulnerabilities which have been identified through State security studies with respect to the vendor's component and the unit's architecture; see Test Steps for requirements Volume 1: 6.2.1.1.e and for components using a communications network,

Volume 1: 6.5.4 for details. These tests will include testing of the physical protections such as locks and security seals, integrity, man-in-themiddle and replay attack scenarios.

Vol 2, A 4.3.5
Security: SysTest labs has designed security testing procedures to ensure the integrity and security of the voting system by validating the security capabilities with respect to modification or disruption during pre-voting, voting and post voting processing by unauthorized access to critical components and data, including the audit trails, and security mechanisms. Each component of the Voting System will be tested as stand-alone and as an integrated component of the system, validating the required security posture of the voting system. Specific tests have been designed to ensure the overall integrity of the voting system.

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

Table 8 - ES&S Unity 4.0 Security Functional Testing

ES&S Unity 4.0 Security Functional Testing														
VSS 2002 Volume I Section 6 Security Functional Requirements	**Unity Software (Windows XP)**								**Unity Election Hardware/Firmware**					
Software and Hardware System Components	**AM**	**EDM**	**ESSIM**	**iVIM**	**HPM**	**DAM**	**ERM**	**AutoMark AIMS**	**DS200**	**M100**	**M650**	**iVotronic**	**ABCR**	**AutoMark VAT**
6.2 Access Control														
6.2.1 Access Control Policy														
6.2.1.1 General Access Control Policy														
6.2.1.1.a Software access controls	X	X	X	X	X	X	X	X	X	X	X	X	X	X
6.2.1.1.b Hardware access controls	X	X	X	X	X	X	X	N/A	X	X	X	X	N/A	X
6.2.1.1.c Communications	X	X	X	X	X	X	X	N/A	X	X	X	X	N/A	N/A
6.2.1.1.d Effective password management	X	X	X	X	X	X	X	X	X	X	N/A	X	N/A	X
6.2.1.1.e Protection ablilities of a particular operating system	X	X	X	X	X	X	X	X	X	X	X	X	X	X
6.2.1.1.f General characteristics of supervisory access privileges	X	X	X	X	X	X	X	X	X	X	X	X	X	X
6.2.1.1.g Segregation of duties	X	X	X	X	X	X	X	X	X	X	X	X	X	N/A
6.2.1.1.h Additional relevant characteristics	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
6.2.1.2 Individual Access Control Policy														
6.2.1.2.a Authentication	X	X	X	X	X	X	X	X	X	X	X	N/A	X	X
6.2.1.2.b Authorization	X	X	X	X	X	X	X	X	X	X	X	X	X	X
6.2.1.2.c Access Restriction	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	X	X	N/A	X	N/A	X
6.2.2 Access Control Measures														
6.2.2.a Use of data and user authorization	X	X	X	X	X	X	X	X	X	X	X	X	X	X
6.2.2.b Program unit ownership and other regional boundries	X	X	X	X	X	X	X	X	N/A	N/A	N/A	N/A	X	X
6.2.2.c Protection Devices	X	X	X	X	X	X	X	N/A	X	X				N/A
6.2.2.f Special protocols	X	X	X	X	X	X	X	N/A	X	N/A	X	X	N/A	N/A
6.2.2.g Message encryption	X	X	X	X	X	X	X	X	X	X	X	X	X	N/A
6.2.2.h Controlled Access Security	X	X	X	X	X	X	X	N/A	X	N/A	X	X	X	N/A

ES&S Unity 4.0 Security Functional Testing														
VSS 2002 Volume I Section 6 Security Functional Requirements	**Unity Software (Windows XP)**								**Unity Election Hardware/Firmware**					
Software and Hardware System Components	**AM**	**EDM**	**ESSIM**	**iVIM**	**HPM**	**DAM**	**ERM**	**AutoMark AIMS**	**DS200**	**M100**	**M650**	**iVotronic**	**ABCR**	**AutoMark VAT**
6.3 Physical Security Measures														
6.3.1 Polling Place Security														
6.3.1.a Detection of Tampering	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	X	X	X	X	X	X
6.3.2 Central Count Location Security														
6.3.2 Central Count Location Security	X	X	X	X	X	X	X	N/A	X	X	X	X	X	N/A
6.3.2.c Counting operations	X	X	X	X	X	X	X	N/A	X	X	X	X	X	N/A
6.3.2.d Reporting data	X	X	X	X	X	X	X	N/A	X	X	X	N/A	X	N/A
6.4 Software Security														
6.4.1 Software and Firmware Installation														
6.4.1.a Validation of ROM devices	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	X	X	X	N/A
6.4.1.c Protection from unathorized access or activation	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	X	X	X	X	X	X
6.4.1.d Separaton of OS from election data	X	X	X	X	X	X	X	N/A	N/A	N/A	X	X	X	N/A
6.4.2 Protection Against Malicious Software														
6.4.2 Protection Against Malicious Software	X	X	X	X	X	X	X	X	N/A	N/A	X	X	X	N/A
6.5 Telecommunications and Data Transmission														
6.5.1 Access Control														
6.5.1 Security requirements for telecommunications	N/A	N/A	N/A	N/A	N/A	X	X	N/A	X	X	X	X	N/A	N/A
6.5.2 Data Integrity														
6.5.2 Data integrity and detection of transmission errors	N/A	N/A	N/A	N/A	N/A	X	X	N/A	X	X	X	X	N/A	N/A
6.5.3 Data Interception Prevention														
6.5.3.a US Federal approved encryption standards compliance	X	X	X	X	X	X	X	N/A	X	X	X	X	N/A	N/A
6.5.3.b Detection of intrusion	X	X	X	X	X	X	X	N/A	X	X	X	X	N/A	N/A
6.5.4 Protection Against External Threats														
6.5.4 Protection of commercial	X	X	X	X	X	X	X	N/A	X	X	X	X	N/A	N/A

ES&S Unity 4.0 Security Functional Testing														
VSS 2002 Volume I Section 6 Security Functional Requirements	**Unity Software (Windows XP)**								**Unity Election Hardware/Firmware**					
Software and Hardware System Components	**AM**	**EDM**	**ESSIM**	**iVIM**	**HPM**	**DAM**	**ERM**	**AutoMark AIMS**	**DS200**	**M100**	**M650**	**iVotronic**	**ABCR**	**AutoMark VAT**
products against external threats														
6.5.4.1 Identification of COTS Products														
6.5.4.1 Identification of COTS Products	X	X	X	X	X	X	X	N/A	X	X	X	X	N/A	N/A
6.5.4.1.a Operating Systems	X	X	X	X	X	X	X	N/A	X	X	X	X	N/A	N/A
6.5.4.1.b Communications Routers	X	X	X	X	X	X	X	N/A	N/A	N/A	X	N/A	N/A	N/A
6.5.4.1.c Modem drivers	X	X	X	X	X	X	X	N/A	N/A	N/A	X	X	N/A	N/A
6.5.4.1.d Dial-up networking software	X	X	X	X	X	X	X	N/A	N/A	N/A	N/A	X	N/A	N/A
6.5.4.2 Use of Protective Software														
6.5.4.2.a Detect the presence of a threat in a transmission	X	X	X	X	X	X	X	N/A	X	X	X	X	N/A	N/A
6.5.4.2.b Removal of threats from infected files/data	X	X	X	X	X	X	X	N/A	X	X	X	X	N/A	N/A
6.5.4.2.c Prevent against storage of the threat anywhere on the receiving device.	X	X	X	X	X	X	X	N/A	X	X	X	X	N/A	N/A
6.5.4.2.d Scan for threats in system memory and connected storage media	X	X	X	X	X	X	X	N/A	X	X	X	X	N/A	N/A
6.5.4.2.e Audit log of threat and ensuing processing performed	X	X	X	X	X	X	X	N/A	X	X	X	X	N/A	N/A
6.5.4.3 Monitoring and Responding to External Threats														
6.5.4.3.c Monitoring threat alerts from CERT, NIPC, FedCIRC	X	X	X	X	X	X	X	N/A	N/A	N/A	X	X	X	N/A
6.5.4.3.f.2 Procedures to disable public telecommunications mode of system	X	X	X	X	X	X	X	N/A	N/A	N/A	X	X	N/A	N/A
6.5.4.3.f.3 Procedures to update and patch election systems to address threats	X	X	X	X	X	X	X	N/A	N/A	N/A	X	X	N/A	N/A
6.5.5 Shared Operating Environment														
6.5.5 Shared Operating	X	X	X	X	X	X	X	N/A	N/A	N/A	N/A	N/A	N/A	N/A

ES&S Unity 4.0 Security Functional Testing														
VSS 2002 Volume I Section 6 Security Functional Requirements	**Unity Software (Windows XP)**								**Unity Election Hardware/Firmware**					
Software and Hardware System Components	**AM**	**EDM**	**ESSIM**	**iVIM**	**HPM**	**DAM**	**ERM**	**AutoMark AIMS**	**DS200**	**M100**	**M650**	**iVotronic**	**ABCR**	**AutoMark VAT**
Environment														
6.5.5.a Control access to system functions	X	X	X	X	X	X	X	N/A	N/A	N/A	N/A	N/A	N/A	N/A
6.5.5.b Compartmentalization of voting system functions	X	X	X	X	X	X	X	N/A	N/A	N/A	N/A	N/A	N/A	N/A
6.5.5.c Control system access, restriction of access to necessary functions only	X	X	X	X	X	X	X	N/A	N/A	N/A	N/A	N/A	N/A	N/A
6.5.5.d Preclude leakage of data through shared system resources	X	X	X	X	X	X	X	N/A	N/A	N/A	N/A	N/A	N/A	N/A
6.5.6 Access to Incomplete Election Returns and Interactive Queries														
6.5.6.a Ability to restrict external access to incomplete election returns	X	X	X	X	X	X	X	N/A	N/A	N/A	X	X	N/A	N/A
6.5.6.b.1 No write-access back to election system	X	X	X	X	X	X	X	N/A	N/A	N/A	X	X	N/A	N/A
6.5.6.b.2 Denial of write-access to persons authorized for read-access only	X	X	X	X	X	X	X	N/A	N/A	N/A	X	X	N/A	N/A
6.6 Security for Transmission of Offical Data Over Public Communication Networks														
6.6.1 General Security Requirements for Systems Transmitting Data Over Public Networks														
6.6.1.a Privacy of voter's ballot choices	N/A	N/A	N/A	N/A	N/A	X	X	N/A	N/A	N/A	X	X	N/A	N/A
6.6.1.b Digital signatures for network communication with vote server	N/A	N/A	N/A	N/A	N/A	X	X	N/A	N/A	N/A	X	X	N/A	N/A
6.6.1.c Require two election officials to activate processing of transmitted ballots	N/A	N/A	N/A	N/A	N/A	X	X	N/A	N/A	N/A	X	X	N/A	N/A
6.6.2 Voting Process Security for Casting Individual Ballots over a Public Telecommunications Network														
6.6.2 Voting Process Security for Casting Individual Ballots over a Public Telecommunications Network	N/A	N/A	N/A	N/A	N/A	X	X	N/A	N/A	N/A	N/A	X	N/A	N/A

ES&S Unity 4.0 Security Functional Testing														
VSS 2002 Volume I Section 6 Security Functional Requirements	**Unity Software (Windows XP)**								**Unity Election Hardware/Firmware**					
Software and Hardware System Components	**AM**	**EDM**	**ESSIM**	**iVIM**	**HPM**	**DAM**	**ERM**	**AutoMark AIMS**	**DS200**	**M100**	**M650**	**iVotronic**	**ABCR**	**AutoMark VAT**
6.6.2.1 Documentation of Mandatory Security Activities														
6.6.2.1.a Security procedures for setup and testing of voting systems that cast individual ballots over a telecommunications network	N/A	N/A	N/A	N/A	N/A	X	X	N/A	N/A	N/A	N/A	X	N/A	N/A
6.6.2.2 Capabilities to Operate During Interruption of Telecommunication Capabilities														
6.6.2.2 Provide resistance to interruptions of telecommunications service	N/A	N/A	N/A	N/A	N/A	X	N/A	N/A	N/A	N/A	N/A	X	N/A	N/A
6.6.2.2.a Detection of interruption and switching to alternative mode	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	X	N/A	N/A
6.6.2.2.b Alternative mode supports functionality of conventional DRE	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	X	N/A	N/A
6.6.2.2.c Audit trail of votes cast during interruption	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	X	N/A	N/A
6.6.2.2.d Upon reconnect, transmit and process votes stored in conventional DRE mode	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	X	N/A	N/A
6.6.2.2.e Ensure voter identification and authentication throught procedures employed by the system to counteract potential interruptions of telecommunications	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	X	N/A	N/A

4.3.7 System Level Test Case Design

System level tests shall be performed on the ES&S Unity 4.0 voting system for the purpose of assessing the response of the software to a range of conditions. Paper ballots will be used in several of these test cases.

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

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 9 - 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.	Volume and Stress 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.	Telecommunications Test case for each component
Performance Tests	
Tests accuracy, processing rate, ballot format, handling capability and other performance attributes claimed by vendor	All System 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:

- AM - 3.0 View Log
- DS200 - 3.2 Opening Polls Functions: Open Polls with more than one Precinct
- ERM - Expanded Precincts (M100)
- ERM - Expanded Precincts (DS200)
- Maximum Candidates
- L&A Vote Selected Ballot Test
- L&A Multi-Vote Test
- L&A Vote for One Test
- M100 with Plastic Ballot Box

    (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 - Unity 4.0 Test Case Matrix, for an outline of functionality being tested in each test case.

Table 10 - Matrix of Additional Testing

Test Case No.	Test Case	Execution
N/A	Hi Capacity Ballot Test, 11X36 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). Scan the ballot on the scanners (M100, DS200, M650), utilizing random orientations to test all orientations. (V1: 2.3.4.2.a)
N/A	Hi Capacity Ballot Test, 14X36 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). Scan the ballot on the scanners (M100, DS200, M650), utilizing random orientations to test all orientations. (V1: 2.3.4.2.a)
N/A	Hi Capacity Ballot Test, 14X48 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). Scan the ballot on the scanners (M100, DS200, M650), utilizing random orientations to test all orientations. (V1: 2.3.4.2.a)
N/A	Hi Capacity Ballot Test, 17X41 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 17x41 ballot (6 contest w/ 40 candidates). Scan the ballot on the scanners (M100, DS200, M650). Utilized random orientations to test all orientations.
N/A	Hi Capacity Ballot Test, 17X45 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). Scan the ballot on the scanners (M100, DS200, M650), utilizing random orientations to test all orientations. (V1: 2.3.4.2.a)
N/A	Hi Capacity Ballot Test, 17X60 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). Scan the ballot on the scanners (M100, DS200, M650), utilizing random orientations to test all orientations. (V1: 2.3.4.2.a)
N/A	Hi Capacity Ballot Test, 19X51 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). Scan the ballot on the scanners (M100, DS200, M650), utilizing random orientations to test all orientations. (V1: 2.3.4.2.a)
N/A	Hi Capacity Ballot Test, 19X68 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). Scan the ballot on the scanners (M100, DS200, M650), utilizing random orientations to test all orientations. (V1: 2.3.4.2.a)
N/A	Expanded Precincts (M100)	Using M100 firmware, create PCMCIA card for early voting containing 494 precincts on one card. Verify the card can be created and read into ERM.
N/A	Expanded Precincts (DS200)	Using DS200 firmware, create DS200 USB drive for early voting containing 494 precincts on one USB drive. Verify the card can be created and read into ERM.
N/A	Auto Recovery	Using the iVotronic Auto Recovery procedure v 9.2.0.0, vote an election and recover the results from the U2-D chip. (U2-D chip is a SanDisk). Manual provided and steps were completed, as only a trained ES&S technician completes this procedure.
B6225	Maximum Candidates	In ERM load election database "02PNELAN" with more than 1000 candidates in a precinct. ERM limits 1000 counters in a single precinct. Verify that an attempt to load over 1000 counters gives an error messages stating "Aborted-over 1000 candidate in precinct: 211 ERM create results database failed. Connect election definition HPM and then retry."
N/A	L&A Vote Selected Ballot Test	Using ES&S test case, for the iVotronic, "L&A Vote Selected Ballot Test" to verify the logic and accuracy vote selected ballot test. The voter selects a particular ballot to vote and that vote logic is applied to a select number of

Test Case No.	Test Case	Execution
		ballots designated for the voter to cast.
N/A	L&A Multi-Vote Test	Using ES&S test case, for the iVotronic, "L&A Vote Multi-Vote Test" to verify the logic and accuracy of the multi vote test. Votes for each candidate will increase from one to the next, as in 1, 2, 3, 4, 5, etc.
N/A	L&A Vote for One Test	Using ES&S test case, for the iVotronic, "L&A Vote For One Test" to verify the logic and accuracy of the vote for one test. Each candidate within a contest will receive one vote. There will be an additional undervote assigned in each contest.
AM 3.0	View Log	Using an existing election (GEN01), select a user and verify Audit Manager has captured all activity(ies) carried out in all applicable applications (EDM, AM, and ESSIM).
DS200 3.2	Opening the Polls Functions	Use this test case to determine if the DS200 can open polls with an election definition that has more than one precinct. The HPM Report Level option must be 'Precinct'.
N/A	M100 with Plastic Ballot Box	Using ES&S test case "Model 100 with Plastic Ballot Box" to verify that the M100 can process ballots accurately when seated in the plastic ballot box. **Note: Testing was completed with the Plastic Ballot Box; however, the box has not been subject to environmental testing.**

4.3.10 Volume, Performance, Stress and Error Recovery Test Approach

As part of the certification of the Unity 4.0 System, an analysis of the system to include Unity 4.0 windows based applications and devices was completed. Based upon this analysis, the following sections outline the approach that will be used in the validation of system behavior as maximum thresholds are achieved and exceeded. It was also determined from a system perspective, the system level test for volume is only applicable to the ERM application as all vote data will flow to the ERM application for final results reporting. All other devices or applications are subject to specific types of volume, stress, and performance tests. Error Recovery and Error Messaging is synonymous with Stress level tests with the focus being "How does the system react / recover when a defined or identified limit is met or exceeded.

The following list identifies the areas of focus for each device or application of the system.

- Volume
  - EDM, HPM, ERM, AM, iVotronic, M100, DS200, M650, ABCR
    - File size limits
    - Storage Limits
  - ESSIM, iVIM, DAM
    - File size limits
- Performance
  - ERM
  - iVotronic, M100, DS200, M650
    - Ballot complexity
- Stress and Error Recovery
  - EDM, HPM, ERM, M100, DS200, M650, DAM

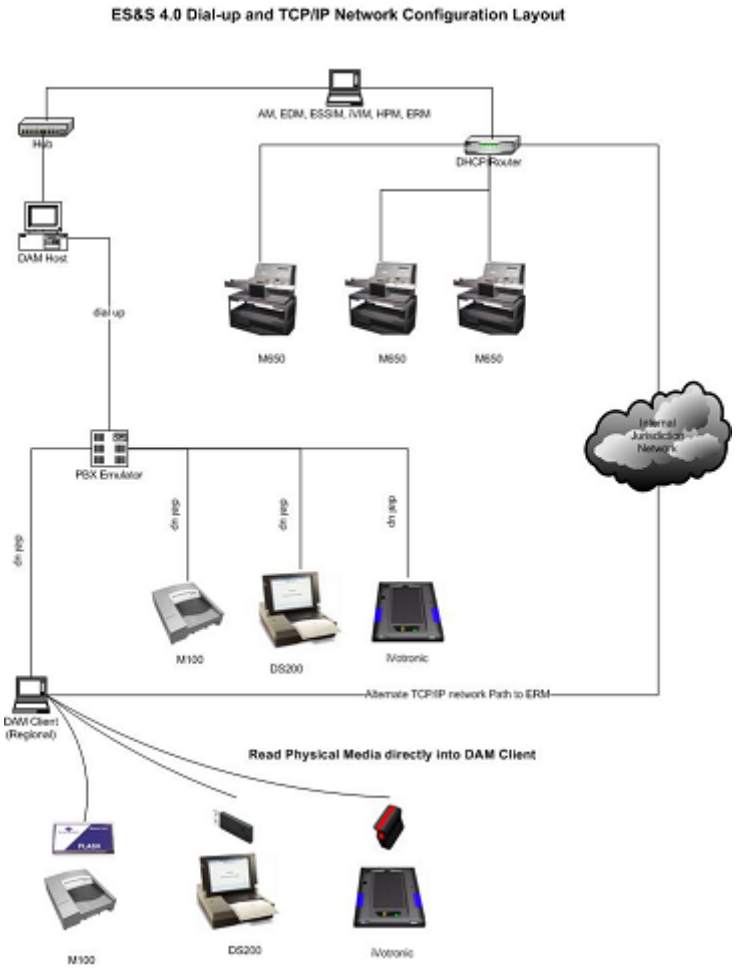
4.3.10.1 System Configuration

The Unity 4.0 Voting system can support multiple configurations and deployments that a jurisdiction may use. The Unity 4.0 windows based applications can support a distributed deployment or a partial distributed deployment. Based upon our analysis, it was determined that a partial distributed deployment configuration would provide the necessary loading factors than what would be achieved in a distributed system. This would ensure additional loading of CPU, Memory, I/O, and Storage Media.

The application configuration will be deployed and configured in the following manner using 2 laptops and 1 Desktop.

- Laptop 1 will have the following applications installed and was selected to increase the loading factor from a CPU, Memory, I/O, and storage media perspective.
    - AM
    - EDM
    - ESSIM
    - iVIM
    - HPM
    - ERM
- Laptop 2 will have the following application installed and was selected to cover all possible transmission paths of vote data to the main reporting system.
    - DAM (Client)
- Desktop 1 will have the following application installed and was selected to replicate the network connectivity between the DAM Host and the personal computer running the ERM application.
    - DAM (Host)

The network layout configuration was selected to support the multiple paths that vote data can be transferred to the main reporting application.



4.3.10.2 Voting Variations

The following voting variations will be used to achieve meeting or exceeding the limitations of the system or device. The ballot to be used for this testing is based upon the largest ballot the vendor can support across all paper based scanning devices which is currently a (8 ½ X 19" (4 ovals per inch) (68 X 3 columns = 204/side, 408 total) and meets the limitation definition that all ballots within an election must be the same size and have the same position capacity. Using this ballot size provides the required density of possible vote positions and ballot layouts. The voting pattern that will be used for this testing will be based upon a set of 2 ballots marked double sided with alternating marks. Ballot 1 will be marked all evens, ballot 2 will be marked all odds. Additional ballots will be created that span greater than a single ballot to achieve meeting and exceeding the maximum candidate / counters allowed per precinct. The same applicable ballot definitions, layouts and approach will be used for the DRE devices. The mock elections that will be used for this test will be based upon a general election without straight party supporting cross party votes, which are unconditionally tabulated and an open primary election. The use of mock elections will allow for the proper population of the reporting database and provide support for meeting or exceeding the system limitations. The EDM System will be populated with data (offices, candidates, referendums, etc…) to support Federal, State, County, City, and judicial elections.

The attached spreadsheet provides a matrix of limitations gathered based upon the vendor provided System Limitations document. Specific functional test cases will be created as required verify device and system level limitations. Any additional limitations identified during certification will be added to the spreadsheet and submitted as part of the certification report.

4.3.10.3 System / Device Level Tests

As part of this analysis, there was particular focus applied to the types of information being saved to media that is used to transfer election information and vote total information between the Windows based applications and the physical voting devices and information that is exchanged between the applications.

There are field limitations that exist throughout the applications that have been reviewed and the following criteria will be used to determine the specific test cases that will be created.

- If exceeding a limit of a field or file causes the application to follow a different path in file creation or data creation
- When a field length in one function is defined as 7 bytes and a similar field length in the same application but a different function is defined as 6 bytes
- When a field length in one application is defined as 7 bytes and a similar field length in a different application is defined as 6 bytes
- When field limits are fixed in a given file and populated through the user interface
- When information goes through a conversion process
- When information is imported or exported
- File name limits

There are many performance definitions provided in the SDS documentation that is impacted based upon the size of the election. As part of this verification, a simplified election definition will be created as a baseline for validating performance variations based upon election size definitions.

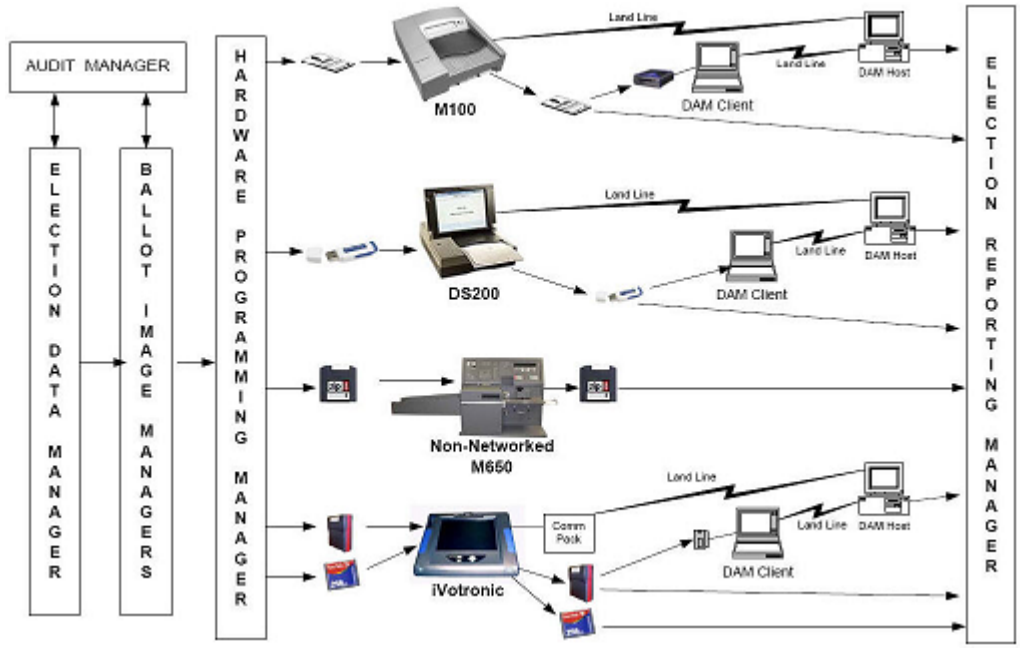
Error Recovery and Error Messaging is synonymous with any test case that produces an error message. As an example, Stress Level tests have a focus of exceeding the capabilities of any given device or system with the focus being "How does the system react / recover" when a defined or identified limit is met or exceeded.

Where system limitations are defined as a combination of two variables (example: Variable A and Variable b), the following validation sequence will occur.

- Variable A = Max; Variable B = 0
- Variable A = 0; Variable B = Max
- Variable A = Max + 1; Variable B = 1
- Variable A = 1; Variable B = Max + 1
- Both Variables at Max + 1

With the exception of the iVO and the M650, different media sizes are available for the M100 and the DS200. Based upon this information, the verification tests will use the smallest available media size. In an effort to reduce the time required to build the file sizes to exceed storage media capabilities and verify / validate error recovery, there will be an attempt to save large graphic images on any media that supports "windows based" recognizable file systems. Some media does not use any "windows based" recognizable file system support, therefore this type of time reduction will not be applicable. As part of security measurements built into the system by the Vendor, it may not be possible to add other files to this media as it will fail system level or device level integrity verification tests. The use of automated ballot reading modes (L&A for the DRE and Shoeshine mode for the M100 and DS200) will be used to push the file size limits to exceed the storage capacity of the media and ERM application. We will also use the "ERM Only Candidate File Maintenance" feature in HPM that allows the capability of adding ERM Only candidates to contests that are not included in the tabulator data definition but are associated with any designated contests that it is coded for. This allows the ERM database to have a counter assigned but have the position skipped over on tabulator data upload. Data in this field can be manually entered into ERM and will appear on all contest reports containing this "candidate". This feature will be used for achieving maximum limits on the ERM as required.

The following diagram was used as a reference point as it depicts the paths that information from application to voting devices can flow. Another diagram that was referenced as part of this analysis can be located in section 9.2 of the HPM SDS Document, which depicts the particular files that are transferred between applications and devices.



The following information depicts the types of test cases / verification steps that will be executed based upon this analysis.

The AM application implements a database with a known limitation of 2GB. It is also known that when this limit is reached or exceeded, database corruption may occur. As part of this verification, an attempt will be made to reach and exceed this limit to determine how the system will react. As part of this verification, the performance of the application as well as CPU and Memory usage will be tracked and documented.

The EDM application has two methods for creating election information. One is through import routines and the other is through manual entry using the user interface. As part of this verification, files will be created to achieve the maximum defined limits as well as files that exceed the defined limits. These files will then be imported into the application to validate database creation, storage, performance and where applicable error recovery. Additional test steps will be added to verify user interface input when the application has reached its limits. Additional test cases and or test steps will be added to validate field limitations at the file level as required.

The ESSIM and iVIM image managers will be validated for proper layout, positioning, and formatting of candidate information as field length limitations meet or exceed the defined limit.

The HPM application creates the final database files for all the devices to include the ERM application and burns all the media for all devices. Field size limits, media size limits, imports, and conversions of information will be validated as part of the verification process with a focus on error recovery and performance of burning media based upon the size of the election. The HPM application also creates the DAM Precinct list. In certain instances, exceeding the maximum limit of a file causes the system to re-distribute the file across multiple media for the same device. This will also be verified.

The ERM application is the reporting database for the Unity System. To support the import of election information from non-ES&S devices, the application allows for the manual entry of information. The results maybe entered or modified. The application also has the capabilities to export results to a variety of file types. Field size limits, file size limits, import of invalid vote information, and export functions will be validated as part of the verification process with a focus on performance and error recovery as limits are reached and exceeded.

The HPM and ERM applications share the same interpreter but do not share the same database.

For the M100, election definition, audit logs, and vote data is saved on the same media. There are 4 different sizes of media that can be supported which are 256K, 512K, 4MB, or 6MB. As part of this validation, only 256K and 512K will be used in an effort to validate error recovery when storage media capability is exceeded. Different levels of ballot complexity will be used to validate the performance of the scanner. Additional test cases will be created and executed to validate System and Device level limitations.

For the DS200, election definition, audit logs, and vote data is saved on the same media. There are 4 different sizes of media that can be supported which are 1GB, 2GB, 4GB and 8GB. As part of this validation, only the 1GB will be used in an effort to validate error recovery when storage media capability is exceeded. Different levels of ballot complexity will be used to validate the performance of the scanner. Additional test cases will be created and executed to validate System and Device level limitations.

For the M650, it uses an internal solid-state drive for storage and allows election information and vote data to be transferred via a ZIP disk or Ethernet communication. It maintains election information and an audit log on the internal solid-state drive. Different levels of ballot complexity will be used to validate the performance of the scanner. Additional test cases will be created and executed to validate System and Device level limitations using both internal and zip disk media.

For the iVotronic, it uses a PEB and CF card to support election definitions, ballot images, audio files for ADA, and audit log information. Test cases will be created and executed to validate File size, System and Device level limitations using the different types of PEB media and CF Card Media.

4.3.10.4 Additional Items

4.3.10.4.1 Dial-Up

The typical deployment as provided by the Vendor is support for 16 ports, however, the use of 8 port modem cards is only limited by the number of cards any personal computer can accommodate. The DAM (Host) application has a limit of 24 concurrent dialup connection. Based upon this information, the dial-up test should consist of 3 x 8 port cards installed in the personal computer hosting the DAM application configured as the Host server. The use of a mix of M100's, DS200's, and iVotronic devices to comprise a total of 24 devices should be used as part of this test transmitting data simultaneously to the DAM configured host. While all 24 devices are transmitting, a single device of each type should also be tested for transmission of information to ensure that proper handling of a busy signal does occur within each device. Additional tests should comprise the transmission of corrupted data (if possible), verification that devices configured for early voting cannot transmit data, and that data can be transmitted manually. These types of tests can be executed as a single device tests but may use the same system configuration as is used for volume testing.

In order to achieve this test, it will require many devices to be housed in a single location with the proper POTS configuration or the use of a PBX emulator and the ability for all 24devices to transmit data simultaneously.

Additional item to note that were identified in the DAM SDS document shows support for up to 96 modems using a mix of discrete modems or multiple 23 channel T1/ESD lines.

For the M100, in order to support dial-up communications between the M100 and the DAM host, it is required that the 512K media be used. For devices that do not support dial-up communication, only 256K media is required. As part of an error recovery validation test, a M100 will be configured to support dial-up communications, but 256K media will be used when creating the media.

4.3.10.4.2 Networking

The typical deployment as provided by the Vendor based upon the largest jurisdiction is 6 M650's. Since a TCP/IP network can support 255 distinct IP addresses, if no limitations exist on the reporting system, it is feasible to test 255 distinct M650's transmitting data simultaneously to the reporting system. Analysis of the 650 shows a QNX node number, which has a range of 1 to 149. Based upon this range, it is expected that only a maximum of 149 central count scanners can be connected to the reporting system at any given time. For this type of test, without the use of simulator software to replicate 149 central count scanners, it will be very difficult to execute such a test due to the availability of that many M650's. One approach that will be used is to define the QNX node number to be 149 and validate the affect on the reporting system as well as defining a QNX node number to be 150.

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 Electronic and paper based Voting 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 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 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 of the ES&S Unity 4.0 voting system will be performed at SysTest Labs' facilities in Denver, Colorado. 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 Unity 4.0 voting system was executed at the NVLAP or A2LA accredited environmental hardware testing facilities shown in Attachment H: Accredited Hardware Test Lab Certifications.

6.2 Test Setup

The ES&S 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 - TDP Documents.** The software will be installed, versions verified, and made operational. The hardware will also be set up and versions verified according to the vendor 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 software certification testing and audits, there are prerequisite tasks for some testing. Tasks and any applicable predecessor tasks are identified in table 10.

Table 11 - 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
Trusted Build	Completion of PCA source code review

Certification Task	Prerequisite Task
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, PCA system configuration audit and environmental testing
FCA System Level Testing	Completion of FCA test case preparation, PCA system configuration audit and environmental testing
FCA Security Testing	Completion of FCA test case preparation, PCA system configuration audit and environmental testing
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 provides step-by-step procedures for each test case to be conducted. Each procedure is assigned a test step and this, along with critical test data and test procedures information, is 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 applicable standards as identified in section 1.3 are marked as **Documentation Discrepancies** or **Functional Discrepancies** (a discrepancy occurs when the voting system component or document does not meet defined 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 and all applicable applications 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.

SysTest Labs uses Vendor documentation to determine Voter facing error messages as defined in V2: A.4.3.5, V1: 2.2.5.2.2 (a - g). These functional tests force the generation and validation of documented Voter facing error message(s) pertaining to ballot input, invalid ballot type, ballot casting, over votes, under-votes, or any other error messages that the vendor has defined to be voter facing. Additional functional tests are created and executed to cover power failures while voting as it pertains to precinct devices where applicable. The contents of the error message (s) are verified to be applicable to the error condition being validated and to provide the voter with enough information to progress to the next step in the voting process.

SysTest Labs uses Vendor documentation, Vendor provided test cases, and System Analysis to determine the scope of testing for Jurisdiction Facing error messages as it pertains to VSS V2: A.4.3.5, VSS V1: 2.2.3 (a - c), VSS 2.2.5.2.2 (b – g), VSS: V1: 2.2.5.2.3. Based upon an Analysis of the system and vendor provided test cases, SysTest Labs will execute a sampling of vendor test cases for verification of the Vendors test coverage or create additional functional tests where specific areas of the system will be tested. Test case sampling is used in cases where replicating vendor testing for field input validation and application path analysis would not provide any additional confidence in the overall core functions of the application or system. Any error messages received during functional testing are verified for proper content and against vendor documentation to ensure next steps are clearly defined and documented. Upon restoration of the system or device from an error condition, the system is validated to be restored to the condition prior to the error occurring. Audit logs are reviewed to verify proper capturing and reporting of error messages and proper recovery of the system or device. Areas where additional focus will be applied pertain to the creation of election definition information in the key areas of candidate mapping to ballot positions that the tabulator uses for tabulation purposes and the transition of vote data throughout the system.

7 Appendix A – Test Cases

SysTest Labs executed all System and Functional Level tests on each of the system configurations identified in VSS Volumes 1 and 2. This testing consisted of a set of standard system and functional level regression tests customized for each system configuration. This incorporated end-to-end election scenarios testing the functionality supported by the vendor.

This effort also included documentation review of the Technical Data Package requirements, source code review, and testing of the vendor's Voting System according to FEC VSS 2002 requirements. Testing consisted of the development of a test plan, managing system configurations, executing a subset of functional test cases based on vendor test requirements, executing a sampling of vendor test cases, executing readiness tests, performing system level tests prepared by SysTest Labs and analysis of results. The review was performed at SysTest Labs' Denver, Colorado facility.

7.1 Sampling of Vendor Testing Results

Test Detail	Test Methodology
Test Case Name	**Sampling of Vendor Testing**
Scope	A sampling of vendor test cases was run and validated against The 2002 Voting System Standards (VSS) guidelines. SysTest Labs executed 9 sample test cases provided by Vendor via TDP.
Objective	To validate that the vendor's test case results are repeatable.
Sample Test Cases	See the following vendor TDPs for test case details.

7.2 System Level Test Results

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**.*
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: • 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 (V1:2.2.8.2) *Refer to each test case for the election specific **Voting Variations**.*
Variables: Election Variations	*Refer to each test case for specific **Election Variations**.*

Test Detail	Test Methodology
	(Election Core definition)
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 • 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

Test Detail	Test Methodology
	(Election Core definition)
	• 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. (V1:3.2.4.4.2.6) 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** **Pre-vote:** **Ballot Preparation procedures verifications**	Verification of Common standards includes the following and ensures that the system: • Enables the automatic formatting of ballots in accordance with the requirements for offices, candidates, and measures qualified to be placed on the ballot for each political subdivision and district • Collects and maintains data pertaining to offices and their associated labels and instructions, candidate names and their associated labels, and issues and measures and their associated text • Supports the maximum number of potentially active voting positions as indicated in vendor documentation • For Primary Elections, generates ballots that segregate the choices in partisan races by party affiliation • Generates ballots that contain identifying codes or marks uniquely associated with each new format • Ensures the vote response fields, selection buttons, or switches properly align with the specific candidate names and/or issues printed or displayed on the ballot (V1: 2.3.1.1.1) Verification of Paper-Based systems ensures that the system: • Enables voters to make selections by marking a mark in areas designated for this

Test Detail	Test Methodology
	(Election Core definition)
(cont.)	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) In addition to the common standards, vendor documentation for marksense systems is verified to contain specifications for ballot materials to ensure that vote selections are read from only a single ballot at a time, without detection of marks from multiple ballots concurrently (e.g., reading of bleed-through from other ballots). (V1:2.3.1.3.2) 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 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:	System Preparation - Security:

Test Detail	Test Methodology
	(Election Core definition)
Preparation - Security	• System username/password authentication and other access controls are set up according to system documentation guidelines for all devices being tested. • Any/all unnecessary processes are disabled and/or required process control measures noted in the documentation are followed. • All COTS and vendor subsystems used for system security are configured and active as recommended by the system documentation. This includes all connection, port, virus, and data or authorized process restriction systems. • Any other pre-election system security measures listed in the documentation are followed including setup of additional hardware or software not covered above. Please also see the Documentation section of the Security Test Case within Appendix A.
Readiness Testing and Poll Verification	Verification of Common Standards for Readiness Testing ensures that: • Voting machines or vote recording and data processing equipment, precinct and central count equipment are properly prepared for an election, and collect data that verifies equipment readiness • Status and data reports from each set of equipment can be obtained • The correct installation and interface of all system equipment • Hardware and software function correctly • Consolidated data reports at the polling place and higher jurisdictional levels can be generated • There is Segregation of test data from actual voting data, either procedurally or by hardware/software features 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, 4.4.2) 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: • The election's identification data • The identification of all equipment units • The identification of the polling place • The identification of all ballot formats • The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain only zeros) • A list of all ballot fields that can be used to invoke special voting options • Other information needed to confirm the readiness of the equipment, and to accommodate administrative reporting requirements (V1:2.3.5) In addition, 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

Test Detail	Test Methodology
	(Election Core definition)
	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 (V1:2.3.5) 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: • The election's identification data • The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain all zeros) • Other information needed to ensure the readiness of the equipment and to accommodate administrative reporting requirements (V1:2.3.6) Verification is performed to ensure that 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 performs 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 the Polling Place (Precinct Count Systems) ensures that: • An internal test of diagnostic capability to verify that all of the polling place 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) All Paper-Based Systems are verified to ensure that the following exist: • 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

Test Detail	Test Methodology
	(Election Core definition)
Voting: **Opening the Polls Verification (cont.)**	• Secure receptacles for holding voted ballots (V1: 2.4.1.2.1) Precinct Count Paper-Based Systems are verified to ensure that they have a means of: • 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 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

Test Detail	Test Methodology
	(Election Core definition)
	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:
Voting: **Opening the Polls Verification (cont.)**	• 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 • 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

Test Detail	Test Methodology
	(Election Core definition)
	• 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** **Voting:** **Required functionality verifications (cont.)**	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 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) System auditing and functional testing is performed in order to validate vote data, precinct counts, central counts, audit records and error logs. Verification is performed on the error logs based on the standards listed in 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

Test Detail	Test Methodology
	(Election Core definition)
Voting: **Required functionality verifications (cont.)**	• 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 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)

Test Detail	Test Methodology
	(Election Core definition)
Voting: **Required functionality verifications (cont.)**	Common Standards are used to ensure system integrity by validating that the voting system: • Protects, by a means compatible with these Standards, against a single point of failure that would prevent further voting at the polling place • Protects against the interruption of electronic power • Protects against generated or induced electromagnetic radiation • Protects against ambient temperature and humidity fluctuations • Protects against the failure of any data input or storage device • Protects against any attempt at improper data entry or retrieval • Records and report the date and time of normal and abnormal events • Maintains a permanent record of all original audit data that cannot be modified or overridden but may be augmented by designated authorized officials in order to adjust for errors or omissions (e.g. during the canvassing process.) • Detect and record every event, including the occurrence of an error condition that the system cannot overcome, and time-dependent or programmed events that occur without the intervention of the voter or a polling place operator • Include built-in measurement, self-test, and diagnostic software and hardware for detecting and reporting the system's status and degree of operability (V1:2.2.4.1) For paper based recording, verification is performed to ensure that the system ignores, and does not record, extraneous perforations, smudges, and folds (V1:3.2.5.2.b) DRE Systems Standards are used to ensure system integrity by validating that the voting system: • Maintains a record of each ballot cast using a process and storage location that differs from the main vote detection, interpretation, processing, and reporting path • Provides a capability to retrieve ballot images in a form readable by humans. (V1:2.2.4.2) Audit records are prepared for all testing phases of election operations using devices designed to be controlled by the jurisdiction or its contractors. These records rely upon automated audit data acquisition and machine-generated reports, with manual input of some information. These records address the ballot preparation and election definition phase, system readiness tests, and voting and ballot-counting operations. Individual test cases and steps contain instructions on how and when to generate and validate this information. (V1:2.2.5.2, 4.4, 4.4.3) Additionally, verification is done to ensure that **all** redundant DRE memory locations are being utilized and that the data is truly redundant in each location. (V1:2.2.2.2) 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

Test Detail	Test Methodology
	(Election Core definition)
Voting: **Required functionality verifications (cont.)**	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 • 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) 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-

Test Detail	Test Methodology
	(Election Core definition)
	based systems: • Outstack the ballot, or • Stop the ballot reader and display a message prompting the election official or designee to remove the ballot, or • Mark the ballot with an identifying mark to facilitate its later identification. (V1:3.2.5.1.2) 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: • An unreadable or blank ballot - return the ballot and provide a message prompting the voter to examine the ballot • Ballot with a write-in vote - segregate the ballot or mark the ballot with an identifying mark to facilitate its later identification • A ballot with an overvote the system: o Provides a capability to identify an overvoted ballot o Returns the ballot o Provides an indication prompting the voter to examine the ballot; o Allows the voter to submit the ballot with the overvote o Provides a means for an authorized election official to deactivate this capability entirely and by contest • In response to a ballot with an undervote the system: o Provides a capability to identify an undervoted ballot o Returns the ballot o Provides an indication prompting the voter to examine the ballot o Allows the voter to submit the ballot with the undervote o Provides a means for an authorized election official to deactivate this capability (V1:3.2.5.1.3) Processing speed is verified for DRE voting systems to ensure that they: • Operate at a speed sufficient to respond to any operator and voter input without perceptible delay (no more than three seconds) • If the consolidation of polling place data is done locally, performs this consolidation in a time not to exceed five minutes for each device in the polling place. (V1: 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**	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

Test Detail	Test Methodology
	(Election Core definition)
	• 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 (V1:2.2.2.1) 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 Volume1, 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: 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 (V1:2.5.1) • All systems provide a means to consolidate vote data from all polling places, and optionally from other sources such as absentee ballots, provisional ballots, and voted ballots requiring human review (e.g., write-in votes). (V1:2.5.2) • All systems are able to create reports summarizing the data on multiple levels. This provides the ability to: o Support geographic reporting, which requires the reporting of all results for each contest at the precinct level and additional jurisdictional levels o Produce a printed report of the number of ballots counted by each tabulator o Produce a printed report for each tabulator of the results of each contest that includes the votes cast for each selection, the count of undervotes, and the count of overvotes o Produce a consolidated printed report of the results for each contest of all votes cast (including the count of ballots from other sources supported by the system as specified by the vendor) that includes the votes cast for each selection, the count of undervotes, and the count of overvotes o Be capable of producing a consolidated printed report of the combination of

Test Detail	Test Methodology
	(Election Core definition)
	overvotes for any contest that is selected by an authorized official (e.g.; the number of overvotes in a given contest combining candidate A and candidate B, combining candidate A and candidate C, etc.) o Produce all system audit information required in Section 4.5 in the form of printed reports, or in electronic memory for printing centrally o Prevent data from being altered or destroyed by report generation, or by the transmission of results over telecommunications lines. (V1:2.5.3.1, 4.4.4) • In addition to the common reporting requirements, all precinct count voting systems are validated to ensure that the system: o Prevents the printing of reports and the unauthorized extraction of data prior to the official close of the polling place o Provides a means to extract information from a transportable programmable memory device or data storage medium for vote consolidation o Consolidates the data contained in each unit into a single report for the polling place when more than one voting machine or precinct tabulator is used o Prevents data in transportable memory from being altered or destroyed by report generation, or by the transmission of results over telecommunications lines (V1:2.5.3.2) • *If applicable*, the voting systems offer the capability to make unofficial results available to external organizations such as the news media, political party officials, and others. Although this capability is not required, systems that make unofficial results available: o Provide only aggregated results, and not data from individual ballots o Provide no access path from unofficial electronic reports or files to the storage devices for official data o Clearly indicate on each report or file that the results it contains are unofficial (V1:2.5.4)
Post-Vote: **Vote Count Verification**	After all voting listed in the Vote Data Matrix is performed, the election data is examined and all counts are validated on the individual voter level, the voting machine level, the precinct level and the central count level. This verification ensures that the system is correctly tabulating all data and is accurately recording cast ballots, including provisional. (V1:2.2.8.1, 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: • 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.

Test Detail	Test Methodology
	(Election Core definition)
	• 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**	Electronic memory storage devices are required to retain their data for at least 22 months to meet the United States Code Title 42 requirements and various sections of the VSS. The data retention capability of the devices will be verified by engineering analysis including a review of the manufacturer's specifications to ensure that it exceeds the requirement. In the absence of other information, such as field failures, the results of this analysis will be used to determine compliance with the 22 month retention requirement." • 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 object of this test case is to verify core functionality and performance by using the vendor's manual(s) to create election ballots, vote, and tally, for a General Election.
Variables: **Voting Variations**	The following are the items verified in this election. See the remaining election test cases for examples of all voting variations supported by the vendor. (V1:2.2.8.2) • 2 Precincts • Split Precincts (3 splits per precinct) • Non-Partisan contest: Vote for 1 of N (Sheriff) (Superintendent of Schools) • Non-Partisan contest: "Vote for 1" race with a single candidate and a write-in (Superintendent of Schools) • Non-Partisan contest: "Vote for 1" race with no declared candidates and write-in (Sheriff) • Non-Partisan contest: Multi-member board (N of M) (County Commissioner) • Non-Partisan contest: Proposition/Question (Proposition X) • Partisan contest: Vote for 1 of N (Secretary of State) (City Council) (Attorney General) (County Treasurer) • Partisan contest: "Vote for 1" race with a single candidate and a write-in (Attorney General) • Partisan contest: "Vote for 1" race with no declared candidates and write-ins (County Treasurer) • Partisan contest: Multi-member board includes declared candidates with write-in voting (City Council) • Partisan contest: "Vote for 1 of M" race where one party does not declare candidates (Secretary of State) • Partisan contest: Slate & Group voting: one selection votes the slate (Governor/Lt. Governor) • Recall Type A: Simple Yes/No question (Recall Judge) • Recall Type B: Retain/Replace (Replace Judge) • Rotation = Standard (Rotates with every new Precinct) (Governor/Lt. Governor) Additional system functionality: • Volatile Flush Header • M650 Network to create 10 node folders • M650 Early Voting Group • Coded Ballots • Onscreen Vote (iVotronic) • Reject (M100/DS200 option only)
Variables: **Election Variations**	**Governor/Lt. Governor**: 4 candidates **Sheriff**: no candidate/write-in **Superintendent of Schools**: 1 candidate/1 write-in **County Commissioner**: 4 candidates **Proposition X:** Y/N

Test Detail	Test Methodology
Test Case Name	**GEN01 - General Election**
	Secretary of State: 3 candidates (no DEM candidate) **City Council**: 6 candidates/write-in **Attorney General**: 1 candidate/write-in **County Treasurer:** no candidate/write-in **Recall Judge (District A):** Y/N **Replace Judge (District B):** Retain = first option, Replace = second and third options
A description of the voting system type and the operational environment	**EDM** - Election Data Manager **iVIM** – iVotronic Image Manager **HPM** - Hardware Programming Manager **AIMS** - AutoMARK Information Management System **AM** - Audit Manager **DAM** - Data Acquisition Manager **ERM** - Election Reporting Manager **ESSIM** - ES&S Ballot Image Manager **VAT** - AutoMARK Voter Assist Terminal (A200) **M100** - Model 100 Ballot Scanner **DS200** - intElect DS200 Ballot Scanner **iVotronic** - iVotronic DRE **M650** - Model 650 Optical Scan Central Count Counter
Additional Voting Functionality Variations	Note: For Provisional/Challenged ballots, the vendor supports tabulation of these ballots at Central Count

Test Detail	Test Methodology
Test Case Name	**GEN 02 – Straight Party**
NOTE	*This test case is to be used in conjunction with the **Election Core definition**.*
Objective	The object of this test case is to verify core functionality and performance by using vendor manual(s) to create election ballots, vote, and tally, for a General Election: Straight Party
Variables: **Voting Variations**	The 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 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 and no split precincts • Straight party (multi-member board) • Cross-over voting • Non-Partisan contest: Vote for 1 of N (Sheriff) (Superintendent of Schools) • Non-Partisan contest: "Vote for 1" race with a single candidate and a write-in (Superintendent of Schools) • Non-Partisan contest: "Vote for 1" race with no declared candidates and write-ins (Sheriff) • Non-Partisan contest: Multi-member board (N of M) (County Commissioner) • Non-Partisan contest: Proposition/Question (Proposition X) • Partisan contest: Vote for 1 of N (Governor/Lt. Governor) (Secretary of State) (City Council) (Attorney General) (County Treasurer) • Partisan contest: "Vote for 1" race with a single candidate and a write-in (Attorney General) • Partisan contest: "Vote for 1" race with no declared candidates and write-ins (County Treasurer) • Partisan contest: Multi-member board includes declared candidates with write-in voting (City Council) • Partisan contest: "Vote for 1 of M" race where one party does not declare candidates (Secretary of State) • Partisan contest: Slate & Group voting: one selection votes the slate (Governor/Lt. Governor) • Recall Type A: Simple Yes/No question (Recall Judge) • Recall Type B: Retain/Replace (Replace Judge) • Recall Type C: Retain/Recall Conditional contest (Judge recall) Additional system functionality: • Networked M650
Variables: **Election Variations**	**Governor/Lt. Governor**: 4 candidates **Sheriff**: no candidate/write-in **Superintendent of Schools**: 1 candidate/1 write-in **County Commissioner**: 4 candidates **Proposition X:** Y/N

Test Detail	Test Methodology
Test Case Name	**GEN 02 – Straight Party**
	Secretary of State: 3 candidates (no DEM candidate) **City Council**: 6 candidates/write-in **Attorney General**: 1 candidate/write-in **County Treasurer:** no candidate/write-in **Recall Judge (District A):** Y/N **Replace Judge (District B):** Retain = first option, Replace = second and third options **Recall/Retain Judge (District C) (1st Contest):** Y/N **Recall/Retain Judge (District C) (2nd Contest):** 1 option to replace with 2 candidates
A description of the voting system type and the operational environment	**EDM** - Election Data Manager **iVIM** – iVotronic Image Manager **HPM** - Hardware Programming Manager **AIMS** - AutoMARK Information Management System **AM** - Audit Manager **DAM** - Data Acquisition Manager **ERM** - Election Reporting Manager **ESSIM** - ES&S Ballot Image Manager **VAT** - AutoMARK Voter Assist Terminal (A100) **M100** - Model 100 Ballot Scanner (with PEB merge) **iVotronic** - iVotronic DRE **M650** - Model 650 Optical Scan central Count Counter
Additional Voting Functionality Variations	Note: For Provisional/Challenged ballots, the vendor supports tabulation of these ballots at Central Count Using the iVotronic Auto Recovery procedure v.9.2.0.0, vote an election and recover the results from the ScanDisk and not the PEB.

Test Detail	Test Methodology
Test Case Name	**GEN02 – Pennsylvania Straight Party with Cross Party Endorsement**
NOTE	*This test case is to be used in conjunction with the **Election Core definition**.*
Objective	The object of this test case is to verify core functionality and performance by using vendor manual(s) to create election ballots, vote, and tally, for a General Election: Straight Party for Pennsylvania
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 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) • Two page ballot election per voter • 7 precincts and no split precincts • Straight party (multi-member board) • Non-Partisan contest: Vote for 1 of N (Sheriff) (Superintendent of Schools) • Non-Partisan contest: "Vote for 1" race with a single candidate and a write-in (Superintendent of Schools) • Non-Partisan contest: "Vote for 1" race with no declared candidates and write-ins (Sheriff) • Non-Partisan contest: Multi-member board (N of M) (County Commissioner) • Non-Partisan contest: Proposition/Question (Proposition X) • • Partisan contest: Vote for 1 of N (Governor/Lt. Governor) (Secretary of State) (City Council) (Attorney General) (County Treasurer) • Partisan contest: "Vote for 1" race with a single candidate and a write-in (Attorney General) • Partisan contest: "Vote for 1" race with no declared candidates and write-ins (County Treasurer) • Partisan contest: Multi-member board and cross-endorsed candidates (City Council) • Partisan contest: "Vote for 1 of M" race where one party does not declare candidates (Secretary of State) • Partisan contest: Slate & Group voting: one selection votes the slate (Governor/Lt. Governor) • Recall Type A: Simple Yes/No question (Recall Judge) • Recall Type B: Retain/Replace (Replace Judge) • Recall Type C: Retain/Recall Conditional contest (Judge recall) • Rotation: Votronic Auto Rotate (rotation with each new voter)
Variables: **Election Variations**	**Governor/Lt. Governor**: 4 candidates **Sheriff**: no candidate/write-in **Superintendent of Schools**: 1 candidate/1 write-in **County Commissioner**: 4 candidates **Proposition X:** Y/N **Secretary of State**: 3 candidates (no DEM candidate) **City Council**: 6 candidates/write-in, cross party endorsement **Attorney General**: 1 candidate/write-in **County Treasurer:** no candidate/write-in **Recall Judge (District A):** Y/N

Test Detail	Test Methodology
Test Case Name	**GEN02 – Pennsylvania Straight Party with Cross Party Endorsement**
	Replace Judge (District B): Retain = first option, Replace = second and third options **Recall/Retain Judge (District C) (1st Contest):** Y/N **Recall/Retain Judge (District C) (2nd Contest):** 1 option to replace with 2 candidates
A description of the voting system type and the operational environment	**EDM** - Election Data Manager **iVIM** – iVotronic Image Manager **HPM** - Hardware Programming Manager **AIMS** - AutoMARK Information Management System **AM** - Audit Manager **DAM** - Data Acquisition Manager **ERM** - Election Reporting Manager **ESSIM** - ES&S Ballot Image Manager **VAT** - AutoMARK Voter Assist Terminal (A200) **M100** - Model 100 Ballot Scanner **iVotronic** - iVotronic DRE **M650** - Model 650 Optical Scan central Count Counter
Additional Voting Functionality Variations	Note: For Provisional/Challenged ballots, the vendor supports tabulation of these ballots at Central Count Note: Blank ballots (Not applicable on the iVotronic)

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 election ballots, vote, and tally, for a General Election while also testing Error Messages, Languages, Usability and Accessibility.
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 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 • Provisional/Challenged ballots • Non-Partisan contest: Vote for 1 of M (Sheriff) • Non-Partisan contest: Proposition/Question (Proposition X) • Partisan contest: Multi-member board, "Vote for 3 of M" race with declared candidates with a voting position defined for write-in (City Council) • Type D: Recall/Retain contest (12" 3-Key only) Additional system functionality: • Multi-language ballots (English and Spanish) • Audio/Visual/Combo ballots • 15" iVotronic with 3-key, 4-Key, 6-Key (6-Key supports sip and puff) • 12" iVotronic 3-Key • VVPAT printer • Error Messages and Recovery (V.1:2.2.5.2.2 and 2.2.3.a)
Variables: **Election Variations**	**Sheriff:** 4 candidates **City Council:** 6 candidates/write-in **Proposition X:** Y/N **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	**EDM** - Election Data Manager **iVIM** – iVotronic Image Manager **HPM** - Hardware Programming Manager **AIMS** - AutoMARK Information Management System **AM** - Audit Manager **ERM** - Election Reporting Manager **ESSIM** - ES&S Ballot Image Manager **VAT** - AutoMARK Voter Assist Terminal (A100) & (A200) **iVotronic** - iVotronic DRE (12" & 15") **ABCR Scanner** – Automatic Bar Code Reader **Voyager Hand-held scanner** – hand held device

Test Detail	Test Methodology
Test Case Name	**GEN03 – Usability and Accessibility**
	Refer to the following tables for complete descriptions: ➢ Matrix of Required Software/Firmware ➢ Matrix of Required Hardware
Additional Voting Functionality Variations	Note: For Provisional/Challenged ballots, the vendor supports tabulation of these ballots at Central Count

Test Detail	Test Methodology
Test Case Name	**40HTEST1 - General Election**
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 the vendor's manual(s) to create election ballots, vote, and tally, for a General Election.
Variables: **Voting Variations**	The following are the items verified in this election. See the remaining election test cases for examples of all voting variations supported by the vendor. (V1:2.2.8.2) • 19 Precincts • Straight Party (multi-member board) • Partisan contest: Vote for 1 of N • Partisan contest: Multi-member board (N of M) • Non-Partisan contest: Proposition/Question (Proposition X) • Recall Type A: Simple Yes/No question (Recall Judge) Additional system functionality: • Two page ballot • Onscreen cast ballot button (iVotronic) • Cast ballot confirmation (iVotronic) • Print undervotes (iVotronic)
Variables: **Election Variations**	**United States Senator:** 2 candidates/write-in **Secretary of State:** 3 candidates/write-in **Auditor of State:** 2 candidates **Treasurer of State:** 2 candidates **US Representative in Congress:** 2 candidates/write-in **State Representative:** 1 candidate **Judge of the Circuit:** 1 candidate **Prosecuting Attorney:** 2 candidate **County Auditor:** 1 candidate **County Treasurer:** 2 candidates **County Sheriff:** 1 candidate **County Assessor:** 1 candidate **County Commissioner:** 1 candidate **County Council Member:** 5 candidates **Township Trustee:** 22 candidates **Township Board Member:** 59 candidates **Recall Judge (District A):** Y/N

Test Detail	Test Methodology
Test Case Name	**40HTEST1 - General Election**
A description of the voting system type and the operational environment	**EDM** - Election Data Manager **HPM** - Hardware Programming Manager **AM** - Audit Manager **ESSIM** - ES&S Ballot Image Manager **iVIM** – iVotronic Image Manager **M100** - Model 100 Ballot Scanner **DS200** - intElect DS200 Ballot Scanner **iVotronic** - iVotronic DRE

Test Detail	Test Methodology
Test Case Name	**40HTEST3 - Functional**
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 the on-screen message(s) change when two different election definitions are utilized containing two different state codes.
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) • 20 Precincts with splits • Partisan contest: Vote for 1 of N • Non-Partisan contest: Vote for 1 of N
Variables: **Election Variations**	**Office 1:** 3 candidates/write-in **Office 2:** 3 candidates/write-in **Office 3:** 2 candidates/write-in **Office 4:** 21 candidates/write-in **Office 5:** 9 candidates/write-in **Office 6:** 6 candidates/write-in **Office 7:** 15 candidates/write-in **Office 8:** 26 candidates/write-in (PRC contest)
A description of the voting system type and the operational environment	**EDM** - Election Data Manager **HPM** - Hardware Programming Manager **AM** - Audit Manager **ESSIM** - ES&S Ballot Image Manager **M100** - Model 100 Ballot Scanner **DS200** - intElect DS200 Ballot Scanner 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. • Two election definitions are required, one must be coded with the state code of FL
Documentation of Test Data & Test Results	For each iteration that the election is run: • Ensure the election definition loaded with the state code of FL suppresses the overvote warning message(s)

Test Detail	Test Methodology
Test Case Name	**40HTEST4 - Functional**

Test Detail	Test Methodology
Test Case Name	**40HTEST4 - Functional**
NOTE	*This test case is to be used in conjunction with the **Election Core definition**.*
Objective	The object of this test case is to create a subset election in HPM, from an existing election, ensure media can be burned, election loaded on an M650, and a ballot can be accepted.
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) • 20 Precincts with splits • Partisan contest: Vote for 1 of N • Non-Partisan contest: Vote for 1 of N
Variables: **Election Variations**	**Office 1:** 3 candidates/write-in **Office 2:** 3 candidates/write-in **Office 3:** 2 candidates/write-in **Office 4:** 21 candidates/write-in **Office 5:** 9 candidates/write-in **Office 6:** 6 candidates/write-in **Office 7:** 15 candidates/write-in **Office 8:** 26 candidates/write-in (PRC contest)
A description of the voting system type and the operational environment	**EDM** - Election Data Manager **HPM** - Hardware Programming Manager **AM** - Audit Manager **ESSIM** - ES&S Ballot Image Manager **M650** - Model 650 Optical Scan central Count Counter
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. • In HPM, create a subset election from the 40HTEST3 election • PRC contest appears and floats
Documentation of Test Data & Test Results	For each iteration that the election is run: • Ensure PRC candidates rotate

Test Detail	Test Methodology
Test Case Name	**40HTEST5 - Functional**
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 HPM can accept an Open Primary election with greater than nine Party Preference contests.
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) • 20 Precincts with splits • Partisan contest: Vote for 1 of N • Non-Partisan contest: Vote for 1 of N • 2 page ballot
Variables: **Election Variations**	**Office 1:** 3 candidates/write-in **Office 2:** 3 candidates/write-in **Office 3:** 2 candidates/write-in **Office 4:** 21 candidates/write-in **Office 5:** 9 candidates/write-in **Office 6:** 6 candidates/write-in **Office 7:** 15 candidates/write-in **Office 8:** 26 candidates/write-in (PRC contest)
A description of the voting system type and the operational environment	**EDM** - Election Data Manager **HPM** - Hardware Programming Manager **AM** - Audit Manager
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. • In HPM, create a subset election from the 40HTEST3 election • PRC contest appears and floats
Documentation of Test Data & Test Results	For each iteration that the election is run: • Ensure PRC candidates rotate

Test Detail	Test Methodology
Test Case Name	**3000 PCTS - Functional**
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 media can be burned for the iVotronic, a ballot can be loaded, voted, cancelled, and the polls can be closed.
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) • 3000 Precincts • Partisan contest: Vote for 1 of N General with Straight Party • 1 page ballot
Variables: **Election Variations**	**US Senator:** 2 candidates **Secretary of State:** 2 candidates **Auditor of State:** 2 candidates **Treasurer of State:** 2 candidates **US Representative in Congress:** 14 candidates **State Senator:** 2 candidates **State Representative:** 1 candidates
A description of the voting system type and the operational environment	**EDM** - Election Data Manager **HPM** - Hardware Programming Manager **AM** - Audit Manager **iVIM** – iVotronic Image Manager **iVotronic** - iVotronic DRE
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. • HPM can import large election (greater than 1300 precincts) • Correctly handles more than 150 straight party contests
Documentation of Test Data & Test Results	For each iteration that the election is run: • No longer manually correct straight party rotation, HPM handles automatically

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 functionality and performance by using vendor manual(s) to create election ballots, vote, and tally, for an Open Primary Election
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 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) • 5 precincts • Non-Partisan contest: Vote for 1 of N (Sheriff) (Superintendent of Schools) • Non-Partisan contest: "Vote for 1" race with a single candidate and a write-in (Superintendent of Schools) • Non-Partisan contest: "Vote for 1" race with no declared candidates and write-ins (Sheriff) • Non-Partisan contest: Multi-member board (N of M) (County Commissioner) • Partisan contest: Vote for 1 of N (Governor/Lt. Governor) (Secretary of State) (City Council) (Attorney General) (County Treasurer) • Partisan contest: "Vote for 1" race with no declared candidates and write-ins (County Treasurer) • Partisan contest: Multi-member board (City Council) • Primary Presidential Nominations List only the nominees, not the delegates • Rotation: Districts by Registered Voters (Non-Partisan) (Rotates based on the precincts registered voters)
Variables: **Election Variations**	**Presidential Nominee:** 3 candidates (DEM) **Presidential Nominee:** 2 candidates (REP) **Presidential Nominee:** 2 candidates (SCI) **Secretary of State:** no declared candidate/1 write-in (DEM) **Secretary of State:** 3 candidates (REP) **Secretary of State:** 2 candidates (SCI) **Alderman:** 3 candidates (DEM) **Alderman:** 4 candidates (REP) **Alderman:** 3 candidates (SCI) **Sheriff:** no declared candidate/1 write-in **Superintendent of Schools:** 1 candidate, 1 write-in **School Board:** 6 candidates/write-in

Test Detail	Test Methodology
Test Case Name	**PRI01 – Open Primary**
A description of the voting system type and the operational environment	**EDM** - Election Data Manager **iVIM** – iVotronic Image Manager **HPM** - Hardware Programming Manager **AIMS** - AutoMARK Information Management System **AM** - Audit Manager **DAM** - Data Acquisition Manager **ERM** - Election Reporting Manager **ESSIM** - ES&S Ballot Image Manager **VAT** - AutoMARK Voter Assist Terminal (A100) **M100** - Model 100 Ballot Scanner **iVotronic** - iVotronic DRE **M650** - Model 650 Optical Scan central Count Counter
Additional Voting Functionality Variations	Note: For Provisional/Challenged ballots, the vendor supports tabulation of these ballots at Central Count 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 functionality and performance by using vendor manual(s) to create election ballots, vote, and tally, for an Open Primary Election, Party selection.
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 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) • 5 precincts • Non-Partisan contest: Vote for 1 of N (Sheriff) (Superintendent of Schools) • Non-Partisan contest: "Vote for 1" race with a single candidate and a write-in (Superintendent of Schools) • Non-Partisan contest: "Vote for 1" race with no declared candidates and write-ins (Sheriff) • Non-Partisan contest: Multi-member board (N of M) (County Commissioner) • Partisan contest: Vote for 1 of N (Governor/Lt. Governor) (Secretary of State) (City Council) (Attorney General) (County Treasurer) • Partisan contest: "Vote for 1" race with no declared candidates and write-ins (County Treasurer) • Partisan contest: Multi-member board (City Council) • Primary Presidential Nominations List only the nominees, not the delegates • Rotation: Standard (Candidate > Vote for)
Variables: **Election Variations**	**Presidential Nominee:** 3 candidates (DEM) **Presidential Nominee:** 2 candidates (REP) **Presidential Nominee:** 2 candidates (SCI) **Secretary of State:** no declared candidate/1 write-in (DEM) **Secretary of State:** 3 candidates (REP) **Secretary of State:** 2 candidates (SCI) **Alderman:** 2 candidates (DEM) **Alderman:** 4 candidates (REP) **Alderman:** 3 candidates (SCI) **Sheriff:** no declared candidate/1 write-in **Superintendent of Schools:** 1 candidate, 1 write-in **School Board:** 6 candidates/write-in

Test Detail	Test Methodology
Test Case Name	**PRI01 – Open Primary with Pick-a-Party/Party Preference**
A description of the voting system type and the operational environment	**EDM** - Election Data Manager **iVIM** – iVotronic Image Manager **HPM** - Hardware Programming Manager **AIMS** - AutoMARK Information Management System **AM** - Audit Manager **DAM** - Data Acquisition Manager **ERM** - Election Reporting Manager **ESSIM** - ES&S Ballot Image Manager **VAT** - AutoMARK Voter Assist Terminal (A200) **M100** - Model 100 Ballot Scanner **iVotronic** - iVotronic DRE **M650** - Model 650 Optical Scan central Count Counter
Additional Voting Functionality Variations	Note: For Provisional/Challenged ballots, the vendor supports tabulation of these ballots at Central Count 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 functionality and performance by using vendor manual(s) to create election ballots, vote, and tally, for a Closed Primary Election.
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 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) • 7 precincts • Non-Partisan contest: Vote for 1 of N (Sheriff) (Superintendent of Schools) • Partisan contest: Vote for 1 of N (Governor/Lt. Governor) (Secretary of State) (City Council) (Attorney General) (County Treasurer) • Partisan contest: Multi-member board (City Council) • Partisan contest: "Vote for 1 of M" race where one party does not declare candidates (Secretary of State) • Primary Presidential Delegates: a delegate slate, display of delegates with nominees • Recall Type D: Retain/Recall Conditional contest (Judge recall) • Query Undervote enabled on Precinct Paper Tabulators (100/200) • M650 Absentee • Rotation: District by Registered Voters (Rotates based on party's registered voters by Party)
Variables: **Election Variations**	**Presidential Delegates:** 3 sets of candidates (DEM) **Presidential Delegates:** 2 sets of candidates (REP) **Presidential Delegates:** 2 sets of candidates (SCI) **Secretary of State:** no declared candidate/1 write-in (DEM) **Secretary of State:** 3 candidates (REP) **Secretary of State:** 2 candidates (SCI) **Alderman:** 2 candidates (DEM) **Alderman:** 4 candidates (REP) **Alderman:** 3 candidates (SCI) **Sheriff:** no declared candidate/1 write-in **Superintendent of Schools:** 1 candidate, 1 write-in **School Board:** 6 candidates/write-in **Recall/Retain Judge (District D) (1st Contest):** Y/N **Recall/Retain Judge (District D) (2nd Contest):** 1 option to replace with 2 candidates

Test Detail	Test Methodology
Test Case Name	**PRI02 – Closed Primary**
A description of the voting system type and the operational environment	**EDM** - Election Data Manager **iVIM** – iVotronic Image Manager **HPM** - Hardware Programming Manager **AIMS** - AutoMARK Information Management System **AM** - Audit Manager **DAM** - Data Acquisition Manager **ERM** - Election Reporting Manager **ESSIM** - ES&S Ballot Image Manager **VAT** - AutoMARK Voter Assist Terminal (A100) **M100** - Model 100 Ballot Scanner **DS200** - intElect DS200 Ballot Scanner **iVotronic** - iVotronic DRE **M650** - Model 650 Optical Scan central Count Counter
Additional Voting Functionality Variations	Note: For Provisional/Challenged ballots, the vendor supports tabulation of these ballots at Central Count Party affiliation is identified on the ballots *where appropriate*

Test Detail	Test Methodology
Test Case Name	**Readiness**
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
A listing of the applicable voting system machines	**EDM** - Election Data Manager **iVIM** – iVotronic Image Manager **HPM** - Hardware Programming Manager **AIMS** - AutoMARK Information Management System (Create & Import) **AM** - Audit Manager **DAM** - Data Acquisition Manager **ERM** - Election Reporting Manager **ESSIM** - ES&S Ballot Image Manager **VAT** - AutoMARK Voter Assist Terminal (A100 & A200) **M100** - Model 100 Ballot Scanner **DS200** - intElect DS200 Ballot Scanner **iVotronic** - iVotronic DRE (12 & 15) **M650** - Model 650 Optical Scan central Count Counter
Pre-requisites and initialization of the test case	This testing is to be executed on initial testing and each time the system is to be shut down and restarted.
Documentation of Test Data & Test Results	For each iteration that the election is run: • Capture all voting steps in order to maintain repeatability of the test • Record election, ballot, and vote data fields on the corresponding worksheet tabs • Save all worksheet tabs for all iterations of the test case • Record results of test run by entering 'Accept/Reject' on the Test Results Matrix • Provide comments when observing deviations, discrepancies or notable observations • Log discrepancies on the Discrepancy Report
System Preparation - Security	System Preparation - Security: • System username/password authentication and other access controls are set up according to system documentation guidelines for all devices being tested. • Any/all unnecessary processes are disabled and/or required process control measures noted in the documentation are followed. • All COTS and vendor subsystems used for system security are configured and active as recommended by the system documentation. This includes all connection, port, virus, and data or authorized process restriction systems. • Any other pre-election system security measures listed in the documentation are followed including setup of additional hardware or software not covered above.

Test Detail	Test Methodology
Test Case Name	**Readiness**
	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 Data manager (EDM) Checklist** **Election Day Training manual** Unity Version 4.0 Release Date: August 2007 **Audit Manager Checklist** **Election Day Training manual** Unity Version 4.0 Release Date: August 2007 **Hardware Programming Manager (HPM) Checklist** **Election Day Training manual** Unity Version 4.0 Release Date: August 2007 **iVotronic Voting System** **Election Day Training manual** Unity Version 4.0 Release Date: August 2007 **Model 100 Precinct Scanner** **Pre-Election Day Checklist** Unity Version 4.0 Release Date: August 2007 **Model 650 Central Scanner** **Pre-Election Day Checklist** Unity Version 4.0 Release Date: August 2007

Test Detail	Test Methodology
Test Case Name	**Readiness**
	Windows XP on Dell Optiplex **Installation Guide** Version 5.1 Release Date: August 20, 2007 **ESS Image Manager (ESSIM) Checklist** **Election Day Training manual** Unity Version 4.0 Release Date: August 2007 **DS200 Precinct Scanner** **Election Day Checklist** Unity Version 4.0 Release Date: September 2007 **DAM/ERM Checklist** **Election Day Training manual** Unity Version 4.0 Release Date: September 2007 **iVotronic Image Manager (iVIM) Checklist** **Election Day Training manual** Unity Version 4.0 Release Date: August 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.
Documentation of Test Data & Test Results	For each iteration that the election is run: • Capture all voting steps in order to maintain repeatability of the test • Record election, ballot, and vote data fields on the corresponding worksheet tabs • Save all worksheet tabs for all iterations of the test case • Record results of test run by entering 'Accept/Reject' on the Test Results Matrix • Provide comments when observing deviations, discrepancies or notable observations • Log discrepancies on the Discrepancy Report
Operational Status Check Verification	During this process, all equipment will be operated in a manner and environmental conditions that simulate election use to verify the functional status of the system. Prior to the conduct of each of the environmental hardware non-operating tests, a supplemental test will be made to determine that the operational state of the equipment is within acceptable performance limits. The following procedures will be followed to verify the equipment status: Step 1: Arrange the system for normal operation. Step 2: Turn on power, and allow the system to reach recommended operating temperature. Step 3: Perform any servicing, and make any adjustments necessary, to achieve operational status. Step 4: Operate the equipment in all modes, demonstrating all functions and features that would be used during election operations. Step 5: Verify that all system functions have been correctly executed.
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

Test Detail	Test Methodology
Test Case Name	**Operational Status Check**
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	**EDM** - Election Data Manager **iVIM** – iVotronic Image Manager **HPM** - Hardware Programming Manager **AIMS** - AutoMARK Information Management System (Create & Import) **AM** - Audit Manager **DAM** - Data Acquisition Manager **ERM** - Election Reporting Manager **ESSIM** - ES&S Ballot Image Manager **VAT** - AutoMARK Voter Assist Terminal (A100 & A200) **M100** - Model 100 Ballot Scanner

Test Detail	Test Methodology
Test Case Name	**Security**
	DS200 - intElect DS200 Ballot Scanner **iVotronic** - iVotronic DRE (12 & 15) **M650** - Model 650 Optical Scan central Count Counter 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 **1.12** Hardware component BIOS or Firmware is protected from modifications (V1:6.2.1.1.b)

Test Detail	Test Methodology
Test Case Name	**Security**
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 • 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) • System provides access controls that conform to requirement V2:6.4.1
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 private or public 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) **3.3** Security tests are designed to defeat the security provisions of the system including modification or disruption of pre-voting, voting, and post voting processing; unauthorized access to, deletion, or modification of data, including audit trail data; and modification or elimination of security mechanisms; (V2:A4.5.3e)
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

Test Detail	Test Methodology
Test Case Name	**Security**
	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 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

Test Detail	Test Methodology
Test Case Name	**Security**
	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 private or public data networks using 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 **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

Test Detail	Test Methodology
Test Case Name	**Security**
	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 **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.

Test Detail	Test Methodology
Test Case Name	**Security**
	(V1:6.2.2) **11.5** The vendor develops and provides detailed documentation, pertaining to polling place security operations, of measures to anticipate and counteract vandalism, civil disobedience, and similar occurrences of. The measures: (V1:6.3.1) • 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 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

Test Detail	Test Methodology
Test Case Name	**Security**
	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 • 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

Test Detail	Test Methodology
Test Case Name	**Security**
	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 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)

Test Detail	Test Methodology
Test Case Name	**Telecommunications**
Scope	A functional test that uses the 2002 Voting System Standards (VSS) guidelines to validate required functionality. Testing includes Telecommunications capability of the vendor's voting system. During the FCA and PCA, all communication components of the Voting System are identified. Telecom and related Security tests are necessary for each component (DATA UNIT or DU) participating in a data interchange. Each DU (scanner, tabulator, DRE, PC) with the supported mediums of data exchange and roles of SENDER and RECEIVER creates a baseline to establish the initial scope of the required Telecommunications and Security conformance tests. The type of data and physical communication link technology employed by a DU (Serial, Dial-up, Lan, Wan, Wifi, GPRS) will necessitate a test case and will influence the overall scope of the testing, laboratory environment preparation, and required hardware and software testing toolsets.
Objective	The object of this test case is to verify that the physical, technical, and procedural (documentation) controls correspond correctly for Telecommunication features.
Standards Documents	Voting System Standards 2002, vol. 1 Voting System Standards 2002, vol. 2 Specific standards are noted in following steps.
A description of the voting system type and the operational environment	The ES&S Unity 4.0 system has specific components involved in the storage, transfer and validation of election results after the polls are closed. The iVotronic DRE, M100 and DS200 ballot scanners, store the election results during the election voting phase, and when configured with communications capability, will transmit their respective results files via public telephone lines to the Central Count location. The ERM (Election Reporting Manager) module contains the central vote tallying functions and supports reading of the election equipment media directly into the election database. The ERM PC may be configured with various media reader/writer devices, from which the election results of the supported election equipment is hand carried to the ERM (Central Count) location, and subsequently read and stored in the election central database. Additionally, the ERM computer can also read results from an iVotronic DRE with a directly connected serial (null modem) cable. The DAM (Data Acquisition Manager) module has two configurations, (Host and Remote) and is dedicated to the transfer of election results from precincts and polling places to the ERM Central Count location. The DAM Remote module operates at the precincts and polling places to read in media from the voting equipment and transmit the election results via public telephone lines to the DAM Host at the Central Count location. DAM Host, upon receipt of election results from either a DAM Remote computer or a communications equipped voting machine, stores the election results on a shared folder where the ERM module can read the results for tabulating and reporting. The DAM Host module maintains a precinct status file, which enables the user to view the completion status of the overall election results from all precincts and polling places. The last major component of the DAM Host is the TCP Host, which runs on the Central Count LAN to consolidate election results from the M650 high-speed ballot scanners. The M650s configured with NICs (Network Interface Cards) can store their election results to shared folders on the same LAN as ERM

Test Detail	Test Methodology
Test Case Name	**Telecommunications**
Test Classifications	Voting System telecommunications capabilities and associated components identified by the FCA and PCA are assigned to a predefined baseline test class, or a specialized class is created for any unique functionality or technology employed. Due to user configurable system options present in Voting Systems, each DU test component may have relevance in one or more phases of the System Level testing processes. **Telecommunication Test Case Classifications:**

Test Id	Test Class	Telecommunication Test Class Description
	Setup	
1	base test	Configure and validate basic device communication functionality, usability
	Pre Election	
2	no com	PC Election / Ballot to Device using media
3	direct com	PC Election / Ballot to Device using Serial, Parallel, USB ports
4	Land line modem	PC Election / Ballot to Device using Dialup public telephone network
5	Lan	PC Election / Ballot to Device using LAN
6	Wan	PC Election / Ballot to Device using WAN
7	RF Lan	PC Election / Ballot to Device data using wireless private LAN
8	RF Wan	PC Election / Ballot to Device using public / global wireless WAN
	Post Election	
101	no com	Device poll results using device media to PC with media readers
102	direct connect	Device poll results using direct cable connect to PC com ports
201	Public land line 1	Device transmit results to PC
202	Public land line 2	PC transmit consolidated device results to PC
301	Private Lan 1	Device results to PC
302	Private Lan 2	PC consolidated device results to PC
303	Private Wan 1	Device results to PC on private WAN
304	Public Wan 1	Device results to PC using public WAN / Internet
401	Private RF Lan 1	Device results to PC using private LAN (&/or WAN)
402	Public RF Lan 1	Device results to PC using Wireless Internet

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

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

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

Test Detail	Test Methodology
Test Case Name	**Telecommunications**

Operational, Exception Handling and Security Test Case Classifications:

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

Pre-requisites and initialization of the test case

The Setup and Pre Election phases of testing may determine a Data Unit's communications behavior; thereby requiring instances of repeatable test steps in separate phases of a System Level Test cycle. Testing procedures will employ either software prescribed, or administrative system backups, and restorations, to eliminate the replication of System Level end-to-end testing.

- Prepare device & test specific option setting
- Prepare computer and device peripheral hardware options
- Load firmware/data media
- Validate basic device communication functionality, usability

Test Verifications

Evaluation and verification of the voting system components and associated documentation involved with telecommunications ensure compliance with the following VSS 2002 requirements:

1. Verify that data is transmitted with no alteration, or unauthorized disclosure and such transmissions shall not violate the privacy, secrecy, and integrity demands of the Standards (V1: 2.2.10)
    - Ballot Definition:
    - Vote Count:
    - **N/A** for Unity 4.0 system: Voter Authentication: Vote Transmission to Central Site: List of Voters:

2. Verify the Data Network Requirements to ensure all components of the Voting system residing on a local or remote data network, shall comply with the telecommunications requirements described in Section 5 of the Standards and the Security requirements described in Section 6. (V1: 3.2.2.15)

3. Verify and document type of components on the components tab using the vendor documentation. (V1: 5.1.1)

Test Detail	Test Methodology
Test Case Name	Telecommunications
	4. Voting-related transmission over a public network. Verify components acquired by the Jurisdiction for the purpose of Voting, and components acquired by others used at settings supervised by election officials (V1: 5.1.2) 5. Verify the types of data transmissions used for preparation and execution of an election, and the preservation of the system data and audit trails following an election (V1: 5.1.3) • Ballot Definition: • Vote Count: • **N/A** for Unity 4.0 system: Voter Authentication: Vote Transmission to Central Site: List of Voters: 6. Verify the Design, Construction, and Maintenance Requirements - Capabilities considered basic to all data transmissions to ensure that all telecommunications components meet: (V1: 5.2) • Accuracy requirements of Section 3.2.1. (V1: 5.2.1) • Durability requirements of Section 3.4.2. (V1: 5.2.2) • Reliability requirements of Section 3.4.3. (V1: 5.2.3) • Maintainability requirements of Section 3.4.4. (V1: 5.2.4) • Availability requirements of Section 3.4.5. (V1: 5.2.5) 7. Verify Integrity - For WANs using public telecommunications, boundary definition and implementation shall meet the following requirements. (V1: 5.2.6) • Outside service providers and subscribers of such providers shall not be given direct access or control of any resource inside the boundary; • Voting system administrators shall not require any type of control of resources outside this boundary. Regardless of the technology used, the boundary point must ensure that everything on one side is locally configured and controlled while everything on the other side is controlled by an outside service provider; and • The system shall be designed and configured such that it is not vulnerable to a single point of failure in the connection to the public network causing total loss of voting capabilities at any polling place. 8. Verify Confirmation of the successful or unsuccessful completion of the data transmission. To provide confirmation, the telecommunications components of a voting system shall: (V1: 5.2.7) • Notify the user of the successful or unsuccessful completion of the data transmission; and • In the event of unsuccessful transmission, notify the user of the action to be taken. 9. Verify Access Control procedures and system capabilities that detect or limit access to system components in order to guard against loss of system integrity, availability, confidentiality, and accountability (V1: 6.5.1 & V1: 6.2), Verify all system access control measures designed to permit authorized access to the system and prevent unauthorized access, such measures include: (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;

Test Detail	Test Methodology
Test Case Name	Telecommunications
	• Security kernels; • Computer-generated password keys; • Special protocols; • Message encryption; and • Controlled access security. 10. Verify Data Integrity by validating that transmission of data shall ensure the receipt of valid vote records is verified at the receiving station. Verify use of standard transmission error detection and correction methods such as checksums or message digest hashes. Verification of correct transmission shall occur at the voting system application level and ensure that the correct data is recorded on all relevant components consolidated within the polling place prior to the voter completing casting of his or her ballot. (V1: 6.5.2) 11. ***Requirement for Data Interception Prevention does not apply to the Unity 4.0 system, no communications occurs between components during Voting***. "Voting systems that use telecommunications as defined in Section 5 to communicate between system components and locations before the poll site is officially closed shall: (V1: 6.5.3)" – N/A • Implement an encryption standard currently documented and validated for use by an agency of the U.S. Federal Government; and • Provide a means to detect the presence of an intrusive process, such as an Intrusion Detection System. 12. Verify system for Protection Against External Threats: Voting systems that use public telecommunications networks shall implement protections against external threats to which commercial products used in the system may be susceptible. Verfiy if requirement is satisfied by confirmng the proper implementation of proven commercial security software. (V1: 6.5.4 & V1: 9.4.1.4) 13. Verify that Vendor documentation provides Identification of COTS Products that clearly identifies all COTS hardware and software products and communications services used in the development and/or operation of the voting system, including: • Operating systems; • Communications routers; • Modem drivers; and • Dial-up networking software. • Such documentation shall identify the name, vendor, and version used for each such component. 14. Verify the Use of Protective Software at the receiving-end of all communications 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; and • Provide data to the system audit log indicating the detection of a threat and the processing performed. • Validate the use of multiple forms of protective software as needed to provide capabilities for the full range of products used by the voting system.

Test Detail	Test Methodology
Test Case Name	**Telecommunications**
	15. Verify Vendor documentation to ensure conformance of Monitoring and Responding to External Threats to which their voting systems are vulnerable. This documentation shall provide a detailed description, including scheduling information, of the procedures the vendor will use to: (V1: 6.5.4.3) • Monitor threats, such as through the review of assessments, advisories, and alerts for COTS components • Evaluate the threats and, if any, proposed responses; • Develop responsive updates to the system and/or corrective procedures; • Submit the proposed response to the ITAs and appropriate states for approval, identifying the exact changes and whether or not they are temporary or permanent; • After implementation of the proposed response is approved by the state, assist clients, either directly or through detailed written procedures, how to update their systems and/or to implement the corrective procedures no later than one month before an election; and • Address threats emerging too late to correct the system at least one month before the election, including: 1. Providing prompt, emergency notification to the ITAs and the affected states and user jurisdictions; 2. Assisting client jurisdictions directly, or advising them through detailed written procedures, to disable the public telecommunications mode of the system; and 3. After the election, modifying the system to address the threat; submitting the modified system to an ITA and appropriate state certification authority for approval, and assisting client jurisdictions directly, or advising them through detailed written procedures, to update their systems and/or to implement the corrective procedures after approval. 16. ***Requirement for Voting Process Security does not apply to the Unity 4.0 system, Individual Ballot information is not transmitted between system components.*** Voting Process Security for Casting Individual Ballots over a Public Telecommunications Network (V1: 6.6.2) – N/A
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
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

Test Detail	Test Methodology
Test Case Name	**Telecommunications**
	• **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	**Accuracy**
Note	This test case is to be used in conjunction with the Election Core Definition
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.
A description of the voting system type and the operational environment	**EDM** - Election Data Manager **iVIM** – iVotronic Image Manager **HPM** - Hardware Programming Manager **DAM** - Data Acquisition Manager **ERM** - Election Reporting Manager **ESSIM** - ES&S Ballot Image Manager **VAT** - AutoMARK Voter Assist Terminal (A100, A200) **M100** - Model 100 Ballot Scanner **DS200** - intElect DS200 Ballot Scanner **iVotronic** - iVotronic DRE **M650** - Model 650 Optical Scan Central Count Counter **ABCR Scanner** – Automatic Bar Code Reader Refer to the following tables for complete descriptions: ➢ Matrix of Required Software/Firmware ➢ Matrix of Required Hardware

Calculation of Ballots to be processed

Terminal	Ballot Description		Batch Description		Requirement
					1549703
M100	Number of Contests	6			
	Number of Candidates	44			
	Number of Batches	NA	Number of Batches	1	19
	Number of Ballots	1	Number of Ballots (Total)	320	6080
	Number of Machines	4	Odd marked	40	760
			Even Marked	40	760
			Blank (unmarked)	10	190
			All-Fill marked	230	4370
	Number of Ballot Positions	264	Number of Ballot Positions	84480	1605120
DS200	Number of Contests	6			
	Number of Candidates	44			
	Number of Batches	NA	Number of Batches	1	19
	Number of Ballots	1	Number of Ballots (Total)	320	6080

Test Detail	Test Methodology					
Test Case Name	Accuracy					
		Number of Machines	3	Odd marked	40	760
				Even Marked	40	760
				Blank (unmarked)	10	190
				All-Fill marked	230	4370
		Number of Ballot Positions	264	Number of Ballot Positions	84480	1605120
	M650	Number of Contests	6			
		Number of Candidates	44			
		Number of Batches	NA	Number of Batches	1	19
		Number of Ballots	1	Number of Ballots (Total)	320	6080
		Number of Machines	2	Odd marked	40	760
				Even Marked	40	760
				Blank (unmarked)	10	190
				All-Fill marked	230	4370
		Number of Ballot Positions	264	Number of Ballot Positions	84480	1605120
	iVotronic	Number of Contests	6			
		Number of Candidates	44			
		Number of Batches	NA	Number of Batches	1	19
		Number of Ballots	1	Number of Ballots (Total)	320	6080
		Number of Machines	6	Odd marked	40	760
				Even Marked	40	760
				Blank (unmarked)	10	190
				All-Fill marked	230	4370
		Number of Ballot Positions	264	Number of Ballot Positions	84480	1605120
	VAT	Number of Contests	6			
		Number of Candidates	44			
		Number of Batches	NA	Number of Batches	1	74
		Number of Ballots	1	Number of Ballots	80	5920
		Number of Machines	2	Odd marked	0	0

<table>
<tr><th>Test Detail</th><th colspan="6">Test Methodology</th></tr>
<tr><th>Test Case Name</th><th colspan="6">Accuracy</th></tr>
<tr><td></td><td colspan="6"><table>
<tr><td></td><td></td><td></td><td>Even Marked</td><td>0</td><td>0</td></tr>
<tr><td></td><td></td><td></td><td>Blank (unmarked)</td><td>80</td><td>5920</td></tr>
<tr><td></td><td></td><td></td><td>All-Fill marked</td><td>0</td><td>0</td></tr>
<tr><td></td><td>Number of Ballot Positions</td><td>264</td><td>Number of Ballot Positions</td><td>21120</td><td>1562880</td></tr>
</table></td></tr>
<tr><td>Accuracy: Error Rate</td><td colspan="6">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)

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</td></tr>
</table>

8 Appendix B – EAC Interpretations

RFI	Applicable	Reason if not applicable, high level overview if applicable
07-01	Yes	Documentation will be validated to contain required text, as listed in the RFI
07-02	Yes	This RFI determination was applied during the Source Code Review process
07-03	Yes	Alternative language (Spanish) is being supported in this certification.
07-04	No	Specific to VVSG 2005
07-05	Yes	Applicable devices will be verified to conform to RFI
07-06	Yes	The capability to record and report undervotes is being supported in this certification
08-01	Yes	Will be applied to the hardware testing phase
08-02	Yes	Optical scan systems are subject to the backup power requirement
08-03	No	Test Plan submitted prior to effective date noted in the RFI.
08-04	Yes	Alternative language (Spanish) is being supported in this certification
08-05	Yes	A durability conformance letter will be requested from the vendor
08-06	Yes	Central count scanner is being supported in this certification
08-07	Yes	All devices will be verified to provide unambiguous warnings for election officials as well as proper recording in the device audit log
08-08	Yes	The ABCR is a part of this certification
08-09	No	Test Plan submitted/approved prior to effective date
08-10	No	Specific to VVSG 2005
NOC	**Applicable**	**Reason if not Applicable, high level overview if applicable**
07-001	Yes	Verify the application was accepted by the EAC
07-002	No	SysTest Labs does not participate in ES&S development efforts
07-003	Yes	Any state testing will be noted
07-004	No	Applicable to manufacturer not the VSTL
07-005	Yes	SysTest Labs will manage and oversee 3rd party testing, specifically in hardware testing, as described
08-001	Yes	Per this NOC, all ES&S hardware was subjected to ESD testing, see hardware reports in Certification Report
08-002	No	This NOC applies to vendor responsibilities post certification
08-003	Yes	All devices and applications will be verified to be compliant with this NOC

Approval Signatures

SysTest Labs:

Traci Mapps
VSTL Director of Operations
November 17, 2008

End of Certification Test Plan