Election Assistance Commission
Voting System Certification Testing

Certification Test Plan

Document Number 07-V-ESS-035-CTP-01, Rev 07
March 18, 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:

SysTest labs®

216 16th St.
Suite 700
Denver, CO 80202

NVLAP®
NVLAP LAB CODE 200733-0

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

Revision History

Date	Description of Revision	Author	Revision #
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

TABLE OF CONTENTS

LIST OF TABLES

1 INTRODUCTION

This Certification Test Plan outlines the approach SysTest Labs will implement to perform Election Assistance Commission (EAC) certification testing 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' National Voluntary Lab Accreditation Program (NVLAP) audited and approved Quality System Manual and associated SysTest Labs Procedures (SLP), include:

- Physical Configuration Audit (PCA)
  - Verification of software and hardware functional and physical configurations
  - Iterative documentation review and assessment
  - Iterative source code review

- Functional Configuration Audit (FCA)
  - 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

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, Figure 1 Overview of Unity 4.0 Election Support Process 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-inch Real-Time Audit Log printer • iVotronic DRE with a 9.5-inch Real-Time Audit Log printer • iVotronic DRE without a 4-inch Real-Time Audit Log printer • iVotronic DRE without a 9.5-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 • Model 650 central count scanners with green light optical sensor to read ovals on the left and right • Model 650 central count scanners with green and red light optical sensors to read ovals on the left

Figure 1 Overview of Unity 4.0 Election Support Process

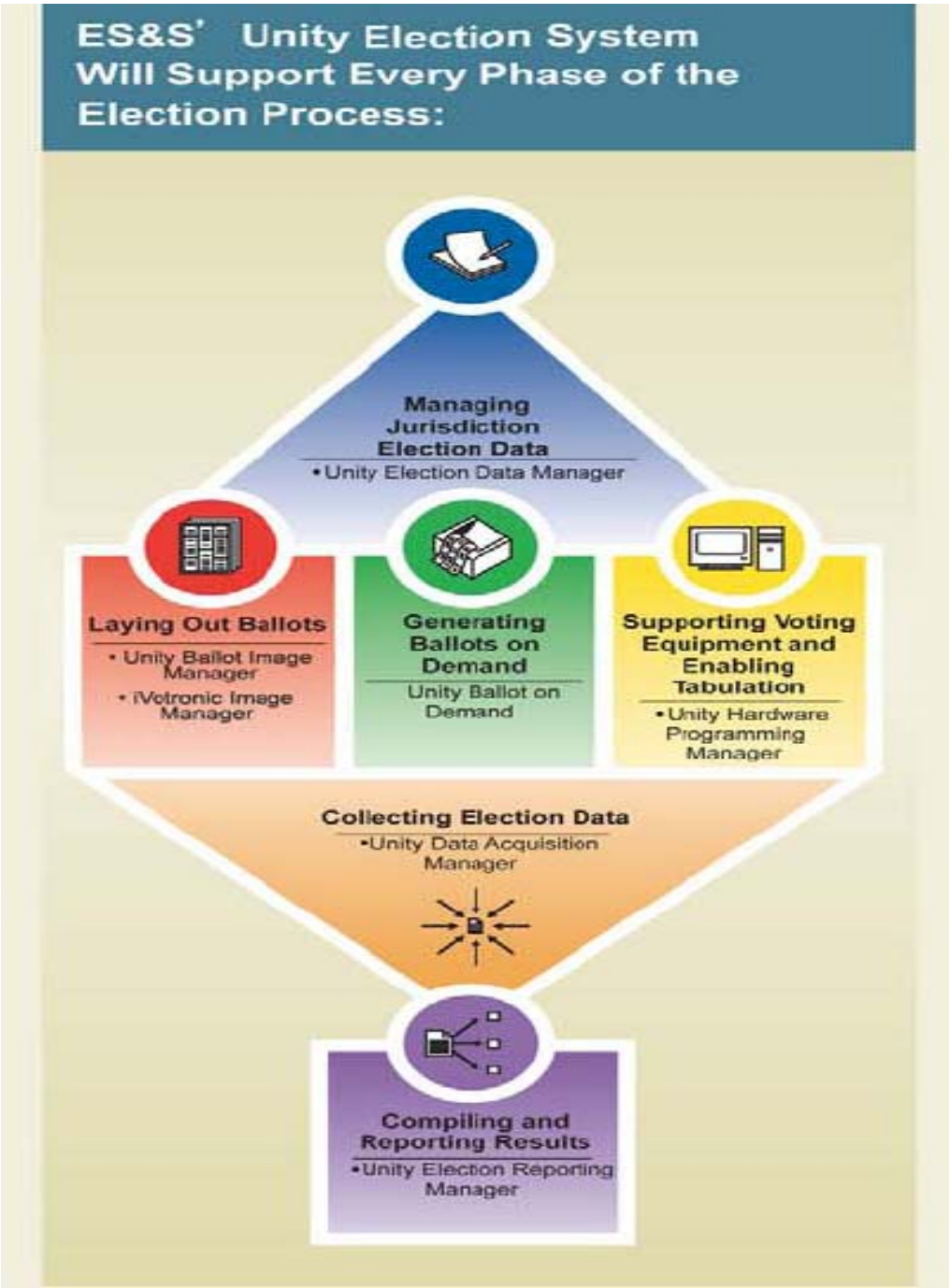
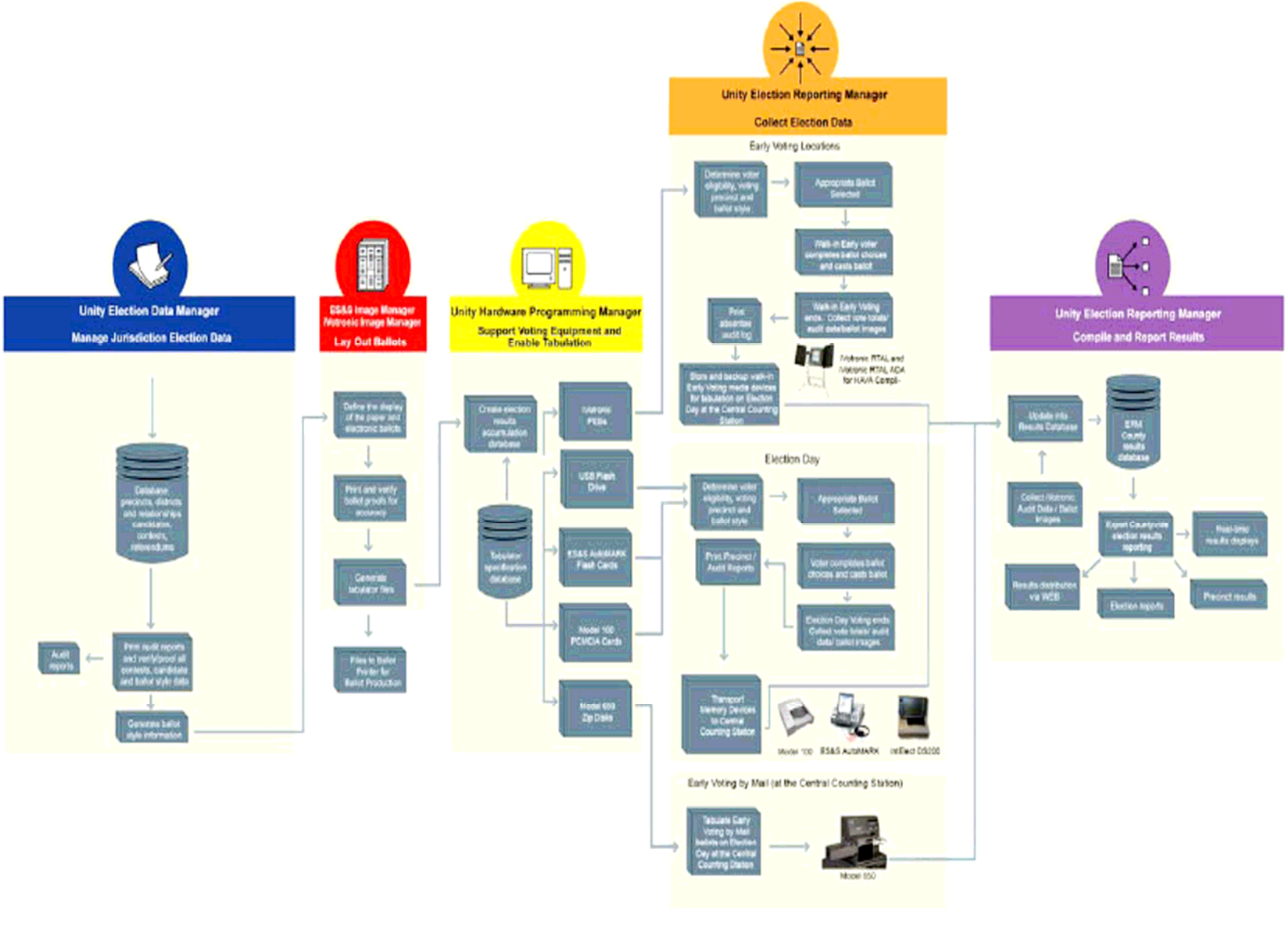


Figure 2 Overview of the Unity 4.0 Components



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

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

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

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

1.5 Terms, Abbreviations and Definitions

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

Term	Abbreviation	Definition
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.
Compact Flash Multi-Card Reader/Writer		The ES&S Compact Flash Multi-Card Reader/Writer reads and writes data to multiple flash cards. A multi-card reader/writer may also be called a gang burner. Use the multi-card reader before an election to transfer ballot data to compact flash cards for the iVotronic. Election coders prepare each election using Election Data Manager, and then prepare compact flash cards and PEBs (personalized electronic ballots) using Hardware Programming Manager. Use the multi-card reader to quickly create additional compact flash cards for iVotronic terminals. The other use for the Compact Flash Multi-Card Reader/Writer is to read in audit data from the iVotronic.
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 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.

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

2.1.1 Physical Configuration Audit

2.1.1.1 Document Review

SysTest Labs conducted a PCA review of 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. The VSTL approved source code is placed on the machine for the build and another hash and image is obtained. The next image and hash is taken after following the vendor's build procedures to compile the source code and produce the executable code. Additional hashes are taken of any installation CDs that are made during the build. 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.

Finally, 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.

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 Review of Ohio and Colorado Voting System Reviews

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

2.1.3 Hardware Environmental Testing Assessment

The acceptance and use of previous hardware environmental testing and certification 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 is planned to be 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
- Readiness Test
- Sampling of ES&S's Unity 4.0 test cases as described below in Section 4 under Sampling Methodology
- SysTest Labs' Gen01 test case
- SysTest Labs' Gen02 rotation and straight party test case
- SysTest Labs' Gen02 PA straight party with Cross party endorsement test case
- SysTest Labs' Gen03 Usability & Accessibility test case
- SysTest Labs' Pri01 Open Primary test case
- SysTest Labs' Pri01 Open Primary with Pick a Party/Party Preference test case
- SysTest Labs' Pri02 Closed Primary test case
- SysTest Labs' Security test case
- SysTest Labs' Telecommunications test case
- System Accuracy test case.

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

2.2.2.2 Review of Ohio and Colorado Voting System Reviews

SysTest Labs has not completed the FCA review of the Ohio and Colorado voting system Reviews. However, as a result of the FCA review of the Ohio and Colorado voting system Reviews, SysTest Labs will develop an addendum to the Certification Test Report that will include the following:

- A summary of the state findings for each system
- How SysTest Labs incorporated (if appropriate) these findings into the test campaign for the Unity 4.0 voting system
- The outcome of any additional testing deemed necessary

2.2.2 Hardware Environmental Analysis of Testing Results

Test reports from previous hardware testing 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.

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	3.1.0.0	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 Manager	ES&S	5.6.2.0	Hardware Programming Manager (HPM) is a complete election package that enables the user to import, format, 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

Application(s)	Manufacturer	Version	Description
			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	6.1.2.0	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	7.4.0.0	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	1.4	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, 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 Installer Intel® PRO Network Adapters and Drivers	Intel	2.01.1000	COTS software for the Server
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

COTS Application(s)	Manufacturer	Version	Description
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
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 Received**	ES&S	DS200	Hardware v. 1.2.0 DS200 Firmware 1.2.0.0 Power Management Firmware 1.0.0.0 Scanner Firmware 2.7.0.0.0	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 **1 Received**	ES&S	N/A	N/A	A storage receptacle to store scanned ballots. (Used with M100 and DS200).
Model 100 (Scanner) – **3 Received**	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) – **1 Received**	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 w/ diverter) **1 Received**	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) **1 Received**	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	An optical scan counter that is used to scan ballots at a central count location. The M650 prints

Item	Manufacturer	Model #	Version/Rev	Description
1 Received			Firmware v. 2.2.1.0	results reports and saves results to a zip disk.
Model 650 – Green – Left (Scanner) **1 Received**	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) – **2 Received**	ES&S	0105-096-90659	Hardware v. 1.1 Firmware v. 9.2.0.0	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) – **2 Received**	ES&S	0105-096-90659	Hardware v. 1.1 Firmware v. 9.2.0.0	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) **1 Received**	ES&S	9VDC 2770mA	Hardware v. 1.1 Firmware v. 9.2.0.0	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) – **2 Received**	ES&S	9VDC 2770mA	Hardware v. 1.1 Firmware v. 9.2.0.0	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) – **2 Received**	ES&S	15” 9VDC 2770mA	Hardware v. 1.1 Firmware v. 9.2.0.0	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) – **15 Received**	ES&S	0105-096-90659	Hardware v. 1.1 Firmware v. 9.2.0.0	A DRE (direct recording electronic) touch screen that displays ballots and records votes. This is 15 inches with no ADA buttons.
15 inch Supervisor iVotronic (RED) – **2 Received**	ES&S	9VDC 2770mA 0150-096-90659	Hardware v. 1.1 Firmware v. 9.2.0.0	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 **1 Received**	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 **1 Received**	Booth: Pivot, Printer: Xten	N/A	Hardware v. N/A Firmware v.	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

Item	Manufacturer	Model #	Version/Rev	Description
			V012	attached to a private voting booth.
ABCR (Automatic Bar Code Reader) – **2 Received**	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 – **15 Received**	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 – **8 Received**	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 Received**	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 **1 Received**	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 (standalone for iVotronic) **1 Received**	Seiko	DPU-3445	N/A	Standalone printer for the iVotronic.
BOD Printer **1 Received**	OkiData	9600		Printer used to print ballots.
Printer (M650 Red Left Printer) – **2 Received**	520 OkiData	GE5258 A	N/A	Printer for audit logs and reports for the M650.
Printer (M650 Green Right Printer) – **2 Received**	520 OkiData	GE5258 A	N/A	Printer for audit logs and reports for the M650.
Printer (M650	Epson Model #	P363A	N/A	Printer for audit logs and reports

Item	Manufacturer	Model #	Version/Rev	Description
Green Left Printer) – **2 Received**	LQ-590			for the M650.
LaserJet Printer **1 Received**	HP	2300N	N/A	Printer for reports created within Unity.
Router **2 Received**	Dlink	1 @ DSH-16, 1 with no identification	1 @ V. B2, 1 with no identification	Directs and controls the flow of data.
Modem **1 Received**	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) **2 Received (1 each)**	Equinox	N/A	N/A	4 and 8 port
Multi-Modem Adapters (Used in DAM PC) **2 Received (1 each)**	Digi	N/A	N/A	4 and 8 Port
Multi-Modem Adapters (Used in DAM PC) **2 Received (1 each)**	Perle	N/A	N/A	4 and 8 Port
Multi-Port Adapter (Used in DAM PC) **3 Received (1 each)**	SeaLevel	N/A	N/A	7801 & 7803 – 8 Port 7406 – 4 Port
USB PEB Reader/Writer **1 Received**	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 **1 Received**	Voyager	MS9544	N/A	A device that reads the barcode printout generated by the iVotronic RTAL printer.
Omni Drive **1 Received**	Omni	D707-94	Rev. C1 USB 1.1	A device used to read/write data to the PCMCIA card.
Omni Drive Professional USB2 **1 Received**	Omni	D707-94	Rev. A USB 2.0	A device used to read/write data to the PCMCIA card.
SanDisk Reader **1 Received**	SanDisk	SDDR-91	N/A	Used to read data off of a SanDisk.
SanDisk ImageMate CF	SanDisk	SDDR-92	N/A	Used to read data off of a SanDisk.

Item	Manufacturer	Model #	Version/Rev	Description
Reader **1 Received**				
Zip Disk **1 Received**	Iomega	Z250US BPCMBP	N/A	Used to store data.
Headphones **3 Received (3 for ES&S, 1 for AutoMARK VAT)**	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.
Multi Compact Flash Reader/Writer (gangburner) **1 Received**	ES&S	N/A	Hardware v. 1.2 iVotronic Compact Flash Get Audit Data Software v. 9.2.0.0 CF Duplicator Software v. 9.2.1.0	A device used to read/write multiple compact flash cards of the same election definition for the iVotronic.
External Volume Control Button **1 Received**	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 **1 Received**	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 **4 Received**	Belkin	N/A	N/A	Backup uninterrupted power source for the M650 and Multi Compact Flash Reader/Writer (gangburner).
Sip n Puff **1 Received**	Pivot	N/A		Device used on the iVotronic 6-key by physically disabled voters
iVotronic booth **3 Received (2 with RTAL space, 1 without RTAL space)**	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 **1 Received**	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® **1 Received**	Dell	N/A	Windows XP Professional, SP2	4 CPU 2.00GHz, 512MB of RAM (PC System 1) (Pre and Post Voting)
Dell PC	Dell	N/A	Windows XP,	4 CPU 2.80GHz, 2.79 GHz, 1.00

Item	Manufacturer	Model #	Version/Rev	Description
Pentium® **1 Received**			SP2	GB of RAM (PC System 2) Pre and Post Voting
Dell PC Pentium® **1 Received**	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 **1 Received**	Dell	N/A		Intel Pentium 4 CPU 1.80 GHz AT/AT compatible 523,763 KB RAM
Dell Laptop D610 Latitude **1 Received**	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 Programmer PC) **1 Received**	Dell	N/A	Windows XP Professional, SP2 Rev A00	Pentium 4 CPU 2.80GHz, 2.79 GHz, 512 MB of RAM (Pre & Post voting)
VAT **1 Received**	ES&S	Model # A100	Hardware v 1.0 Firmware v. 1.4	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 **1 Received**	ES&S	Model # A200	Hardware v 1.0, and 1.1 Firmware v. 1.4	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
USB 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	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 as Attachments to this document.

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 D1H.

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 Displaying Election Information ERM Election Results
b 5. Report Generation- Produce audit data	Verify in Functional Tests: System audit reports voting
Polling Place Functions	

Function	Test Methodology
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 other data processing systems	See b.3
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

Function	Test Methodology
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, firmware vers. 1.2.0.0
- 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. 9.2.0.0
- 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. 1.4

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.

For additional detail, please also refer to the Security Test Case in Appendix 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 8 - Matrix of System Level and Other Functional Testing

Other Functional Testing	Test Methodology
Volume Test	
System's response to processing more than the expected number of ballots/voters per precinct, to processing more than the expected number of precincts, or to any other similar conditions that tend to overload the system's capacity to process, store, and report data.	Accuracy Test Case (described previously in this section)
Stress Tests	
System's responses to transient overload conditions. Subject polling place devices to ballot processing at the high volume rates, evaluate software response to hardware-generated interrupts and wait states.	Hardware is tested to limits outside the range of 'normal' but within specifications for the units.
Usability Tests	
Responses to input, text syntax, error message content, and audit message input	All System-Level Test Cases
Accessibility Test	
Exercises system capabilities of voters with disability features	System-Level Test Case GEN 03
Security Test	
Exercises systems security provisions, unauthorized access, deletion or modification of data, audit trail data, and modification or elimination of security mechanisms.	Security Test case for each component (described previously in this section)
Telecommunications Test	
Exercises telecommunications, maintaining data integrity, protection against external threats, monitoring and responding to external threats, shared operating environment, incomplete election returns, and use of public communications networks.	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 9 - 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, 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 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.

Test Case No.	Test Case	Execution
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.**

4.4 EAC Interpretations

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

The Certification Test Plan and the execution of tests for the ES&S Unity 4.0 voting system identified in this plan do not include any EAC interpretations.

5 TEST DATA

5.1 Data Recording

The FEC Voting System Standards, Volume 2 Test Standards, will be used to measure certification-testing progress against the standards defined for 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 10 - Matrix of Testing Tasks

Certification Task	Prerequisite Task
Scope Definition	Ascertain previous certification Information for the voting system, if applicable
PCA – Review of Source Code and Document TDPs	Receipt of TDPs
FCA – Testing Requirements Determined	Submissions of TDPs by vendor (including QA and testing specifics)
EAC Certification Test Plan	Review of TDPs and vendor testing
FCA – Test Case Development	Documentation TDP review; mapping of test requirements to VSS and vendor testing (or identified risk areas where additional testing is needed)
PCA – System Configuration Audit	Equipment received at SysTest and documentation available
Trusted Build	Completion of PCA source code review
FCA Hardware Environmental Testing	Completion of FCA test case preparation and PCA system configuration audit
FCA Accuracy Testing	Completion of FCA test case preparation, PCA system configuration audit and environmental testing
FCA Functional Testing	Completion of FCA test case preparation, 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 can recover from a non-catastrophic failure of a device, or from any error or malfunction that is within the operator's ability to correct.

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

7 Appendix A – Test Cases

Test Detail	Test Methodology
Test Case Name	**GEN01**
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	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.
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 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)

Test Detail	Test Methodology
Test Case Name	**GEN01**
	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 **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 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

Test Detail	Test Methodology
Test Case Name	**GEN01**
	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 • Is visible to designated election officials (V1: 2.2.9) Additionally, verification is done to ensure that Ballot boxes and ballot transfer boxes, which serve as secure containers for the storage and transportation of voted ballots, adhere to standards. (V1:3.2.4.2.6) For each iteration that the election is run: • All supplies necessary for testing are retrieved. • Verification is performed on the System to ensure that the correct versions of software, firmware and hardware, election and ballot is installed and set up as defined in the user documentation • A supervisory level access 'user' and password' is created or available • The Readiness Check List is completed if applicable

Test Detail	Test Methodology
Test Case Name	**GEN01**
	• The date and tester(s) are documented Testers are informed that the test environment must remain static, if not, no changes shall occur without documentation in the test record and the authorization of the project manager.
Documentation: **Test Data & Test Results**	For each iteration that the election is run: • Capture all voting steps in order to maintain repeatability of the test • Record election, ballot, and vote data fields on the corresponding worksheet tabs • Save all worksheet tabs for all iterations of the test case • Record results of test run by entering 'Accept/Reject' on the Test Results Matrix • Provide comments when observing deviations, discrepancies or notable observations • Log discrepancies on the Discrepancy Report
Pre-vote: **Ballot Preparation procedures verifications**	Verification of Common standards includes the following and ensures that the system: • Enables the automatic formatting of ballots in accordance with the requirements for offices, candidates, and measures qualified to be placed on the ballot for each political subdivision and district • Collects and maintains data pertaining to offices and their associated labels and instructions, candidate names and their associated labels, and issues and measures and their associated text • Supports the maximum number of potentially active voting positions as indicated in vendor documentation • For Primary Elections, generates ballots that segregate the choices in partisan races by party affiliation • Generates ballots that contain identifying codes or marks uniquely associated with each new format • Ensures the vote response fields, selection buttons, or switches properly align with the specific candidate names and/or issues printed or displayed on the ballot (V1: 2.3.1.1.1) Verification of Paper-Based systems ensures that the system: • Enables voters to make selections by marking a mark in areas designated for this purpose • For marksense systems, ensures that the timing marks align properly with the vote response fields (V1: 2.3.1.1.2) Verification of Ballot Production common standards ensures that: • The electronic display or paper ballot is capable of rendering an image of the ballot in any of the languages required by The Voting Rights Act of 1965, as amended, and as supported by the vendor • The electronic display or paper ballot does not show any advertising or commercial logos unless specifically provided for in State law. Electronic

Test Detail	Test Methodology
Test Case Name	**GEN01**
	displays shall not provide connection to such material through a hyperlink • The ballot conforms to the vendor specifications for type of paper stock, weight, size, shape used to record votes, folding, bleed through, and ink for printing if paper ballots are used as part of the voting system (V1: 2.3.1.3, 2.3.1.3.1) For paper based recording, verification is performed to ensure the following: • A ballot can be accurately/securely defined and formatted (V1: 3.2.4.2) • A ballot can be accurately/securely programmed and installed into the appropriate media (V1:3.2.4.2.5) • The system Ignores, and extraneous perforations, smudges, and folds (V1:3.2.5.2.b) During the election definition and ballot preparation process, verification is performed to ensure that the system audits the preparation of the baseline ballot formats and modifications to them, a description of these modifications, and corresponding dates. The log is to include: • The allowable number of selections for an office or issue • The combinations of voting patterns permitted or required by the jurisdiction • The inclusion or exclusion of offices or issues as the result of multiple districting within the polling place • Any other characteristics that may be peculiar to the jurisdiction, the election, or the polling place's location • Manual data maintained by election personnel • Samples of all final ballot formats • Ballot preparation edit listings (V1: 4.4.1) Verification of Ballot Formatting ensures that the system supports: • Creation of newly defined elections • Rapid and error-free definition of elections and associated ballot layouts • Uniform allocation of space and fonts, ensuring no perception of a preferred contest/candidate • Simultaneous display of the maximum number of choices for a contest • Retention of previously defined formats for an election • Prevention of unauthorized modification of any ballot formats • Modifications by authorized personnel of a previously defined ballot format (V1: 2.3.1.2)
Pre-vote: **Preparation - Security**	System Preparation - Security: • System username/password authentication and other access controls are set up according to system documentation guidelines for all devices being tested. • Any/all unnecessary processes are disabled and/or required process control measures noted in the documentation are followed. • All COTS and vendor subsystems used for system security are configured and active as recommended by the system documentation. This includes all connection, port, virus, and data or authorized process restriction systems.

Test Detail	Test Methodology
Test Case Name	**GEN01**
	• Any other pre-election system security measures listed in the documentation are followed including setup of additional hardware or software not covered above. Please also see the Documentation section of the Security Test Case within Appendix A.
Readiness Testing and Poll Verification	Verification of Common Standards for Readiness Testing ensures that: • Voting machines or vote recording and data processing equipment, precinct and central count equipment are properly prepared for an election, and collect data that verifies equipment readiness • Status and data reports from each set of equipment can be obtained • The correct installation and interface of all system equipment • Hardware and software function correctly • Consolidated data reports at the polling place and higher jurisdictional levels can be generated • There is Segregation of test data from actual voting data, either procedurally or by hardware/software features When resident test software, external devices, and special purpose test software may be connected or installed in the voting device to simulate operator and voter functions provided the following standards are verified to ensure that: • These elements are capable of being tested separately, and shall be proven to be reliable verification tools prior to their use • These elements are incapable of altering or introducing any residual effect on the intended operation of the voting device during any succeeding test and operational phase (V1: 2.3.4, 2.3.4.1) Vendor documentation is reviewed, evaluated and used to create steps that ensure all voting systems and equipment function properly before and during an election. Verification of these steps provide a formal record of the following: (V1:2.3.5) • The election's identification data • The identification of all equipment units • The identification of the polling place • The identification of all ballot formats • The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain only zeros) • A list of all ballot fields that can be used to invoke special voting options • Other information needed to confirm the readiness of the equipment, and to accommodate administrative reporting requirements To prepare voting devices to accept voted ballots, all voting systems are verified to ensure that they provide the capability to test each device prior to opening. This verifies that each is operating correctly. The tests include: • Confirmation that there are no hardware or software failures • Confirm that the device is ready to be activated for accepting votes • Confirmation that the test data is separate from voting data without impact to the testing

Test Detail	Test Methodology
Test Case Name	**GEN01**
	Prior to Opening the polls, verification at the Central Location is performed to ensure that vote counting and vote consolidation equipment and software function properly. Any system used in a central count environment provides a printed record of the following: (V1:2.3.6) • The election's identification data • The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain all zeros) • Other information needed to ensure the readiness of the equipment and to accommodate administrative reporting requirements Verification is performed to ensure the following: • A list of all ballot fields is created (V1: 3.2.4.2.1) • The voting device is ready to accept votes (V1:3.2.4.3.1)
Voting: **Opening the Polls Verification**	Verification of the Readiness checklist is performed, ensuring that it is complete. Vendor documentation is reviewed, evaluated and used to create steps that ensure all voting systems and equipment perform voting functions properly. These steps are created, using the guidelines listed in VSS volume 1, section 2.4. Verification of these steps provide a formal record of the following: • Opening the polls • Casting a ballot Additionally, verification ensures that all DRE systems support: • Activating the ballot • Augmenting the election counter • Augmenting the life-cycle counter If necessary, any issues, failures, or unexpected results and their required corrective action(s) are identified and recorded here. (V1: 2.4) Verification of Opening Polls for Precinct Count Systems (paper based) ensures: • An internal test of diagnostic capability to verify that all of the polling place tests specified in section 2.3.5 have been successfully completed • Automatic disabling any device that has not been tested until it has been tested. (V1:2.4.1.1) • A means of verifying that ballot marking devices are properly prepared and ready for use • A voting booth or similar facility, in which the voter may mark the ballot in secrecy • Secure receptacles for holding voted ballots (V1: 2.4.1.2.1) • Activating the ballot counting device • Verifying the device has been correctly activated and is functioning properly • Identifying device failure and corrective action needed (V1: 2.4.1.2.2)

Test Detail	Test Methodology
Test Case Name	**GEN01**
	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 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

Test Detail	Test Methodology
Test Case Name	**GEN01**
	candidate or ballot measure response • Allows the voter to punch or mark the ballot to register a vote • Allows either the voter or the appropriate election official to place the voted ballot into the ballot counting device (for precinct count systems) or into a secure receptacle (for central count systems) • Protects the secrecy of the vote throughout the process. (V1: 2.4.3.2.1) • Provides feedback to the voter that identifies specific contests or ballot issues for which an overvote or undervote is detected • Allows the voter, at the voter's choice, to vote a new ballot or submit the ballot 'as is' without correction • Allows an authorized election official to turn off the capabilities defined above (V1: 2.4.3.2.2) Additionally, verification is performed to ensure that all DRE systems: • Prohibit the voter from accessing or viewing any information on the display screen that has not been authorized by election officials and preprogrammed into the voting system (i.e., no potential for display of external information or linking to other information sources) • Enable the voter to easily identify the selection button or switch, or the active area of the ballot display that is associated with each candidate or ballot measure response • Allow the voter to select his or her preferences on the ballot in any legal number and combination • Indicate that a selection has been made or canceled • Indicate to the voter when no selection, or an insufficient number of selections, has been made in a contest • Prevent the voter from overvoting • Notify the voter when the selection of candidates and measures is completed • Allow the voter, before the ballot is cast, to review his or her choices and, if the voter desires, to delete or change his or her choices before the ballot is cast • For electronic image displays, prompt the voter to confirm the voter's choices before casting his or her ballot, signifying to the voter that casting the ballot is irrevocable and directing the voter to confirm the voter's intention to cast the ballot • Notify the voter after the vote has been stored successfully that the ballot has been cast • Notify the voter that the ballot has not been cast successfully if it is not stored successfully, including storage of the ballot image, and provide clear instruction as to the steps the voter should take to cast his or her ballot should this event occur • Provide sufficient computational performance to provide responses back to each voter entry in no more than three seconds • Ensure that the votes stored accurately represent the actual votes cast; • Prevent modification of the voter's vote after the ballot is cast; • Provide a capability to retrieve ballot images in a form readable by humans (in accordance with the requirements of Section 2.2.2.2 and 2.2.4.2) • Increment the proper ballot position registers or counters

Test Detail	Test Methodology
Test Case Name	**GEN01**
	• Protect the secrecy of the vote throughout the voting process • Prohibit access to voted ballots until after the close of polls • Provide the ability for election officials to submit test ballots for use in verifying the end-to-end integrity of the system • Isolate test ballots such that they are accounted for accurately in vote counts and are not reflect in official vote counts for specific candidates or measures (V1: 2.4.3.3)
Voting: **Required functionality verifications**	Vendor documentation is reviewed, evaluated and used to create Vote Data or the test 'voters' for this test case. This Vote Data is created in matrix form and is used to ensure vote accuracy based on common standards listed in VSS volume 1, section 2.2.2.1. Each 'voter' in the Vote Data Matrix votes the ballot. A SysTest employee performs this manually. The different combinations of candidates selected by each voter in the Vote Data Matrix validates the system's ability to: • Record the election precincts/splits, contests, candidates, and issues exactly as defined by election officials • Record the appropriate options for ballot content, verifying the appropriate contests/issues are displayed as determined in election creation • Record the appropriate options for casting and recording votes across a range of voting options • Record each vote precisely as indicated by the voter and be able to produce an accurate report of all votes cast • Include control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) to demonstrate that the system has been designed for accuracy • Provide software that monitors the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected The process for casting a ballot is defined in detail in individual test case steps. These cases, steps, and verification criteria are created using the requirements stated in the VSS volume 1, section 2.4.3 and section 4.5. Additionally, the Vendor documentation is evaluated and used to enhance the testing procedures. The standards used for validation consist of the following sections: • Common Standards (V1:2.4.3.1) • Paper-Based Systems Standards (V1:2.4.3.2) • DRE Systems Standards (V1:2.4.3.3) • Vote Secrecy (DRE Systems) (V1:4.5) Backup files are made and hard copies printed for all DRE systems to record and retain redundant copies of the original ballot image (V1: 2.2.2.2, 2.2.4.2) System auditing and functional testing is performed in order to validate vote data, prescient counts, central counts, audit records and error logs. Verification is performed

Test Detail	Test Methodology
Test Case Name	**GEN01**
	on the error logs based on the standards listed in the VSS volume 1 section 2.2.5. The test ballots are design with formats and voting patterns sufficient to verify performance of the test election programs. Ballots are cast in a number sufficient to demonstrate proper processing, error handling, and generation of audit data as specified in Volume I, Sections 2 and 4. Test case steps are performed during the Functionality Testing in Parallel with Hardware Testing for Precinct Count Systems to verify voting functions defined in Vol. 1: 2.4 and 2.5 of voting equipment and precinct counting equipment. Verification ensures that: • Preparation of the election programs: o Verify resident firmware, if any o Prepare software (including firmware) to simulate all ballot format and logic options for which the system will be used o Verify program memory device content o Obtain and design test ballots with formats and voting patterns sufficient to verify performance of the test election programs • Procedures to program precinct ballot counters: o Install program and data memory devices, or verify presence if resident o Verify operational status of hardware • Procedures to simulate opening of the polls: o Perform procedures required to prepare hardware for election operations o Obtain a zero report or other evidence that data memory has been cleared o Verify audit record of pre-election operations o Perform procedures required to open the polling place and enable ballot counting • Procedures to simulate counting ballots cast test ballots in a number sufficient to demonstrate proper processing, error handling, and generation of audit data • Procedures to simulate closing of polls: o Perform hardware operations required to disable ballot counting and close polls o Obtain data reports and verify correctness o Obtain audit log and verify correctness (V2: 3.3, 3.3.1) Test case steps are performed during the Functionality Testing in Parallel with Hardware Testing for Central Count Systems to verify voting functions defined in Vol. 1: 2.4 and 2.5. Verification ensures that: • Procedures to prepare election programs: o Verify resident firmware, if any o Prepare software (including firmware) to simulate all ballot format and logic options for which the system will be used, and to enable 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

Test Detail	Test Methodology
Test Case Name	**GEN01**
	identifications sufficient to verify performance of the test election programs • Procedures to simulate counting ballots count test ballots in a number sufficient to demonstrate proper processing, error handling and generation of audit data as specified in Vol. 1, Section 2 and 4. • Procedures to simulate election reports: o Obtain reports at polling places or precinct level o Obtain consolidated reports o Provide query access, if this is a feature of the system o Verify correctness of all reports and queries Obtain audit log and verify correctness (V2: 3.3.2) Integrity measures ensure the physical stability and function of the vote recording and counting processes. Verification is performed to ensure that both Common Standards and DRE Systems Standards are followed. (V1:2.2.4) Common Standards are used to ensure system integrity by validating that the voting system: (2.2.4.1) • Protects, by a means compatible with these Standards, against a single point of failure that would prevent further voting at the polling place • Protects against the interruption of electronic power • Protects against generated or induced electromagnetic radiation • Protects against ambient temperature and humidity fluctuations • Protects against the failure of any data input or storage device • Protects against any attempt at improper data entry or retrieval • Records and report the date and time of normal and abnormal events • Maintains a permanent record of all original audit data that cannot be modified or overridden but may be augmented by designated authorized officials in order to adjust for errors or omissions (e.g. during the canvassing process.) • Detect and record every event, including the occurrence of an error condition that the system cannot overcome, and time-dependent or programmed events that occur without the intervention of the voter or a polling place operator • Include built-in measurement, self-test, and diagnostic software and hardware for detecting and reporting the system's status and degree of operability DRE Systems Standards are used to ensure system integrity by validating that the voting system: (V1:2.2.4.2) • Maintains a record of each ballot cast using a process and storage location that differs from the main vote detection, interpretation, processing, and reporting path • Provides a capability to retrieve ballot images in a form readable by humans. Audit records are prepared for all testing phases of election operations using devices designed to be controlled by the jurisdiction or its contractors. These records rely upon automated audit data acquisition and machine-generated reports, with manual input of some information. These records address the ballot preparation and election definition

Test Detail	Test Methodology
Test Case Name	**GEN01**
	phase, system readiness tests, and voting and ballot-counting operations. Individual test cases and steps contain instructions on how and when to generate and validate this information. (V1:2.2.5.2, 4.4) All voting systems are evaluated and verified to ensure that they meet the following requirements for time, sequence and preservation of Audit Records: • Except where noted, systems provide the capability to create and maintain a real-time audit record • All systems include a real-time clock as part of the system's hardware • All audit record entries include the time-and-date stamp • The audit record are active whenever the system is in an operating mode • The generation of audit record entries are not terminated or altered by program control, or by the intervention of any person • Once the system has been activated for any function, the system preserves the contents of the audit record during any interruption of power to the system until processing and data reporting have been completed • The system is capable of printing a copy of the audit record (V1:2.2.5.2.1, 3.2.7, 3.2.7.2) All voting systems are evaluated and verified to ensure that they meet the following requirements for Error Messages: • The system generates, stores, and reports to the user all error messages as they occur • All error messages requiring intervention by an operator or precinct official are displayed or printed unambiguously in easily understood language text, or by means of other suitable visual indicators • When the system uses numerical error codes for trained technician maintenance or repair, the text corresponding to the code is self-contained, or affixed inside the unit device • All error messages for which correction impacts vote recording or vote processing are written in a manner that is understandable to an election official who possesses training on system use and operation, but does not possess technical training on system servicing and repair • The message cue for all systems clearly state the action to be performed in the event that voter or operator response is required • System design ensures that erroneous responses will not lead to irreversible error • Nested error conditions are corrected in a controlled sequence such that system status shall be restored to the initial state existing before the first error occurred (V1:2.2.5.2.2) All voting systems are evaluated and verified to ensure that they meet the following requirements for Status Messages: • When the jurisdiction requires, some status and information messages are displayed and reported in real-time • Messages that do not require operator intervention may be stored in memory to be recovered after ballot processing has been completed • The system displays and reports critical status messages using unambiguous indicators or English language text • The system need not display non-critical status messages at the time of occurrence

Test Detail	Test Methodology
Test Case Name	**GEN01**
	• 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-based systems: (V1:3.2.5.1.2) • Outstack the ballot, or • Stop the ballot reader and display a message prompting the election official or designee to remove the ballot, or • Mark the ballot with an identifying mark to facilitate its later identification. Exception Handling (Precinct Count) refers to the handling of ballots for a precinct count system when they are unreadable or when some condition is detected requiring that the cards be segregated from normally processed ballots for human review. All paper based precinct count systems are validated to ensure that the following can be accomplished: (V1:3.2.5.1.3) • An unreadable or blank ballot - return the ballot and provide a message prompting the voter to examine the ballot • Ballot with a write-in vote - segregate the ballot or mark the ballot with an identifying mark to facilitate its later identification • A ballot with an overvote the system: o Provides a capability to identify an overvoted ballot o Returns the ballot o Provides an indication prompting the voter to examine the ballot; o Allows the voter to submit the ballot with the overvote o Provides a means for an authorized election official to deactivate this capability entirely and by contest • In response to a ballot with an undervote the system: o Provides a capability to identify an undervoted ballot o Returns the ballot o Provides an indication prompting the voter to examine the ballot o Allows the voter to submit the ballot with the undervote o Provides a means for an authorized election official to deactivate this capability Processing speed is verified for DRE voting systems to ensure that they:

Test Detail	Test Methodology
Test Case Name	**GEN01**
	• 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) Note: For Provisional/Challenged ballots, the vendor supports tabulation of these ballots at Central Count
Voting: Optional functionality verifications	The functionality listed above in "**Variables: Voting Variations"** is verified here.
Post-Vote: **Closing the Polls**	Vendor documentation is reviewed, evaluated and used to create steps that ensure that all voting systems and equipment perform voting functions properly for all Post-Voting Functions. These steps are created, using the guidelines listed in VSS volum1, section 2.5. Verification of these steps provide a formal record of the following: • All systems provide capabilities to accumulate and report results for the jurisdiction and to generate audit trails • Precinct count systems provide a means to close the polling place including generating appropriate reports • The standards for closing the polling place are specific to precinct count systems. The system provides the means for: (V1:2.5.1) o Preventing the further casting of ballots once the polling place has closed o Providing an internal test that verifies that the prescribed closing procedure has been followed, and that the device status is normal o Incorporating a visible indication of system status o Producing a diagnostic test record that verifies the sequence of events, and indicates that the extraction of voting data has been activated o Precluding the unauthorized reopening of the polls once the poll closing has been completed for that election • All systems provide a means to consolidate vote data from all polling places, and optionally from other sources such as absentee ballots, provisional ballots, and voted ballots requiring human review (e.g., write-in votes). (V1:2.5.2) • All systems are able to create reports summarizing the data on multiple levels. (V1:2.5.3) • *If applicable*, the voting systems offer the capability to make unofficial results available to external organizations such as the news media, political party officials, and others. Although this capability is not required, systems that make unofficial results available: (V1:2.5.4) o Provide only aggregated results, and not data from individual ballots o Provide no access path from unofficial electronic reports or files to the storage devices for official data o Clearly indicate on each report or file that the results it contains are

Test Detail	Test Methodology
Test Case Name	**GEN01**
	unofficial
Post-Vote: **Vote Count Verification**	After all voting listed in the Vote Data Matrix is performed, the election data is examined and all counts are validated on the individual voter level, the voting machine level, the precinct level and the central count level. This verification ensures that the system is correctly tabulating all data and is accurately recording cast ballots, including provisional. (V1:2.2.8.1, 2.3.6, 2.5, 3.2.3.1, 3.2.5.2,3.2.6.2.2, 3.2.4.3.3) This tabulation sometimes includes verification of the following: • Ensure undervotes are counted as cast votes • Separate accumulation of Undervotes and Paper Overvotes • Ensure Overvotes are counted on paper ballots and tally correctly
Post-Vote: **Security**	Post-Vote - Security: • System username/password authentication and other access controls are set up according to system documentation guidelines for all devices being tested. • Any/all unnecessary processes are disabled and/or required process control measures noted in the documentation are followed. • All COTS and vendor subsystems used for system security are configured and active as recommended by the system documentation. This includes all connection, port, virus, auditing capability, data or authorized process restriction systems. • Any other system security measures listed in the documentation are followed including setup of additional hardware or software not covered above. Please also see the Documentation section of the Security Test Case within Appendix A.
Post-Vote: **System Audit and Data Retention**	All applicable system reports are produced and verified at this point. The requirements listed in the VSS volume 1 are followed for verifying Data and Document Retention. These include the following: • Data and Document Retention (V1:4.3) • Audit Record Data (V1:4.4) Additionally, the guidelines listed in the VSS volume 1, section 3.2.8.2, are used to validate Data Report Generation.
Results are Observed	Review the outcome of the test(s) against the expected result(s): • **Accept**: expected results is observed • **Reject:** expected result is NOT observed • **Not Testable (NT)**: rejection of a previous test step prevents validation of this step or this was tested in another test case • **Not Applicable (NA):** not applicable to the current test scope or to the component under review • **Not Supported (NS)**: not supported in the current test scope

Test Detail	Test Methodology
Test Case Name	**GEN01**
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	**GEN02 Straight Party**
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	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.
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 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

Test Detail	Test Methodology
Test Case Name	**GEN02 Straight Party**
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 **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 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

Test Detail	Test Methodology
Test Case Name	**GEN02 Straight Party**
	• 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 bility 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 • Is visible to designated election officials (V1: 2.2.9) Additionally, verification is done to ensure that Ballot boxes and ballot transfer boxes, which serve as secure containers for the storage and transportation of voted ballots, adhere to standards. (V1:3.2.4.2.6) For each iteration that the election is run: • All supplies necessary for testing are retrieved. • Verification is performed on the System to ensure that the correct versions of software, firmware and hardware, election and ballot is installed and set up as defined in the user documentation • A supervisory level access 'user' and password' is created or available • The Readiness Check List is completed if applicable • The date and tester(s) are documented Testers are informed that the test environment must remain static, if not, no changes shall occur without documentation in the test record and the authorization of the project manager.
Documentation:	For each iteration that the election is run:

Test Detail	Test Methodology
Test Case Name	**GEN02 Straight Party**
Test Data & Test Results	• Capture all voting steps in order to maintain repeatability of the test • Record election, ballot, and vote data fields on the corresponding worksheet tabs • Save all worksheet tabs for all iterations of the test case • Record results of test run by entering 'Accept/Reject' on the Test Results Matrix • Provide comments when observing deviations, discrepancies or notable observations • Log discrepancies on the Discrepancy Report
Pre-vote: **Ballot Preparation procedures verifications**	Verification of Common standards includes the following and ensures that the system: • Enables the automatic formatting of ballots in accordance with the requirements for offices, candidates, and measures qualified to be placed on the ballot for each political subdivision and district • Collects and maintains data pertaining to offices and their associated labels and instructions, candidate names and their associated labels, and issues and measures and their associated text • Supports the maximum number of potentially active voting positions as indicated in vendor documentation • For Primary Elections, generates ballots that segregate the choices in partisan races by party affiliation • Generates ballots that contain identifying codes or marks uniquely associated with each new format • Ensures the vote response fields, selection buttons, or switches properly align with the specific candidate names and/or issues printed or displayed on the ballot (V1: 2.3.1.1.1) Verification of Paper-Based systems ensures that the system: • Enables voters to make selections by marking a mark in areas designated for this purpose • For marksense systems, ensures that the timing marks align properly with the vote response fields (V1: 2.3.1.1.2) Verification of Ballot Production common standards ensures that: • The electronic display or paper ballot is capable of rendering an image of the ballot in any of the languages required by The Voting Rights Act of 1965, as amended, and as supported by the vendor • The electronic display or paper ballot does not show any advertising or commercial logos unless specifically provided for in State law. Electronic displays shall not provide connection to such material through a hyperlink • The ballot conforms to the vendor specifications for type of paper stock, weight, size, shape used to record votes, folding, bleed through, and ink for printing if paper ballots are used as part of the voting system (V1: 2.3.1.3, 2.3.1.3.1) For paper based recording, verification is performed to ensure the following: • A ballot can be accurately/securely defined and formatted (V1: 3.2.4.2) • A ballot can be accurately/securely programmed and installed into the

Test Detail	Test Methodology
Test Case Name	**GEN02 Straight Party**
	appropriate media (V1: 3.2.4.2.5) 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: **Preparation - Security**	System Preparation - Security: • System username/password authentication and other access controls are set up according to system documentation guidelines for all devices being tested. • Any/all unnecessary processes are disabled and/or required process control measures noted in the documentation are followed. • All COTS and vendor subsystems used for system security are configured and active as recommended by the system documentation. This includes all connection, port, virus, and data or authorized process restriction systems. • Any other pre-election system security measures listed in the documentation are followed including setup of additional hardware or software not covered above. Please also see the Documentation section of the Security Test Case within Appendix A.

Test Detail	Test Methodology
Test Case Name	**GEN02 Straight Party**
Readiness Testing and Poll Verification	Verification of Common Standards for Readiness Testing ensures that: • Voting machines or vote recording and data processing equipment, precinct and central count equipment are properly prepared for an election, and collect data that verifies equipment readiness • Status and data reports from each set of equipment can be obtained • The correct installation and interface of all system equipment • Hardware and software function correctly • Consolidated data reports at the polling place and higher jurisdictional levels can be generated • There is Segregation of test data from actual voting data, either procedurally or by hardware/software features When resident test software, external devices, and special purpose test software may be connected or installed in the voting device to simulate operator and voter functions provided the following standards are verified to ensure that: • These elements are capable of being tested separately, and shall be proven to be reliable verification tools prior to their use • These elements are incapable of altering or introducing any residual effect on the intended operation of the voting device during any succeeding test and operational phase (V1: 2.3.4, 2.3.4.1) Vendor documentation is reviewed, evaluated and used to create steps that ensure all voting systems and equipment function properly before and during an election. Verification of these steps provide a formal record of the following: (V1:2.3.5) • The election's identification data • The identification of all equipment units • The identification of the polling place • The identification of all ballot formats • The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain only zeros) • A list of all ballot fields that can be used to invoke special voting options • Other information needed to confirm the readiness of the equipment, and to accommodate administrative reporting requirements To prepare voting devices to accept voted ballots, all voting systems are verified to ensure that they provide the capability to test each device prior to opening. This verifies that each is operating correctly. The tests include: • Confirmation that there are no hardware or software failures • Confirm that the device is ready to be activated for accepting votes • Confirmation that the test data is separate from voting data without impact to the testing Prior to Opening the polls, verification at the Central Location is performed to ensure that vote counting and vote consolidation equipment and software function properly. Any system used in a central count environment provides a printed record of the following: (V1:2.3.6)

Test Detail	Test Methodology
Test Case Name	**GEN02 Straight Party**
	• The election's identification data • The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain all zeros) • Other information needed to ensure the readiness of the equipment and to accommodate administrative reporting requirements Verification is performed to ensure the following: • A list of all ballot fields is created (V1: 3.2.4.2.1) • The voting device is ready to accept votes (V1:3.2.4.3.1)
Voting: **Opening the Polls Verification**	Verification of the Readiness checklist is performed, ensuring that it is complete. Vendor documentation is reviewed, evaluated and used to create steps that ensure all voting systems and equipment perform voting functions properly. These steps are created, using the guidelines listed in VSS volume 1, section 2.4. Verification of these steps provide a formal record of the following: • Opening the polls • Casting a ballot Additionally, verification ensures that all DRE systems support: • Activating the ballot • Augmenting the election counter • Augmenting the life-cycle counter If necessary, any issues, failures, or unexpected results and their required corrective action(s) are identified and recorded here. (V1: 2.4) Verification of Opening Polls for Precinct Count Systems (paper based) ensures: • An internal test of diagnostic capability to verify that all of the polling place tests specified in section 2.3.5 have been successfully completed • Automatic disabling any device that has not been tested until it has been tested. (V1: 2.4.1.1) • A means of verifying that ballot marking devices are properly prepared and ready for use • A voting booth or similar facility, in which the voter may mark the ballot in secrecy • Secure receptacles for holding voted ballots (V1: 2.4.1.2.1) • Activating the ballot counting device • Verifying the device has been correctly activated and is functioning properly • Identifying device failure and corrective action needed (V1: 2.4.1.2.2) Verification of Opening Polls for Precinct Count Systems (DRE) ensures that: • A security seal, password, or a data code recognition capability to prevent the inadvertent or unauthorized actuation of the poll-opening function • A means of enforcing the execution of steps in the proper sequence • A means of verifying the system as been activated correctly • A means of identifying system failure and any corrective action needed

Test Detail	Test Methodology
Test Case Name	**GEN02 Straight Party**
	(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 of a telecommunications connection within the polling place or between the polling place and any other location. (Vol. 1: 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); and • 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

Test Detail	Test Methodology
Test Case Name	**GEN02 Straight Party**
	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; and • Allows an authorized election official to turn off the capabilities defined above (V1: 2.4.3.2.2) Additionally, verification is performed to ensure that all DRE systems: • Prohibit the voter from accessing or viewing any information on the display screen that has not been authorized by election officials and preprogrammed into the voting system (i.e., no potential for display of external information or linking to other information sources) • Enable the voter to easily identify the selection button or switch, or the active area of the ballot display that is associated with each candidate or ballot measure response • Allow the voter to select his or her preferences on the ballot in any legal number and combination • Indicate that a selection has been made or canceled • Indicate to the voter when no selection, or an insufficient number of selections, has been made in a contest • Prevent the voter from overvoting • Notify the voter when the selection of candidates and measures is completed • Allow the voter, before the ballot is cast, to review his or her choices and, if the voter desires, to delete or change his or her choices before the ballot is cast • For electronic image displays, prompt the voter to confirm the voter's choices before casting his or her ballot, signifying to the voter that casting the ballot is irrevocable and directing the voter to confirm the voter's intention to cast the ballot • Notify the voter after the vote has been stored successfully that the ballot has been cast • Notify the voter that the ballot has not been cast successfully if it is not stored successfully, including storage of the ballot image, and provide clear instruction as to the steps the voter should take to cast his or her ballot should this event occur • Provide sufficient computational performance to provide responses back to each voter entry in no more than three seconds • Ensure that the votes stored accurately represent the actual votes cast; • Prevent modification of the voter's vote after the ballot is cast; • Provide a capability to retrieve ballot images in a form readable by humans (in accordance with the requirements of Section 2.2.2.2 and 2.2.4.2) • Increment the proper ballot position registers or counters • Protect the secrecy of the vote throughout the voting process • Prohibit access to voted ballots until after the close of polls • Provide the ability for election officials to submit test ballots for use in verifying the end-to-end integrity of the system • Isolate test ballots such that they are accounted for accurately in vote counts and are not reflect in official vote counts for specific candidates or measures (V1: 2.4.3.3)

Test Detail	Test Methodology
Test Case Name	**GEN02 Straight Party**
Voting: **Required functionality verifications**	Vendor documentation is reviewed, evaluated and used to create Vote Data or the test 'voters' for this test case. This Vote Data is created in matrix form and is used to ensure vote accuracy based on common standards listed in VSS volume 1, section 2.2.2.1. Each 'voter' in the Vote Data Matrix votes the ballot. A SysTest employee performs this manually. The different combinations of candidates selected by each voter in the Vote Data Matrix validates the system's ability to: • Record the election precincts/splits, contests, candidates, and issues exactly as defined by election officials • Record the appropriate options for ballot content, verifying the appropriate contests/issues are displayed as determined in election creation • Record the appropriate options for casting and recording votes across a range of voting options • Record each vote precisely as indicated by the voter and be able to produce an accurate report of all votes cast • Include control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) to demonstrate that the system has been designed for accuracy • Provide software that monitors the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected The process for casting a ballot is defined in detail in individual test case steps. These cases, steps, and verification criteria are created using the requirements stated in the VSS volume 1, section 2.4.3 and section 4.5. Additionally, the Vendor documentation is evaluated and used to enhance the testing procedures. The standards used for validation consist of the following sections: • Common Standards (V1:2.4.3.1) • Paper-Based Systems Standards (V1:2.4.3.2) • DRE Systems Standards (V1:2.4.3.3) • Vote Secrecy (DRE Systems) (V1:4.5) Backup files are made and hard copies printed for all DRE systems to record and retain redundant copies of the original ballot image (V1: 2.2.2.2, 2.2.4.2) System auditing and functional testing is performed in order to validate vote data, prescient counts, central counts, audit records and error logs. Verification is performed on the error logs based on the standards listed in the VSS volume 1 section 2.2.5. The test ballots are design with formats and voting patterns sufficient to verify performance of the test election programs. Ballots are cast in a number sufficient to demonstrate proper processing, error handling, and generation of audit data as specified in Volume I, Sections 2 and 4. Test case steps are performed during the Functionality Testing in Parallel with Hardware Testing for Precinct Count Systems to verify voting functions defined in Vol. 1: 2.4 and 2.5 of voting equipment and precinct counting equipment. Verification

Test Detail	Test Methodology
Test Case Name	**GEN02 Straight Party**
	ensures that: • Preparation of the election programs: o Verify resident firmware, if any o Prepare software (including firmware) to simulate all ballot format and logic options for which the system will be used o Verify program memory device content o Obtain and design test ballots with formats and voting patterns sufficient to verify performance of the test election programs • Procedures to program precinct ballot counters: o Install program and data memory devices, or verify presence if resident o Verify operational status of hardware • Procedures to simulate opening of the polls: o Perform procedures required to prepare hardware for election operations o Obtain a zero report or other evidence that data memory has been cleared o Verify audit record of pre-election operations o Perform procedures required to open the polling place and enable ballot counting • Procedures to simulate counting ballots cast test ballots in a number sufficient to demonstrate proper processing, error handling, and generation of audit data • Procedures to simulate closing of polls: o Perform hardware operations required to disable ballot counting and close polls o Obtain data reports and verify correctness o Obtain audit log and verify correctness (V2: 3.3, 3.3.1) Test case steps are performed during the Functionality Testing in Parallel with Hardware Testing for Central Count Systems to verify voting functions defined in Vol. 1: 2.4 and 2.5. Verification ensures that: • Procedures to prepare election programs: o Verify resident firmware, if any o Prepare software (including firmware) to simulate all ballot format and logic options for which the system will be used, and to enable 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

Test Detail	Test Methodology
Test Case Name	**GEN02 Straight Party**
	o Obtain consolidated reports o Provide query access, if this is a feature of the system o Verify correctness of all reports and queries Obtain audit log and verify correctness (V2: 3.3.2) Integrity measures ensure the physical stability and function of the vote recording and counting processes. Verification is performed to ensure that both Common Standards and DRE Systems Standards are followed. (V1:2.2.4) Common Standards are used to ensure system integrity by validating that the voting system: (2.2.4.1) • Protects, by a means compatible with these Standards, against a single point of failure that would prevent further voting at the polling place • Protects against the interruption of electronic power • Protects against generated or induced electromagnetic radiation • Protects against ambient temperature and humidity fluctuations • Protects against the failure of any data input or storage device • Protects against any attempt at improper data entry or retrieval • Records and report the date and time of normal and abnormal events • Maintains a permanent record of all original audit data that cannot be modified or overridden but may be augmented by designated authorized officials in order to adjust for errors or omissions (e.g. during the canvassing process.) • Detect and record every event, including the occurrence of an error condition that the system cannot overcome, and time-dependent or programmed events that occur without the intervention of the voter or a polling place operator • Include built-in measurement, self-test, and diagnostic software and hardware for detecting and reporting the system's status and degree of operability DRE Systems Standards are used to ensure system integrity by validating that the voting system: (V1:2.2.4.2) • Maintains a record of each ballot cast using a process and storage location that differs from the main vote detection, interpretation, processing, and reporting path • Provides a capability to retrieve ballot images in a form readable by humans. Audit records are prepared for all testing phases of election operations using devices designed to be controlled by the jurisdiction or its contractors. These records rely upon automated audit data acquisition and machine-generated reports, with manual input of some information. These records address the ballot preparation and election definition phase, system readiness tests, and voting and ballot-counting operations. Individual test cases and steps contain instructions on how and when to generate and validate this information. (V1:2.2.5.2, 4.4) All voting systems are evaluated and verified to ensure that they meet the following requirements for time, sequence and preservation of Audit Records: • Except where noted, systems provide the capability to create and maintain a real-time audit record • All systems include a real-time clock as part of the system's hardware • All audit record entries include the time-and-date stamp

Test Detail	Test Methodology
Test Case Name	**GEN02 Straight Party**
	• The audit record are active whenever the system is in an operating mode • The generation of audit record entries are not terminated or altered by program control, or by the intervention of any person • Once the system has been activated for any function, the system preserves the contents of the audit record during any interruption of power to the system until processing and data reporting have been completed • The system is capable of printing a copy of the audit record (V1:2.2.5.2.1, 3.2.7, 3.2.7.2) All voting systems are evaluated and verified to ensure that they meet the following requirements for Error Messages: • The system generates, stores, and reports to the user all error messages as they occur • All error messages requiring intervention by an operator or precinct official are displayed or printed unambiguously in easily understood language text, or by means of other suitable visual indicators • When the system uses numerical error codes for trained technician maintenance or repair, the text corresponding to the code is self-contained, or affixed inside the unit device • All error messages for which correction impacts vote recording or vote processing are written in a manner that is understandable to an election official who possesses training on system use and operation, but does not possess technical training on system servicing and repair • The message cue for all systems clearly state the action to be performed in the event that voter or operator response is required • System design ensures that erroneous responses will not lead to irreversible error • Nested error conditions are corrected in a controlled sequence such that system status shall be restored to the initial state existing before the first error occurred (V1:2.2.5.2.2) All voting systems are evaluated and verified to ensure that they meet the following requirements for Status Messages: • When the jurisdiction requires, some status and information messages are displayed and reported in real-time • Messages that do not require operator intervention may be stored in memory to be recovered after ballot processing has been completed • The system displays and reports critical status messages using unambiguous indicators or English language text • The system need not display non-critical status messages at the time of occurrence • 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)

Test Detail	Test Methodology
Test Case Name	**GEN02 Straight Party**
	Exception Handling (Central Count) refers to the handling of ballots for a central count system when they are unreadable or when some condition is detected requiring that the cards be segregated from normally processed ballots for human review. In response to an unreadable ballot or a write-in vote, verification is done to ensure that all central count paper-based systems: (V1:3.2.5.1.2) • Outstack the ballot, or • Stop the ballot reader and display a message prompting the election official or designee to remove the ballot, or • Mark the ballot with an identifying mark to facilitate its later identification. Exception Handling (Precinct Count) refers to the handling of ballots for a precinct count system when they are unreadable or when some condition is detected requiring that the cards be segregated from normally processed ballots for human review. All paper based precinct count systems are validated to ensure that the following can be accomplished: (V1:3.2.5.1.3) • An unreadable or blank ballot - return the ballot and provide a message prompting the voter to examine the ballot • Ballot with a write-in vote - segregate the ballot or mark the ballot with an identifying mark to facilitate its later identification • A ballot with an overvote the system: o Provides a capability to identify an overvoted ballot o Returns the ballot o Provides an indication prompting the voter to examine the ballot; o Allows the voter to submit the ballot with the overvote o Provides a means for an authorized election official to deactivate this capability entirely and by contest • In response to a ballot with an undervote the system: o Provides a capability to identify an undervoted ballot o Returns the ballot o Provides an indication prompting the voter to examine the ballot o Allows the voter to submit the ballot with the undervote o Provides a means for an authorized election official to deactivate this capability Processing speed is verified for DRE voting systems to ensure that they: • Operate at a speed sufficient to respond to any operator and voter input without perceptible delay (no more than three seconds) • 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) 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

Test Detail	Test Methodology
Test Case Name	**GEN02 Straight Party**
	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) 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.
Voting: Optional functionality verifications	The functionality listed above in "**Variables: Voting Variations"** is verified here.
Post-Vote: **Closing the Polls**	Vendor documentation is reviewed, evaluated and used to create steps that ensure that all voting systems and equipment perform voting functions properly for all Post-Voting Functions. These steps are created, using the guidelines listed in VSS volum1, section 2.5. Verification of these steps provide a formal record of the following: • All systems provide capabilities to accumulate and report results for the jurisdiction and to generate audit trails • Precinct count systems provide a means to close the polling place including generating appropriate reports • The standards for closing the polling place are specific to precinct count systems. The system provides the means for: (V1:2.5.1) o Preventing the further casting of ballots once the polling place has closed o Providing an internal test that verifies that the prescribed closing procedure has been followed, and that the device status is normal o Incorporating a visible indication of system status o Producing a diagnostic test record that verifies the sequence of events, and indicates that the extraction of voting data has been activated o Precluding the unauthorized reopening of the polls once the poll closing has been completed for that election • All systems provide a means to consolidate vote data from all polling places, and optionally from other sources such as absentee ballots, provisional ballots, and voted ballots requiring human review (e.g., write-in votes). (V1:**2.5.2)** • All systems are able to create reports summarizing the data on multiple levels. (V1:**2.5.3)** • *If applicable*, the voting systems offer the capability to make unofficial results available to external organizations such as the news media, political party officials, and others. Although this capability is not required, systems that make unofficial results available: (V1:2.5.4) o Provide only aggregated results, and not data from individual ballots o Provide no access path from unofficial electronic reports or files to the storage devices for official data

Test Detail	Test Methodology
Test Case Name	**GEN02 Straight Party**
	o Clearly indicate on each report or file that the results it contains are unofficial
Post-Vote: **Vote Count Verification**	After all voting listed in the Vote Data Matrix is performed, the election data is examined and all counts are validated on the individual voter level, the voting machine level, the precinct level and the central count level. This verification ensures that the system is correctly tabulating all data and is accurately recording cast ballots, including provisional. (V1:2.2.8.1, 2.3.6, 2.5, 3.2.3.1, 3.2.5.2,3.2.6.2.2, 3.2.4.3.3) This tabulation sometimes includes verification of the following: • Ensure undervotes are counted as cast votes • Separate accumulation of Undervotes and Paper Overvotes • Ensure Overvotes are counted on paper ballots and tally correctly
Post-Vote: **Security**	Post-Vote - Security: • System username/password authentication and other access controls are set up according to system documentation guidelines for all devices being tested. • Any/all unnecessary processes are disabled and/or required process control measures noted in the documentation are followed. • All COTS and vendor subsystems used for system security are configured and active as recommended by the system documentation. This includes all connection, port, virus, auditing capability, data or authorized process restriction systems. • Any other system security measures listed in the documentation are followed including setup of additional hardware or software not covered above. Please also see the Documentation section of the Security Test Case within Appendix A.
Post-Vote: **System Audit and Data Retention**	All applicable system reports are produced and verified at this point. The requirements listed in the VSS volume 1 are followed for verifying Data and Document Retention. These include the following: • Data and Document Retention (V1:4.3) • Audit Record Data (V1:4.4) Additionally, the guidelines listed in the VSS volume 1, section 3.2.8.2, are used to validate Data Report Generation.
Results are Observed	Review the outcome of the test(s) against the expected result(s): • **Accept**: expected results is observed • **Reject:** expected result is NOT observed • **Not Testable (NT)**: rejection of a previous test step prevents validation of this step or this was tested in another test case • **Not Applicable (NA):** not applicable to the current test scope or to the component under review • **Not Supported (NS)**: not supported in the current test scope

Test Detail	Test Methodology
Test Case Name	**GEN02 Straight Party**
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	**GEN02 PA Straight Party**
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	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.
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 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)

Test Detail	Test Methodology
Test Case Name	**GEN02 PA Straight Party**
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 **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 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

Test Detail	Test Methodology
Test Case Name	**GEN02 PA Straight Party**
	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 bility 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 • Is visible to designated election officials (V1: 2.2.9) Additionally, verification is done to ensure that Ballot boxes and ballot transfer boxes, which serve as secure containers for the storage and transportation of voted ballots, adhere to standards. (V1:3.2.4.2.6) For each iteration that the election is run: • All supplies necessary for testing are retrieved. • Verification is performed on the System to ensure that the correct versions of software, firmware and hardware, election and ballot is installed and set up as defined in the user documentation • A supervisory level access 'user' and password' is created or available • The Readiness Check List is completed if applicable • The date and tester(s) are documented Testers are informed that the test environment must remain static, if not, no changes shall occur without documentation in the test record and the authorization of the project manager.
Documentation:	For each iteration that the election is run:

Test Detail	Test Methodology
Test Case Name	**GEN02 PA Straight Party**
Test Data & Test Results	• Capture all voting steps in order to maintain repeatability of the test • Record election, ballot, and vote data fields on the corresponding worksheet tabs • Save all worksheet tabs for all iterations of the test case • Record results of test run by entering 'Accept/Reject' on the Test Results Matrix • Provide comments when observing deviations, discrepancies or notable observations • Log discrepancies on the Discrepancy Report
Pre-vote: **Ballot Preparation procedures verifications**	Verification of Common standards includes the following and ensures that the system: • Enables the automatic formatting of ballots in accordance with the requirements for offices, candidates, and measures qualified to be placed on the ballot for each political subdivision and district • Collects and maintains data pertaining to offices and their associated labels and instructions, candidate names and their associated labels, and issues and measures and their associated text • Supports the maximum number of potentially active voting positions as indicated in vendor documentation • For Primary Elections, generates ballots that segregate the choices in partisan races by party affiliation • Generates ballots that contain identifying codes or marks uniquely associated with each new format • Ensures the vote response fields, selection buttons, or switches properly align with the specific candidate names and/or issues printed or displayed on the ballot (V1: 2.3.1.1.1) Verification of Paper-Based systems ensures that the system: • Enables voters to make selections by marking a mark in areas designated for this purpose • For marksense systems, ensures that the timing marks align properly with the vote response fields (V1: 2.3.1.1.2) Verification of Ballot Production common standards ensures that: • The electronic display or paper ballot is capable of rendering an image of the ballot in any of the languages required by The Voting Rights Act of 1965, as amended, and as supported by the vendor • The electronic display or paper ballot does not show any advertising or commercial logos unless specifically provided for in State law. Electronic displays shall not provide connection to such material through a hyperlink • The ballot conforms to the vendor specifications for type of paper stock, weight, size, shape used to record votes, folding, bleed through, and ink for printing if paper ballots are used as part of the voting system (V1: 2.3.1.3, 2.3.1.3.1)

Test Detail	Test Methodology
Test Case Name	**GEN02 PA Straight Party**
	For paper based recording, verification is performed to ensure the following: • A ballot can be accurately/securely defined and formatted (V1: 3.2.4.2) • A ballot can be accurately/securely programmed and installed into the appropriate media (V1:3.2.4.2.5) • The system Ignores, and extraneous perforations, smudges, and folds (V1:3.2.5.2.b) During the election definition and ballot preparation process, verification is performed to ensure that the system audits the preparation of the baseline ballot formats and modifications to them, a description of these modifications, and corresponding dates. The log is to include: • The allowable number of selections for an office or issue • The combinations of voting patterns permitted or required by the jurisdiction • The inclusion or exclusion of offices or issues as the result of multiple districting within the polling place • Any other characteristics that may be peculiar to the jurisdiction, the election, or the polling place's location • Manual data maintained by election personnel • Samples of all final ballot formats • Ballot preparation edit listings (V1: 4.4.1) Verification of Ballot Formatting ensures that the system supports: • Creation of newly defined elections • Rapid and error-free definition of elections and associated ballot layouts • Uniform allocation of space and fonts, ensuring no perception of a preferred contest/candidate • Simultaneous display of the maximum number of choices for a contest • Retention of previously defined formats for an election • Prevention of unauthorized modification of any ballot formats • Modifications by authorized personnel of a previously defined ballot format (V1: 2.3.1.2)
Pre-vote: **Preparation - Security**	System Preparation - Security: • System username/password authentication and other access controls are set up according to system documentation guidelines for all devices being tested. • Any/all unnecessary processes are disabled and/or required process control measures noted in the documentation are followed. • All COTS and vendor subsystems used for system security are configured and active as recommended by the system documentation. This includes all connection, port, virus, and data or authorized process restriction systems. • Any other pre-election system security measures listed in the documentation are followed including setup of additional hardware or software not covered above. Please also see the Documentation section of the Security Test Case within Appendix A.

Test Detail	Test Methodology
Test Case Name	**GEN02 PA Straight Party**
Readiness Testing and Poll Verification	Verification of Common Standards for Readiness Testing ensures that: • Voting machines or vote recording and data processing equipment, precinct and central count equipment are properly prepared for an election, and collect data that verifies equipment readiness • Status and data reports from each set of equipment can be obtained • The correct installation and interface of all system equipment • Hardware and software function correctly • Consolidated data reports at the polling place and higher jurisdictional levels can be generated • There is Segregation of test data from actual voting data, either procedurally or by hardware/software features When resident test software, external devices, and special purpose test software may be connected or installed in the voting device to simulate operator and voter functions provided the following standards are verified to ensure that: • These elements are capable of being tested separately, and shall be proven to be reliable verification tools prior to their use • These elements are incapable of altering or introducing any residual effect on the intended operation of the voting device during any succeeding test and operational phase (V1: 2.3.4, 2.3.4.1) Vendor documentation is reviewed, evaluated and used to create steps that ensure all voting systems and equipment function properly before and during an election. Verification of these steps provide a formal record of the following: (V1:2.3.5) • The election's identification data • The identification of all equipment units • The identification of the polling place • The identification of all ballot formats • The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain only zeros) • A list of all ballot fields that can be used to invoke special voting options • Other information needed to confirm the readiness of the equipment, and to accommodate administrative reporting requirements To prepare voting devices to accept voted ballots, all voting systems are verified to ensure that they provide the capability to test each device prior to opening. This verifies that each is operating correctly. The tests include: • Confirmation that there are no hardware or software failures • Confirm that the device is ready to be activated for accepting votes • Confirmation that the test data is separate from voting data without impact to the testing Prior to Opening the polls, verification at the Central Location is performed to ensure that vote counting and vote consolidation equipment and software function properly. Any system used in a central count environment provides a printed record of the following**: (V1:2.3.6)**

Test Detail	Test Methodology
Test Case Name	**GEN02 PA Straight Party**
	• The election's identification data • The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain all zeros) • Other information needed to ensure the readiness of the equipment and to accommodate administrative reporting requirements Verification is performed to ensure the following: • A list of all ballot fields is created (V1: 3.2.4.2.1) • The voting device is ready to accept votes (V1:3.2.4.3.1)
Voting: **Opening the Polls Verification**	Verification of the Readiness checklist is performed, ensuring that it is complete. Vendor documentation is reviewed, evaluated and used to create steps that ensure all voting systems and equipment perform voting functions properly. These steps are created, using the guidelines listed in VSS volume 1, section 2.4. Verification of these steps provide a formal record of the following: • Opening the polls • Casting a ballot Additionally, verification ensures that all DRE systems support: • Activating the ballot • Augmenting the election counter • Augmenting the life-cycle counter If necessary, any issues, failures, or unexpected results and their required corrective action(s) are identified and recorded here. (V1: 2.4) Verification of Opening Polls for Precinct Count Systems (paper based) ensures: • An internal test of diagnostic capability to verify that all of the polling place tests specified in section 2.3.5 have been successfully completed • Automatic disabling any device that has not been tested until it has been tested. (V1: 2.4.1.1) • A means of verifying that ballot marking devices are properly prepared and ready for use • A voting booth or similar facility, in which the voter may mark the ballot in secrecy • Secure receptacles for holding voted ballots (V1: 2.4.1.2.1) • Activating the ballot counting device • Verifying the device has been correctly activated and is functioning properly • Identifying device failure and corrective action needed (V1: 2.4.1.2.2) Verification of Opening Polls for Precinct Count Systems (DRE) ensures that: • A security seal, password, or a data code recognition capability to prevent the inadvertent or unauthorized actuation of the poll-opening function • A means of enforcing the execution of steps in the proper sequence • A means of verifying the system as been activated correctly

Test Detail	Test Methodology
Test Case Name	**GEN02 PA Straight Party**
	• 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 of a telecommunications connection within the polling place or between the polling place and any other location. (Vol. 1: 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); and • Protects the secrecy of the vote throughout the process. **(V1: 2.4.3.2.1)**

Test Detail	Test Methodology
Test Case Name	**GEN02 PA Straight Party**
	• 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; and • Allows an authorized election official to turn off the capabilities defined above (V1: 2.4.3.2.2) Additionally, verification is performed to ensure that all DRE systems: • Prohibit the voter from accessing or viewing any information on the display screen that has not been authorized by election officials and preprogrammed into the voting system (i.e., no potential for display of external information or linking to other information sources) • Enable the voter to easily identify the selection button or switch, or the active area of the ballot display that is associated with each candidate or ballot measure response • Allow the voter to select his or her preferences on the ballot in any legal number and combination • Indicate that a selection has been made or canceled • Indicate to the voter when no selection, or an insufficient number of selections, has been made in a contest • Prevent the voter from overvoting • Notify the voter when the selection of candidates and measures is completed • Allow the voter, before the ballot is cast, to review his or her choices and, if the voter desires, to delete or change his or her choices before the ballot is cast • For electronic image displays, prompt the voter to confirm the voter's choices before casting his or her ballot, signifying to the voter that casting the ballot is irrevocable and directing the voter to confirm the voter's intention to cast the ballot • Notify the voter after the vote has been stored successfully that the ballot has been cast • Notify the voter that the ballot has not been cast successfully if it is not stored successfully, including storage of the ballot image, and provide clear instruction as to the steps the voter should take to cast his or her ballot should this event occur • Provide sufficient computational performance to provide responses back to each voter entry in no more than three seconds • Ensure that the votes stored accurately represent the actual votes cast; • Prevent modification of the voter's vote after the ballot is cast; • Provide a capability to retrieve ballot images in a form readable by humans (in accordance with the requirements of Section 2.2.2.2 and 2.2.4.2) • Increment the proper ballot position registers or counters • Protect the secrecy of the vote throughout the voting process • Prohibit access to voted ballots until after the close of polls • Provide the ability for election officials to submit test ballots for use in verifying the end-to-end integrity of the system • Isolate test ballots such that they are accounted for accurately in vote counts and are not reflect in official vote counts for specific candidates or measures

Test Detail	Test Methodology
Test Case Name	**GEN02 PA Straight Party**
	(V1: 2.4.3.3)
Voting: **Required functionality verifications**	Vendor documentation is reviewed, evaluated and used to create Vote Data or the test 'voters' for this test case. This Vote Data is created in matrix form and is used to ensure vote accuracy based on common standards listed in VSS volume 1, section 2.2.2.1. Each 'voter' in the Vote Data Matrix votes the ballot. A SysTest employee performs this manually. The different combinations of candidates selected by each voter in the Vote Data Matrix validates the system's ability to: • Record the election precincts/splits, contests, candidates, and issues exactly as defined by election officials • Record the appropriate options for ballot content, verifying the appropriate contests/issues are displayed as determined in election creation • Record the appropriate options for casting and recording votes across a range of voting options • Record each vote precisely as indicated by the voter and be able to produce an accurate report of all votes cast • Include control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) to demonstrate that the system has been designed for accuracy • Provide software that monitors the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected The process for casting a ballot is defined in detail in individual test case steps. These cases, steps, and verification criteria are created using the requirements stated in the VSS volume 1, section 2.4.3 and section 4.5. Additionally, the Vendor documentation is evaluated and used to enhance the testing procedures. The standards used for validation consist of the following sections: • Common Standards (V1:2.4.3.1) • Paper-Based Systems Standards (V1:2.4.3.2) • DRE Systems Standards (V1:2.4.3.3) • Vote Secrecy (DRE Systems) (V1:4.5) Backup files are made and hard copies printed for all DRE systems to record and retain redundant copies of the original ballot image (V1: 2.2.2.2, 2.2.4.2) System auditing and functional testing is performed in order to validate vote data, prescient counts, central counts, audit records and error logs. Verification is performed on the error logs based on the standards listed in the VSS volume 1 section 2.2.5. The test ballots are design with formats and voting patterns sufficient to verify performance of the test election programs. Ballots are cast in a number sufficient to demonstrate proper processing, error handling, and generation of audit data as specified in Volume I, Sections 2 and 4.

Test Detail	Test Methodology
Test Case Name	**GEN02 PA Straight Party**
	Test case steps are performed during the Functionality Testing in Parallel with Hardware Testing for Precinct Count Systems to verify voting functions defined in Vol. 1: 2.4 and 2.5 of voting equipment and precinct counting equipment. Verification ensures that: • Preparation of the election programs: o Verify resident firmware, if any o Prepare software (including firmware) to simulate all ballot format and logic options for which the system will be used o Verify program memory device content o Obtain and design test ballots with formats and voting patterns sufficient to verify performance of the test election programs • Procedures to program precinct ballot counters: o Install program and data memory devices, or verify presence if resident o Verify operational status of hardware • Procedures to simulate opening of the polls: o Perform procedures required to prepare hardware for election operations o Obtain a zero report or other evidence that data memory has been cleared o Verify audit record of pre-election operations o Perform procedures required to open the polling place and enable ballot counting • Procedures to simulate counting ballots cast test ballots in a number sufficient to demonstrate proper processing, error handling, and generation of audit data • Procedures to simulate closing of polls: o Perform hardware operations required to disable ballot counting and close polls o Obtain data reports and verify correctness o Obtain audit log and verify correctness (V2: 3.3, 3.3.1) Test case steps are performed during the Functionality Testing in Parallel with Hardware Testing for Central Count Systems to verify voting functions defined in Vol. 1: 2.4 and 2.5. Verification ensures that: • Procedures to prepare election programs: o Verify resident firmware, if any o Prepare software (including firmware) to simulate all ballot format and logic options for which the system will be used, and to enable 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

Test Detail	Test Methodology
Test Case Name	**GEN02 PA Straight Party**
	audit data as specified in Vol. 1, Section 2 and 4. • Procedures to simulate election reports: o Obtain reports at polling places or precinct level o Obtain consolidated reports o Provide query access, if this is a feature of the system o Verify correctness of all reports and queries Obtain audit log and verify correctness (V2: 3.3.2) Integrity measures ensure the physical stability and function of the vote recording and counting processes. Verification is performed to ensure that both Common Standards and DRE Systems Standards are followed. (V1:2.2.4) Common Standards are used to ensure system integrity by validating that the voting system: (2.2.4.1) • Protects, by a means compatible with these Standards, against a single point of failure that would prevent further voting at the polling place • Protects against the interruption of electronic power • Protects against generated or induced electromagnetic radiation • Protects against ambient temperature and humidity fluctuations • Protects against the failure of any data input or storage device • Protects against any attempt at improper data entry or retrieval • Records and report the date and time of normal and abnormal events • Maintains a permanent record of all original audit data that cannot be modified or overridden but may be augmented by designated authorized officials in order to adjust for errors or omissions (e.g. during the canvassing process.) • Detect and record every event, including the occurrence of an error condition that the system cannot overcome, and time-dependent or programmed events that occur without the intervention of the voter or a polling place operator • Include built-in measurement, self-test, and diagnostic software and hardware for detecting and reporting the system's status and degree of operability DRE Systems Standards are used to ensure system integrity by validating that the voting system: (V1:2.2.4.2) • Maintains a record of each ballot cast using a process and storage location that differs from the main vote detection, interpretation, processing, and reporting path • Provides a capability to retrieve ballot images in a form readable by humans. Audit records are prepared for all testing phases of election operations using devices designed to be controlled by the jurisdiction or its contractors. These records rely upon automated audit data acquisition and machine-generated reports, with manual input of some information. These records address the ballot preparation and election definition phase, system readiness tests, and voting and ballot-counting operations. Individual test cases and steps contain instructions on how and when to generate and validate this information. (V1:2.2.5.2, 4.4) All voting systems are evaluated and verified to ensure that they meet the following

Test Detail	Test Methodology
Test Case Name	**GEN02 PA Straight Party**
	requirements for time, sequence and preservation of Audit Records: • Except where noted, systems provide the capability to create and maintain a real-time audit record • All systems include a real-time clock as part of the system's hardware • All audit record entries include the time-and-date stamp • The audit record are active whenever the system is in an operating mode • The generation of audit record entries are not terminated or altered by program control, or by the intervention of any person • Once the system has been activated for any function, the system preserves the contents of the audit record during any interruption of power to the system until processing and data reporting have been completed • The system is capable of printing a copy of the audit record (V1:2.2.5.2.1, 3.2.7, 3.2.7.2) All voting systems are evaluated and verified to ensure that they meet the following requirements for Error Messages: • The system generates, stores, and reports to the user all error messages as they occur • All error messages requiring intervention by an operator or precinct official are displayed or printed unambiguously in easily understood language text, or by means of other suitable visual indicators • When the system uses numerical error codes for trained technician maintenance or repair, the text corresponding to the code is self-contained, or affixed inside the unit device • All error messages for which correction impacts vote recording or vote processing are written in a manner that is understandable to an election official who possesses training on system use and operation, but does not possess technical training on system servicing and repair • The message cue for all systems clearly state the action to be performed in the event that voter or operator response is required • System design ensures that erroneous responses will not lead to irreversible error • Nested error conditions are corrected in a controlled sequence such that system status shall be restored to the initial state existing before the first error occurred (V1:2.2.5.2.2) All voting systems are evaluated and verified to ensure that they meet the following requirements for Status Messages: • When the jurisdiction requires, some status and information messages are displayed and reported in real-time • Messages that do not require operator intervention may be stored in memory to be recovered after ballot processing has been completed • The system displays and reports critical status messages using unambiguous indicators or English language text • The system need not display non-critical status messages at the time of occurrence • 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

Test Detail	Test Methodology
Test Case Name	**GEN02 PA Straight Party**
	• 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-based systems: (V1:3.2.5.1.2) • Outstack the ballot, or • Stop the ballot reader and display a message prompting the election official or designee to remove the ballot, or • Mark the ballot with an identifying mark to facilitate its later identification. Exception Handling (Precinct Count) refers to the handling of ballots for a precinct count system when they are unreadable or when some condition is detected requiring that the cards be segregated from normally processed ballots for human review. All paper based precinct count systems are validated to ensure that the following can be accomplished: (V1:3.2.5.1.3) • An unreadable or blank ballot - return the ballot and provide a message prompting the voter to examine the ballot • Ballot with a write-in vote - segregate the ballot or mark the ballot with an identifying mark to facilitate its later identification • A ballot with an overvote the system: o Provides a capability to identify an overvoted ballot o Returns the ballot o Provides an indication prompting the voter to examine the ballot; o Allows the voter to submit the ballot with the overvote o Provides a means for an authorized election official to deactivate this capability entirely and by contest • In response to a ballot with an undervote the system: o Provides a capability to identify an undervoted ballot o Returns the ballot o Provides an indication prompting the voter to examine the ballot o Allows the voter to submit the ballot with the undervote o Provides a means for an authorized election official to deactivate this capability Processing speed is verified for DRE voting systems to ensure that they: • Operate at a speed sufficient to respond to any operator and voter input without perceptible delay (no more than three seconds) • 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)

Test Detail	Test Methodology
Test Case Name	**GEN02 PA Straight Party**
	Note: For Provisional/Challenged ballots, the vendor supports tabulation of these ballots at Central Count Note: Blank ballots (Not applicable on the iVotronic)
Voting: Optional functionality verifications	The functionality listed above in "**Variables: Voting Variations"** is verified here.
Post-Vote: **Closing the Polls**	Vendor documentation is reviewed, evaluated and used to create steps that ensure that all voting systems and equipment perform voting functions properly for all Post-Voting Functions. These steps are created, using the guidelines listed in VSS volum1, section 2.5. Verification of these steps provide a formal record of the following: • All systems provide capabilities to accumulate and report results for the jurisdiction and to generate audit trails • Precinct count systems provide a means to close the polling place including generating appropriate reports • The standards for closing the polling place are specific to precinct count systems. The system provides the means for: (V1:2.5.1) o Preventing the further casting of ballots once the polling place has closed o Providing an internal test that verifies that the prescribed closing procedure has been followed, and that the device status is normal o Incorporating a visible indication of system status o Producing a diagnostic test record that verifies the sequence of events, and indicates that the extraction of voting data has been activated o Precluding the unauthorized reopening of the polls once the poll closing has been completed for that election • All systems provide a means to consolidate vote data from all polling places, and optionally from other sources such as absentee ballots, provisional ballots, and voted ballots requiring human review (e.g., write-in votes). (V1:2.5.2) • All systems are able to create reports summarizing the data on multiple levels. (V1:2.5.3) • *If applicable*, the voting systems offer the capability to make unofficial results available to external organizations such as the news media, political party officials, and others. Although this capability is not required, systems that make unofficial results available: (V1:2.5.4) o Provide only aggregated results, and not data from individual ballots o Provide no access path from unofficial electronic reports or files to the storage devices for official data o Clearly indicate on each report or file that the results it contains are unofficial
Post-Vote:	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

Test Detail	Test Methodology
Test Case Name	**GEN02 PA Straight Party**
Vote Count Verification	level, the precinct level and the central count level. This verification ensures that the system is correctly tabulating all data and is accurately recording cast ballots, including provisional. (V1:2.2.8.1, 2.3.6, 2.5, 3.2.3.1, 3.2.5.2,3.2.6.2.2, 3.2.4.3.3) This tabulation sometimes includes verification of the following: • Ensure undervotes are counted as cast votes • Separate accumulation of Undervotes and Paper Overvotes • Ensure Overvotes are counted on paper ballots and tally correctly
Post-Vote: **Security**	Post-Vote - Security: • System username/password authentication and other access controls are set up according to system documentation guidelines for all devices being tested. • Any/all unnecessary processes are disabled and/or required process control measures noted in the documentation are followed. • All COTS and vendor subsystems used for system security are configured and active as recommended by the system documentation. This includes all connection, port, virus, auditing capability, data or authorized process restriction systems. • Any other system security measures listed in the documentation are followed including setup of additional hardware or software not covered above. Please also see the Documentation section of the Security Test Case within Appendix A.
Post-Vote: **System Audit and Data Retention**	All applicable system reports are produced and verified at this point. The requirements listed in the VSS volume 1 are followed for verifying Data and Document Retention. These include the following: • Data and Document Retention (V1:4.3) • Audit Record Data (V1:4.4) Additionally, the guidelines listed in the VSS volume 1, section 3.2.8.2, are used to validate Data Report Generation.
Results are Observed	Review the outcome of the test(s) against the expected result(s): • **Accept**: expected results is observed • **Reject:** expected result is NOT observed • **Not Testable (NT)**: rejection of a previous test step prevents validation of this step or this was tested in another test case • **Not Applicable (NA):** not applicable to the current test scope or to the component under review • **Not Supported (NS)**: not supported in the current test scope

Test Detail	Test Methodology
Test Case Name	**GEN02 PA Straight Party**
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	**PRI01 Open Primary**
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	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.
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 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 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 bility to select from a range of voting options to conform to the laws of

Test Detail	Test Methodology
Test Case Name	**PRI01 Open Primary**
	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 • Is visible to designated election officials (V1: 2.2.9) Additionally, verification is done to ensure that Ballot boxes and ballot transfer boxes, which serve as secure containers for the storage and transportation of voted ballots, adhere to standards. (V1:3.2.4.2.6) For each iteration that the election is run: • All supplies necessary for testing are retrieved. • Verification is performed on the System to ensure that the correct versions of software, firmware and hardware, election and ballot is installed and set up as defined in the user documentation • A supervisory level access 'user' and password' is created or available • The Readiness Check List is completed if applicable • The date and tester(s) are documented Testers are informed that the test environment must remain static, if not, no changes shall occur without documentation in the test record and the authorization of the project manager.
Documentation: **Test Data & Test Results**	For each iteration that the election is run: • Capture all voting steps in order to maintain repeatability of the test • Record election, ballot, and vote data fields on the corresponding worksheet tabs • Save all worksheet tabs for all iterations of the test case • Record results of test run by entering 'Accept/Reject' on the Test Results Matrix • Provide comments when observing deviations, discrepancies or notable observations • Log discrepancies on the Discrepancy Report
Pre-vote: **Ballot Preparation**	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

Test Detail	Test Methodology
Test Case Name	**PRI01 Open Primary**
procedures verifications	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 purpose • For marksense systems, ensures that the timing marks align properly with the vote response fields (V1: 2.3.1.1.2) Verification of Ballot Production common standards ensures that: • The electronic display or paper ballot is capable of rendering an image of the ballot in any of the languages required by The Voting Rights Act of 1965, as amended, and as supported by the vendor • The electronic display or paper ballot does not show any advertising or commercial logos unless specifically provided for in State law. Electronic displays shall not provide connection to such material through a hyperlink • The ballot conforms to the vendor specifications for type of paper stock, weight, size, shape used to record votes, folding, bleed through, and ink for printing if paper ballots are used as part of the voting system (V1: 2.3.1.3, 2.3.1.3.1) For paper based recording, verification is performed to ensure the following: • A ballot can be accurately/securely defined and formatted (V1: 3.2.4.2) • A ballot can be accurately/securely programmed and installed into the appropriate media (V1:3.2.4.2.5) • The system Ignores, and extraneous perforations, smudges, and folds (V1:3.2.5.2.b) During the election definition and ballot preparation process, verification is performed to ensure that the system audits the preparation of the baseline ballot formats and modifications to them, a description of these modifications, and corresponding dates. The log is to include: • The allowable number of selections for an office or issue • The combinations of voting patterns permitted or required by the jurisdiction • The inclusion or exclusion of offices or issues as the result of multiple

Test Detail	Test Methodology
Test Case Name	**PRI01 Open Primary**
	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: **Preparation - Security**	System Preparation - Security: • System username/password authentication and other access controls are set up according to system documentation guidelines for all devices being tested. • Any/all unnecessary processes are disabled and/or required process control measures noted in the documentation are followed. • All COTS and vendor subsystems used for system security are configured and active as recommended by the system documentation. This includes all connection, port, virus, and data or authorized process restriction systems. • Any other pre-election system security measures listed in the documentation are followed including setup of additional hardware or software not covered above. Please also see the Documentation section of the Security Test Case within Appendix A.
Readiness Testing and Poll Verification	Verification of Common Standards for Readiness Testing ensures that: • Voting machines or vote recording and data processing equipment, precinct and central count equipment are properly prepared for an election, and collect data that verifies equipment readiness • Status and data reports from each set of equipment can be obtained • The correct installation and interface of all system equipment • Hardware and software function correctly • Consolidated data reports at the polling place and higher jurisdictional levels can be generated • There is Segregation of test data from actual voting data, either procedurally or by hardware/software features When resident test software, external devices, and special purpose test software may be connected or installed in the voting device to simulate operator and voter functions provided the following standards are verified to ensure that: • These elements are capable of being tested separately, and shall be proven to

Test Detail	Test Methodology
Test Case Name	**PRI01 Open Primary**
	be reliable verification tools prior to their use • These elements are incapable of altering or introducing any residual effect on the intended operation of the voting device during any succeeding test and operational phase (V1: 2.3.4, 2.3.4.1) Vendor documentation is reviewed, evaluated and used to create steps that ensure all voting systems and equipment function properly before and during an election. Verification of these steps provide a formal record of the following: (V1:2.3.5) • The election's identification data • The identification of all equipment units • The identification of the polling place • The identification of all ballot formats • The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain only zeros) • A list of all ballot fields that can be used to invoke special voting options • Other information needed to confirm the readiness of the equipment, and to accommodate administrative reporting requirements To prepare voting devices to accept voted ballots, all voting systems are verified to ensure that they provide the capability to test each device prior to opening. This verifies that each is operating correctly. The tests include: • Confirmation that there are no hardware or software failures • Confirm that the device is ready to be activated for accepting votes • Confirmation that the test data is separate from voting data without impact to the testing Prior to Opening the polls, verification at the Central Location is performed to ensure that vote counting and vote consolidation equipment and software function properly. Any system used in a central count environment provides a printed record of the following: (V1:2.3.6) • The election's identification data • The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain all zeros) • Other information needed to ensure the readiness of the equipment and to accommodate administrative reporting requirements Verification is performed to ensure the following: • A list of all ballot fields is created (V1: 3.2.4.2.1) • The voting device is ready to accept votes (V1:3.2.4.3.1)
Voting: **Opening the Polls Verification**	Verification of the Readiness checklist is performed, ensuring that it is complete. Vendor documentation is reviewed, evaluated and used to create steps that ensure all voting systems and equipment perform voting functions properly. These steps are created, using the guidelines listed in VSS volume 1, section 2.4. Verification of these steps provide a formal record of the following:

Test Detail	Test Methodology
Test Case Name	**PRI01 Open Primary**
	• Opening the polls • Casting a ballot Additionally, verification ensures that all DRE systems support: • Activating the ballot • Augmenting the election counter • Augmenting the life-cycle counter If necessary, any issues, failures, or unexpected results and their required corrective action(s) are identified and recorded here. (V1: 2.4) Verification of Opening Polls for Precinct Count Systems (paper based) ensures: • An internal test of diagnostic capability to verify that all of the polling place tests specified in section 2.3.5 have been successfully completed • Automatic disabling any device that has not been tested until it has been tested. (V1: 2.4.1.1) • A means of verifying that ballot marking devices are properly prepared and ready for use • A voting booth or similar facility, in which the voter may mark the ballot in secrecy • Secure receptacles for holding voted ballots (V1: 2.4.1.2.1) • Activating the ballot counting device • Verifying the device has been correctly activated and is functioning properly • Identifying device failure and corrective action needed (V1: 2.4.1.2.2) Verification of Opening Polls for Precinct Count Systems (DRE) ensures that: • A security seal, password, or a data code recognition capability to prevent the inadvertent or unauthorized actuation of the poll-opening function • A means of enforcing the execution of steps in the proper sequence • A means of verifying the system as been activated correctly • A means of identifying system failure and any corrective action needed (V1: 2.4.1.3) Verification of Activating the Ballot (DRE) ensures that the system: • Enables election officials to control the content of the ballot presented to the voter, whether presented in printed form or electronic display, such that each voter is permitted to record votes only in contests in which that voter is authorized to vote • Allows each eligible voter to cast a ballot • Prevents a voter from casting more than one ballot in the same election • Activates the casting of a ballot in a general election • Enables the selection of the ballot that is appropriate to the party affiliation declared by the voter in a primary election • Activates all portions of the ballot upon which the voter is entitled to vote • Disables all portions of the ballot upon which the voter is not entitled to vote (V1: 2.4.2)

Test Detail	Test Methodology
Test Case Name	**PRI01 Open Primary**
	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 of a telecommunications connection within the polling place or between the polling place and any other location. (Vol. 1: 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); and • 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; and • Allows an authorized election official to turn off the capabilities defined above (V1: 2.4.3.2.2) Additionally, verification is performed to ensure that all DRE systems: • Prohibit the voter from accessing or viewing any information on the display screen that has not been authorized by election officials and preprogrammed into the voting system (i.e., no potential for display of external information or linking to other information sources) • Enable the voter to easily identify the selection button or switch, or the active area of the ballot display that is associated with each candidate or ballot measure response • Allow the voter to select his or her preferences on the ballot in any legal

Test Detail	Test Methodology
Test Case Name	**PRI01 Open Primary**
	number and combination • Indicate that a selection has been made or canceled • Indicate to the voter when no selection, or an insufficient number of selections, has been made in a contest • Prevent the voter from overvoting • Notify the voter when the selection of candidates and measures is completed • Allow the voter, before the ballot is cast, to review his or her choices and, if the voter desires, to delete or change his or her choices before the ballot is cast • For electronic image displays, prompt the voter to confirm the voter's choices before casting his or her ballot, signifying to the voter that casting the ballot is irrevocable and directing the voter to confirm the voter's intention to cast the ballot • Notify the voter after the vote has been stored successfully that the ballot has been cast • Notify the voter that the ballot has not been cast successfully if it is not stored successfully, including storage of the ballot image, and provide clear instruction as to the steps the voter should take to cast his or her ballot should this event occur • Provide sufficient computational performance to provide responses back to each voter entry in no more than three seconds • Ensure that the votes stored accurately represent the actual votes cast; • Prevent modification of the voter's vote after the ballot is cast; • Provide a capability to retrieve ballot images in a form readable by humans (in accordance with the requirements of Section 2.2.2.2 and 2.2.4.2) • Increment the proper ballot position registers or counters • Protect the secrecy of the vote throughout the voting process • Prohibit access to voted ballots until after the close of polls • Provide the ability for election officials to submit test ballots for use in verifying the end-to-end integrity of the system • Isolate test ballots such that they are accounted for accurately in vote counts and are not reflect in official vote counts for specific candidates or measures (V1: 2.4.3.3)
Voting: **Required functionality verifications**	Vendor documentation is reviewed, evaluated and used to create Vote Data or the test 'voters' for this test case. This Vote Data is created in matrix form and is used to ensure vote accuracy based on common standards listed in VSS volume 1, section 2.2.2.1. Each 'voter' in the Vote Data Matrix votes the ballot. A SysTest employee performs this manually. The different combinations of candidates selected by each voter in the Vote Data Matrix validates the system's ability to: • Record the election precincts/splits, contests, candidates, and issues exactly as defined by election officials • Record the appropriate options for ballot content, verifying the appropriate contests/issues are displayed as determined in election creation

Test Detail	Test Methodology
Test Case Name	**PRI01 Open Primary**
	• Record the appropriate options for casting and recording votes across a range of voting options • Record each vote precisely as indicated by the voter and be able to produce an accurate report of all votes cast • Include control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) to demonstrate that the system has been designed for accuracy • Provide software that monitors the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected The process for casting a ballot is defined in detail in individual test case steps. These cases, steps, and verification criteria are created using the requirements stated in the VSS volume 1, section 2.4.3 and section 4.5. Additionally, the Vendor documentation is evaluated and used to enhance the testing procedures. The standards used for validation consist of the following sections: • Common Standards (V1:2.4.3.1) • Paper-Based Systems Standards (V1:2.4.3.2) • DRE Systems Standards (V1:2.4.3.3) • Vote Secrecy (DRE Systems) (V1:4.5) Backup files are made and hard copies printed for all DRE systems to record and retain redundant copies of the original ballot image (V1: 2.2.2.2, 2.2.4.2) System auditing and functional testing is performed in order to validate vote data, prescient counts, central counts, audit records and error logs. Verification is performed on the error logs based on the standards listed in the VSS volume 1 section 2.2.5. The test ballots are design with formats and voting patterns sufficient to verify performance of the test election programs. Ballots are cast in a number sufficient to demonstrate proper processing, error handling, and generation of audit data as specified in Volume I, Sections 2 and 4. Test case steps are performed during the Functionality Testing in Parallel with Hardware Testing for Precinct Count Systems to verify voting functions defined in Vol. 1: 2.4 and 2.5 of voting equipment and precinct counting equipment. Verification ensures that: • Preparation of the election programs: o Verify resident firmware, if any o Prepare software (including firmware) to simulate all ballot format and logic options for which the system will be used o Verify program memory device content o Obtain and design test ballots with formats and voting patterns sufficient to verify performance of the test election programs • Procedures to program precinct ballot counters: o Install program and data memory devices, or verify presence if resident o Verify operational status of hardware • Procedures to simulate opening of the polls:

Test Detail	Test Methodology
Test Case Name	**PRI01 Open Primary**
	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) Common Standards are used to ensure system integrity by validating that the voting system: (2.2.4.1) • Protects, by a means compatible with these Standards, against a single point

Test Detail	Test Methodology
Test Case Name	**PRI01 Open Primary**
	of failure that would prevent further voting at the polling place • Protects against the interruption of electronic power • Protects against generated or induced electromagnetic radiation • Protects against ambient temperature and humidity fluctuations • Protects against the failure of any data input or storage device • Protects against any attempt at improper data entry or retrieval • Records and report the date and time of normal and abnormal events • Maintains a permanent record of all original audit data that cannot be modified or overridden but may be augmented by designated authorized officials in order to adjust for errors or omissions (e.g. during the canvassing process.) • Detect and record every event, including the occurrence of an error condition that the system cannot overcome, and time-dependent or programmed events that occur without the intervention of the voter or a polling place operator • Include built-in measurement, self-test, and diagnostic software and hardware for detecting and reporting the system's status and degree of operability DRE Systems Standards are used to ensure system integrity by validating that the voting system: (V1:2.2.4.2) • Maintains a record of each ballot cast using a process and storage location that differs from the main vote detection, interpretation, processing, and reporting path • Provides a capability to retrieve ballot images in a form readable by humans. Audit records are prepared for all testing phases of election operations using devices designed to be controlled by the jurisdiction or its contractors. These records rely upon automated audit data acquisition and machine-generated reports, with manual input of some information. These records address the ballot preparation and election definition phase, system readiness tests, and voting and ballot-counting operations. Individual test cases and steps contain instructions on how and when to generate and validate this information. (V1:2.2.5.2, 4.4) All voting systems are evaluated and verified to ensure that they meet the following requirements for time, sequence and preservation of Audit Records: • Except where noted, systems provide the capability to create and maintain a real-time audit record • All systems include a real-time clock as part of the system’s hardware • All audit record entries include the time-and-date stamp • The audit record are active whenever the system is in an operating mode • The generation of audit record entries are not terminated or altered by program control, or by the intervention of any person • Once the system has been activated for any function, the system preserves the contents of the audit record during any interruption of power to the system until processing and data reporting have been completed • The system is capable of printing a copy of the audit record (V1:2.2.5.2.1, 3.2.7, 3.2.7.2) All voting systems are evaluated and verified to ensure that they meet the following requirements for Error Messages: • The system generates, stores, and reports to the user all error messages as they occur • All error messages requiring intervention by an operator or precinct official are

Test Detail	Test Methodology
Test Case Name	**PRI01 Open Primary**
	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-based systems: (V1:3.2.5.1.2) • Outstack the ballot, or • Stop the ballot reader and display a message prompting the election official or designee to remove the ballot, or • Mark the ballot with an identifying mark to facilitate its later identification. Exception Handling (Precinct Count) refers to the handling of ballots for a precinct count system when they are unreadable or when some condition is detected requiring that the cards be segregated from normally processed ballots for human review. All

Test Detail	Test Methodology
Test Case Name	**PRI01 Open Primary**
	paper based precinct count systems are validated to ensure that the following can be accomplished: (V1:3.2.5.1.3) • An unreadable or blank ballot - return the ballot and provide a message prompting the voter to examine the ballot • Ballot with a write-in vote - segregate the ballot or mark the ballot with an identifying mark to facilitate its later identification • A ballot with an overvote the system: o Provides a capability to identify an overvoted ballot o Returns the ballot o Provides an indication prompting the voter to examine the ballot; o Allows the voter to submit the ballot with the overvote o Provides a means for an authorized election official to deactivate this capability entirely and by contest • In response to a ballot with an undervote the system: o Provides a capability to identify an undervoted ballot o Returns the ballot o Provides an indication prompting the voter to examine the ballot o Allows the voter to submit the ballot with the undervote o Provides a means for an authorized election official to deactivate this capability Processing speed is verified for DRE voting systems to ensure that they: • Operate at a speed sufficient to respond to any operator and voter input without perceptible delay (no more than three seconds) • 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) Note: For Provisional/Challenged ballots, the vendor supports tabulation of these ballots at Central Count Party affiliation is identified on the ballots *where appropriate*
Voting: Optional functionality verifications	The functionality listed above in "**Variables: Voting Variations"** is verified here.
Post-Vote: **Closing the Polls**	Vendor documentation is reviewed, evaluated and used to create steps that ensure that all voting systems and equipment perform voting functions properly for all Post-Voting Functions. These steps are created, using the guidelines listed in VSS volum1, section 2.5. Verification of these steps provide a formal record of the following: • All systems provide capabilities to accumulate and report results for the jurisdiction and to generate audit trails • Precinct count systems provide a means to close the polling place including

Test Detail	Test Methodology
Test Case Name	**PRI01 Open Primary**
	generating appropriate reports • The standards for closing the polling place are specific to precinct count systems. The system provides the means for: (V1:2.5.1) o Preventing the further casting of ballots once the polling place has closed o Providing an internal test that verifies that the prescribed closing procedure has been followed, and that the device status is normal o Incorporating a visible indication of system status o Producing a diagnostic test record that verifies the sequence of events, and indicates that the extraction of voting data has been activated o Precluding the unauthorized reopening of the polls once the poll closing has been completed for that election • All systems provide a means to consolidate vote data from all polling places, and optionally from other sources such as absentee ballots, provisional ballots, and voted ballots requiring human review (e.g., write-in votes). (V1:2.5.2) • All systems are able to create reports summarizing the data on multiple levels. (V1:2.5.3) • *If applicable*, the voting systems offer the capability to make unofficial results available to external organizations such as the news media, political party officials, and others. Although this capability is not required, systems that make unofficial results available: (V1:2.5.4) o Provide only aggregated results, and not data from individual ballots o Provide no access path from unofficial electronic reports or files to the storage devices for official data o Clearly indicate on each report or file that the results it contains are unofficial
Post-Vote: **Vote Count Verification**	After all voting listed in the Vote Data Matrix is performed, the election data is examined and all counts are validated on the individual voter level, the voting machine level, the precinct level and the central count level. This verification ensures that the system is correctly tabulating all data and is accurately recording cast ballots, including provisional. (V1:2.2.8.1, 2.3.6, 2.5, 3.2.3.1, 3.2.5.2,3.2.6.2.2, 3.2.4.3.3) This tabulation sometimes includes verification of the following: • Ensure undervotes are counted as cast votes • Separate accumulation of Undervotes and Paper Overvotes • Ensure Overvotes are counted on paper ballots and tally correctly

Test Detail	Test Methodology
Test Case Name	**PRI01 Open Primary**
Post-Vote: **Security**	Post-Vote - Security: • System username/password authentication and other access controls are set up according to system documentation guidelines for all devices being tested. • Any/all unnecessary processes are disabled and/or required process control measures noted in the documentation are followed. • All COTS and vendor subsystems used for system security are configured and active as recommended by the system documentation. This includes all connection, port, virus, auditing capability, data or authorized process restriction systems. • Any other system security measures listed in the documentation are followed including setup of additional hardware or software not covered above. Please also see the Documentation section of the Security Test Case within Appendix A.
Post-Vote: **System Audit and Data Retention**	All applicable system reports are produced and verified at this point. The requirements listed in the VSS volume 1 are followed for verifying Data and Document Retention. These include the following: • Data and Document Retention (V1:4.3) • Audit Record Data (V1:4.4) Additionally, the guidelines listed in the VSS volume 1, section 3.2.8.2, are used to validate Data Report Generation.
Results are Observed	Review the outcome of the test(s) against the expected result(s): • **Accept**: expected results is observed • **Reject:** expected result is NOT observed • **Not Testable (NT)**: rejection of a previous test step prevents validation of this step or this was tested in another test case • **Not Applicable (NA):** not applicable to the current test scope or to the component under review • **Not Supported (NS)**: not supported in the current test scope
Record Observations and all input/outputs for each election	All information used in processing the test case is captured. This includes: inputs, outputs, deviations and any other item that may impact the validation of the test case. Any failure of the test against the EAC guidelines is reported and implies failure of the system. Failures are reported as Defect Issues in the Discrepancy Report and are provided to the manufacturer. Before the final 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	**PRI01 Pick-a-Party/Party Preference**
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	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.
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 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 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 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

Test Detail	Test Methodology
Test Case Name	**PRI01 Pick-a-Party/Party Preference**
	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 • Is visible to designated election officials (V1: 2.2.9) Additionally, verification is done to ensure that Ballot boxes and ballot transfer boxes, which serve as secure containers for the storage and transportation of voted ballots, adhere to standards. (V1:3.2.4.2.6) For each iteration that the election is run: • All supplies necessary for testing are retrieved. • Verification is performed on the System to ensure that the correct versions of software, firmware and hardware, election and ballot is installed and set up as defined in the user documentation • A supervisory level access 'user' and password' is created or available • The Readiness Check List is completed if applicable • The date and tester(s) are documented Testers are informed that the test environment must remain static, if not, no changes shall occur without documentation in the test record and the authorization of the project manager.
Documentation: **Test Data & Test Results**	For each iteration that the election is run: • Capture all voting steps in order to maintain repeatability of the test • Record election, ballot, and vote data fields on the corresponding worksheet tabs • Save all worksheet tabs for all iterations of the test case • Record results of test run by entering 'Accept/Reject' on the Test Results Matrix • Provide comments when observing deviations, discrepancies or notable observations • Log discrepancies on the Discrepancy Report
Pre-vote: **Ballot Preparation**	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

Test Detail	Test Methodology
Test Case Name	**PRI01 Pick-a-Party/Party Preference**
procedures verifications	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 purpose • For marksense systems, ensures that the timing marks align properly with the vote response fields (V1: 2.3.1.1.2) Verification of Ballot Production common standards ensures that: • The electronic display or paper ballot is capable of rendering an image of the ballot in any of the languages required by The Voting Rights Act of 1965, as amended, and as supported by the vendor • The electronic display or paper ballot does not show any advertising or commercial logos unless specifically provided for in State law. Electronic displays shall not provide connection to such material through a hyperlink • The ballot conforms to the vendor specifications for type of paper stock, weight, size, shape used to record votes, folding, bleed through, and ink for printing if paper ballots are used as part of the voting system (V1: 2.3.1.3, 2.3.1.3.1) For paper based recording, verification is performed to ensure the following: • A ballot can be accurately/securely defined and formatted (V1: 3.2.4.2) • A ballot can be accurately/securely programmed and installed into the appropriate media (V1:3.2.4.2.5) • The system Ignores, and extraneous perforations, smudges, and folds (V1:3.2.5.2.b) During the election definition and ballot preparation process, verification is performed to ensure that the system audits the preparation of the baseline ballot formats and modifications to them, a description of these modifications, and corresponding dates. The log is to include: • The allowable number of selections for an office or issue • The combinations of voting patterns permitted or required by the jurisdiction

Test Detail	Test Methodology
Test Case Name	**PRI01 Pick-a-Party/Party Preference**
	• 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: **Preparation - Security**	System Preparation - Security: • System username/password authentication and other access controls are set up according to system documentation guidelines for all devices being tested. • Any/all unnecessary processes are disabled and/or required process control measures noted in the documentation are followed. • All COTS and vendor subsystems used for system security are configured and active as recommended by the system documentation. This includes all connection, port, virus, and data or authorized process restriction systems. • Any other pre-election system security measures listed in the documentation are followed including setup of additional hardware or software not covered above. Please also see the Documentation section of the Security Test Case within Appendix A.
Readiness Testing and Poll Verification	Verification of Common Standards for Readiness Testing ensures that: • Voting machines or vote recording and data processing equipment, precinct and central count equipment are properly prepared for an election, and collect data that verifies equipment readiness • Status and data reports from each set of equipment can be obtained • The correct installation and interface of all system equipment • Hardware and software function correctly • Consolidated data reports at the polling place and higher jurisdictional levels can be generated • There is Segregation of test data from actual voting data, either procedurally or by hardware/software features When resident test software, external devices, and special purpose test software may be connected or installed in the voting device to simulate operator and voter functions provided the following standards are verified to ensure that:

Test Detail	Test Methodology
Test Case Name	**PRI01 Pick-a-Party/Party Preference**
	• These elements are capable of being tested separately, and shall be proven to be reliable verification tools prior to their use • These elements are incapable of altering or introducing any residual effect on the intended operation of the voting device during any succeeding test and operational phase (V1: 2.3.4, 2.3.4.1) Vendor documentation is reviewed, evaluated and used to create steps that ensure all voting systems and equipment function properly before and during an election. Verification of these steps provide a formal record of the following: (V1:2.3.5) • The election's identification data • The identification of all equipment units • The identification of the polling place • The identification of all ballot formats • The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain only zeros) • A list of all ballot fields that can be used to invoke special voting options • Other information needed to confirm the readiness of the equipment, and to accommodate administrative reporting requirements To prepare voting devices to accept voted ballots, all voting systems are verified to ensure that they provide the capability to test each device prior to opening. This verifies that each is operating correctly. The tests include: • Confirmation that there are no hardware or software failures • Confirm that the device is ready to be activated for accepting votes • Confirmation that the test data is separate from voting data without impact to the testing Prior to Opening the polls, verification at the Central Location is performed to ensure that vote counting and vote consolidation equipment and software function properly. Any system used in a central count environment provides a printed record of the following: (V1:2.3.6) • The election's identification data • The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain all zeros) • Other information needed to ensure the readiness of the equipment and to accommodate administrative reporting requirements Verification is performed to ensure the following: • A list of all ballot fields is created (V1: 3.2.4.2.1) • The voting device is ready to accept votes (V1:3.2.4.3.1)
Voting: **Opening the Polls Verification**	Verification of the Readiness checklist is performed, ensuring that it is complete. Vendor documentation is reviewed, evaluated and used to create steps that ensure all voting systems and equipment perform voting functions properly. These steps are created, using the guidelines listed in VSS volume 1, section 2.4. Verification of these steps provide a formal record of the following:

Test Detail	Test Methodology
Test Case Name	**PRI01 Pick-a-Party/Party Preference**
	• Opening the polls • Casting a ballot Additionally, verification ensures that all DRE systems support: • Activating the ballot • Augmenting the election counter • Augmenting the life-cycle counter If necessary, any issues, failures, or unexpected results and their required corrective action(s) are identified and recorded here. (V1: 2.4) Verification of Opening Polls for Precinct Count Systems (paper based) ensures: • An internal test of diagnostic capability to verify that all of the polling place tests specified in section 2.3.5 have been successfully completed • Automatic disabling any device that has not been tested until it has been tested. (V1: 2.4.1.1) • A means of verifying that ballot marking devices are properly prepared and ready for use • A voting booth or similar facility, in which the voter may mark the ballot in secrecy • Secure receptacles for holding voted ballots (V1: 2.4.1.2.1) • Activating the ballot counting device • Verifying the device has been correctly activated and is functioning properly • Identifying device failure and corrective action needed (V1: 2.4.1.2.2) Verification of Opening Polls for Precinct Count Systems (DRE) ensures that: • A security seal, password, or a data code recognition capability to prevent the inadvertent or unauthorized actuation of the poll-opening function • A means of enforcing the execution of steps in the proper sequence • A means of verifying the system as been activated correctly • A means of identifying system failure and any corrective action needed (V1: 2.4.1.3) Verification of Activating the Ballot (DRE) ensures that the system: • Enables election officials to control the content of the ballot presented to the voter, whether presented in printed form or electronic display, such that each voter is permitted to record votes only in contests in which that voter is authorized to vote • Allows each eligible voter to cast a ballot • Prevents a voter from casting more than one ballot in the same election • Activates the casting of a ballot in a general election • Enables the selection of the ballot that is appropriate to the party affiliation declared by the voter in a primary election • Activates all portions of the ballot upon which the voter is entitled to vote • Disables all portions of the ballot upon which the voter is not entitled to vote (V1: 2.4.2)

Test Detail	Test Methodology
Test Case Name	**PRI01 Pick-a-Party/Party Preference**
	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 of a telecommunications connection within the polling place or between the polling place and any other location. (Vol. 1: 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); and • 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; and • Allows an authorized election official to turn off the capabilities defined above (V1: 2.4.3.2.2) Additionally, verification is performed to ensure that all DRE systems: • Prohibit the voter from accessing or viewing any information on the display screen that has not been authorized by election officials and preprogrammed into the voting system (i.e., no potential for display of external information or linking to other information sources) • Enable the voter to easily identify the selection button or switch, or the active area of the ballot display that is associated with each candidate or ballot measure response

Test Detail	Test Methodology
Test Case Name	**PRI01 Pick-a-Party/Party Preference**
	• Allow the voter to select his or her preferences on the ballot in any legal number and combination • Indicate that a selection has been made or canceled • Indicate to the voter when no selection, or an insufficient number of selections, has been made in a contest • Prevent the voter from overvoting • Notify the voter when the selection of candidates and measures is completed • Allow the voter, before the ballot is cast, to review his or her choices and, if the voter desires, to delete or change his or her choices before the ballot is cast • For electronic image displays, prompt the voter to confirm the voter's choices before casting his or her ballot, signifying to the voter that casting the ballot is irrevocable and directing the voter to confirm the voter's intention to cast the ballot • Notify the voter after the vote has been stored successfully that the ballot has been cast • Notify the voter that the ballot has not been cast successfully if it is not stored successfully, including storage of the ballot image, and provide clear instruction as to the steps the voter should take to cast his or her ballot should this event occur • Provide sufficient computational performance to provide responses back to each voter entry in no more than three seconds • Ensure that the votes stored accurately represent the actual votes cast; • Prevent modification of the voter's vote after the ballot is cast; • Provide a capability to retrieve ballot images in a form readable by humans (in accordance with the requirements of Section 2.2.2.2 and 2.2.4.2) • Increment the proper ballot position registers or counters • Protect the secrecy of the vote throughout the voting process • Prohibit access to voted ballots until after the close of polls • Provide the ability for election officials to submit test ballots for use in verifying the end-to-end integrity of the system • Isolate test ballots such that they are accounted for accurately in vote counts and are not reflect in official vote counts for specific candidates or measures (V1: 2.4.3.3)
Voting: **Required functionality verifications**	Vendor documentation is reviewed, evaluated and used to create Vote Data or the test 'voters' for this test case. This Vote Data is created in matrix form and is used to ensure vote accuracy based on common standards listed in VSS volume 1, section 2.2.2.1. Each 'voter' in the Vote Data Matrix votes the ballot. A SysTest employee performs this manually. The different combinations of candidates selected by each voter in the Vote Data Matrix validates the system's ability to: • Record the election precincts/splits, contests, candidates, and issues exactly as defined by election officials • Record the appropriate options for ballot content, verifying the appropriate

Test Detail	Test Methodology
Test Case Name	**PRI01 Pick-a-Party/Party Preference**
	contests/issues are displayed as determined in election creation • Record the appropriate options for casting and recording votes across a range of voting options • Record each vote precisely as indicated by the voter and be able to produce an accurate report of all votes cast • Include control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) to demonstrate that the system has been designed for accuracy • Provide software that monitors the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected The process for casting a ballot is defined in detail in individual test case steps. These cases, steps, and verification criteria are created using the requirements stated in the VSS volume 1, section 2.4.3 and section 4.5. Additionally, the Vendor documentation is evaluated and used to enhance the testing procedures. The standards used for validation consist of the following sections: • Common Standards (V1:2.4.3.1) • Paper-Based Systems Standards (V1:2.4.3.2) • DRE Systems Standards (V1:2.4.3.3) • Vote Secrecy (DRE Systems) (V1:4.5) Backup files are made and hard copies printed for all DRE systems to record and retain redundant copies of the original ballot image (V1: 2.2.2.2, 2.2.4.2) System auditing and functional testing is performed in order to validate vote data, prescient counts, central counts, audit records and error logs. Verification is performed on the error logs based on the standards listed in the VSS volume 1 section 2.2.5. The test ballots are design with formats and voting patterns sufficient to verify performance of the test election programs. Ballots are cast in a number sufficient to demonstrate proper processing, error handling, and generation of audit data as specified in Volume I, Sections 2 and 4. Test case steps are performed during the Functionality Testing in Parallel with Hardware Testing for Precinct Count Systems to verify voting functions defined in Vol. 1: 2.4 and 2.5 of voting equipment and precinct counting equipment. Verification ensures that: • Preparation of the election programs: o Verify resident firmware, if any o Prepare software (including firmware) to simulate all ballot format and logic options for which the system will be used o Verify program memory device content o Obtain and design test ballots with formats and voting patterns sufficient to verify performance of the test election programs • Procedures to program precinct ballot counters: o Install program and data memory devices, or verify presence if resident o Verify operational status of hardware

Test Detail	Test Methodology
Test Case Name	**PRI01 Pick-a-Party/Party Preference**
	• 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) Common Standards are used to ensure system integrity by validating that the voting system: (2.2.4.1)

Test Detail	Test Methodology
Test Case Name	**PRI01 Pick-a-Party/Party Preference**
	• Protects, by a means compatible with these Standards, against a single point of failure that would prevent further voting at the polling place • Protects against the interruption of electronic power • Protects against generated or induced electromagnetic radiation • Protects against ambient temperature and humidity fluctuations • Protects against the failure of any data input or storage device • Protects against any attempt at improper data entry or retrieval • Records and report the date and time of normal and abnormal events • Maintains a permanent record of all original audit data that cannot be modified or overridden but may be augmented by designated authorized officials in order to adjust for errors or omissions (e.g. during the canvassing process.) • Detect and record every event, including the occurrence of an error condition that the system cannot overcome, and time-dependent or programmed events that occur without the intervention of the voter or a polling place operator • Include built-in measurement, self-test, and diagnostic software and hardware for detecting and reporting the system's status and degree of operability DRE Systems Standards are used to ensure system integrity by validating that the voting system: (V1:2.2.4.2) • Maintains a record of each ballot cast using a process and storage location that differs from the main vote detection, interpretation, processing, and reporting path • Provides a capability to retrieve ballot images in a form readable by humans. Audit records are prepared for all testing phases of election operations using devices designed to be controlled by the jurisdiction or its contractors. These records rely upon automated audit data acquisition and machine-generated reports, with manual input of some information. These records address the ballot preparation and election definition phase, system readiness tests, and voting and ballot-counting operations. Individual test cases and steps contain instructions on how and when to generate and validate this information. (V1:2.2.5.2, 4.4) All voting systems are evaluated and verified to ensure that they meet the following requirements for time, sequence and preservation of Audit Records: • Except where noted, systems provide the capability to create and maintain a real-time audit record • All systems include a real-time clock as part of the system's hardware • All audit record entries include the time-and-date stamp • The audit record are active whenever the system is in an operating mode • The generation of audit record entries are not terminated or altered by program control, or by the intervention of any person • Once the system has been activated for any function, the system preserves the contents of the audit record during any interruption of power to the system until processing and data reporting have been completed • The system is capable of printing a copy of the audit record (V1:2.2.5.2.1, 3.2.7, 3.2.7.2) All voting systems are evaluated and verified to ensure that they meet the following requirements for Error Messages:

Test Detail	Test Methodology
Test Case Name	**PRI01 Pick-a-Party/Party Preference**
	• 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-based systems: (V1:3.2.5.1.2) • Outstack the ballot, or • Stop the ballot reader and display a message prompting the election official or designee to remove the ballot, or • Mark the ballot with an identifying mark to facilitate its later identification. Exception Handling (Precinct Count) refers to the handling of ballots for a precinct

Test Detail	Test Methodology
Test Case Name	**PRI01 Pick-a-Party/Party Preference**
	count system when they are unreadable or when some condition is detected requiring that the cards be segregated from normally processed ballots for human review. All paper based precinct count systems are validated to ensure that the following can be accomplished: (V1:3.2.5.1.3) • An unreadable or blank ballot - return the ballot and provide a message prompting the voter to examine the ballot • Ballot with a write-in vote - segregate the ballot or mark the ballot with an identifying mark to facilitate its later identification • A ballot with an overvote the system: o Provides a capability to identify an overvoted ballot o Returns the ballot o Provides an indication prompting the voter to examine the ballot; o Allows the voter to submit the ballot with the overvote o Provides a means for an authorized election official to deactivate this capability entirely and by contest • In response to a ballot with an undervote the system: o Provides a capability to identify an undervoted ballot o Returns the ballot o Provides an indication prompting the voter to examine the ballot o Allows the voter to submit the ballot with the undervote o Provides a means for an authorized election official to deactivate this capability Processing speed is verified for DRE voting systems to ensure that they: • Operate at a speed sufficient to respond to any operator and voter input without perceptible delay (no more than three seconds) • 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) Note: For Provisional/Challenged ballots, the vendor supports tabulation of these ballots at Central Count Party affiliation is identified on the ballots *where appropriate*
Voting: Optional functionality verifications	The functionality listed above in "**Variables: Voting Variations"** is verified here.
Post-Vote: **Closing the Polls**	Vendor documentation is reviewed, evaluated and used to create steps that ensure that all voting systems and equipment perform voting functions properly for all Post-Voting Functions. These steps are created, using the guidelines listed in VSS volum1, section 2.5. Verification of these steps provide a formal record of the following: • All systems provide capabilities to accumulate and report results for the jurisdiction and to generate audit trails

Test Detail	Test Methodology
Test Case Name	**PRI01 Pick-a-Party/Party Preference**
	• Precinct count systems provide a means to close the polling place including generating appropriate reports • The standards for closing the polling place are specific to precinct count systems. The system provides the means for: (V1:2.5.1) o Preventing the further casting of ballots once the polling place has closed o Providing an internal test that verifies that the prescribed closing procedure has been followed, and that the device status is normal o Incorporating a visible indication of system status o Producing a diagnostic test record that verifies the sequence of events, and indicates that the extraction of voting data has been activated o Precluding the unauthorized reopening of the polls once the poll closing has been completed for that election • All systems provide a means to consolidate vote data from all polling places, and optionally from other sources such as absentee ballots, provisional ballots, and voted ballots requiring human review (e.g., write-in votes). (V1:2.5.2) • All systems are able to create reports summarizing the data on multiple levels. (V1:2.5.3) • *If applicable*, the voting systems offer the capability to make unofficial results available to external organizations such as the news media, political party officials, and others. Although this capability is not required, systems that make unofficial results available: (V1:2.5.4) o Provide only aggregated results, and not data from individual ballots o Provide no access path from unofficial electronic reports or files to the storage devices for official data o Clearly indicate on each report or file that the results it contains are unofficial
Post-Vote: **Vote Count Verification**	After all voting listed in the Vote Data Matrix is performed, the election data is examined and all counts are validated on the individual voter level, the voting machine level, the precinct level and the central count level. This verification ensures that the system is correctly tabulating all data and is accurately recording cast ballots, including provisional. (V1:2.2.8.1, 2.3.6, 2.5, 3.2.3.1, 3.2.5.2,3.2.6.2.2, 3.2.4.3.3) This tabulation sometimes includes verification of the following: • Ensure undervotes are counted as cast votes • Separate accumulation of Undervotes and Paper Overvotes • Ensure Overvotes are counted on paper ballots and tally correctly

Test Detail	Test Methodology
Test Case Name	**PRI01 Pick-a-Party/Party Preference**
Post-Vote: **Security**	Post-Vote - Security: • System username/password authentication and other access controls are set up according to system documentation guidelines for all devices being tested. • Any/all unnecessary processes are disabled and/or required process control measures noted in the documentation are followed. • All COTS and vendor subsystems used for system security are configured and active as recommended by the system documentation. This includes all connection, port, virus, auditing capability, data or authorized process restriction systems. • Any other system security measures listed in the documentation are followed including setup of additional hardware or software not covered above. Please also see the Documentation section of the Security Test Case within Appendix A.
Post-Vote: **System Audit and Data Retention**	All applicable system reports are produced and verified at this point. The requirements listed in the VSS volume 1 are followed for verifying Data and Document Retention. These include the following: • Data and Document Retention (V1:4.3) • Audit Record Data (V1:4.4) Additionally, the guidelines listed in the VSS volume 1, section 3.2.8.2, are used to validate Data Report Generation.
Results are Observed	Review the outcome of the test(s) against the expected result(s): • **Accept**: expected results is observed • **Reject:** expected result is NOT observed • **Not Testable (NT)**: rejection of a previous test step prevents validation of this step or this was tested in another test case • **Not Applicable (NA):** not applicable to the current test scope or to the component under review • **Not Supported (NS)**: not supported in the current test scope
Record Observations and all input/outputs for each election	All information used in processing the test case is captured. This includes: inputs, outputs, deviations and any other item that may impact the validation of the test case. Any failure of the test against the EAC guidelines is reported and implies failure of the system. Failures are reported as Defect Issues in the Discrepancy Report and are provided to the manufacturer. Before the final Certification Test Report is issued, manufacturers are given the opportunity to correct all discrepancies. If the manufacturer submits corrections, retests are performed. Issues that do not impact the failure of the requirements but could be considered defects are logged as Informational Issues on the Discrepancy Report. It is the manufacturer's option to address these issues.

Test Detail	Test Methodology
Test Case Name	**PRI02 Closed Primary**
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	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.
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 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

Test Detail	Test Methodology
Test Case Name	**PRI02 Closed Primary**
	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 **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 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

Test Detail	Test Methodology
Test Case Name	**PRI02 Closed Primary**
	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 bility 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 • Is visible to designated election officials (V1: 2.2.9) Additionally, verification is done to ensure that Ballot boxes and ballot transfer boxes, which serve as secure containers for the storage and transportation of voted ballots, adhere to standards. (V1:3.2.4.2.6) For each iteration that the election is run: • All supplies necessary for testing are retrieved. • Verification is performed on the System to ensure that the correct versions of software, firmware and hardware, election and ballot is installed and set up as defined in the user documentation • A supervisory level access 'user' and password' is created or available • The Readiness Check List is completed if applicable • The date and tester(s) are documented Testers are informed that the test environment must remain static, if not, no changes shall occur without documentation in the test record and the authorization of the project manager.
Documentation: **Test Data & Test Results**	For each iteration that the election is run: • Capture all voting steps in order to maintain repeatability of the test • Record election, ballot, and vote data fields on the corresponding worksheet tabs • Save all worksheet tabs for all iterations of the test case • Record results of test run by entering 'Accept/Reject' on the Test Results Matrix • Provide comments when observing deviations, discrepancies or notable observations • Log discrepancies on the Discrepancy Report

Test Detail	Test Methodology
Test Case Name	**PRI02 Closed Primary**
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 purpose • For marksense systems, ensures that the timing marks align properly with the vote response fields (V1: 2.3.1.1.2) Verification of Ballot Production common standards ensures that: • The electronic display or paper ballot is capable of rendering an image of the ballot in any of the languages required by The Voting Rights Act of 1965, as amended, and as supported by the vendor • The electronic display or paper ballot does not show any advertising or commercial logos unless specifically provided for in State law. Electronic displays shall not provide connection to such material through a hyperlink • The ballot conforms to the vendor specifications for type of paper stock, weight, size, shape used to record votes, folding, bleed through, and ink for printing if paper ballots are used as part of the voting system (V1: 2.3.1.3, 2.3.1.3.1) For paper based recording, verification is performed to ensure the following: • A ballot can be accurately/securely defined and formatted (V1: 3.2.4.2) • A ballot can be accurately/securely programmed and installed into the appropriate media (V1:3.2.4.2.5) • The system Ignores, and extraneous perforations, smudges, and folds (V1:3.2.5.2.b) During the election definition and ballot preparation process, verification is performed to ensure that the system audits the preparation of the baseline ballot formats and modifications to them, a description of these modifications, and corresponding dates.

Test Detail	Test Methodology
Test Case Name	**PRI02 Closed Primary**
	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: **Preparation - Security**	System Preparation - Security: • System username/password authentication and other access controls are set up according to system documentation guidelines for all devices being tested. • Any/all unnecessary processes are disabled and/or required process control measures noted in the documentation are followed. • All COTS and vendor subsystems used for system security are configured and active as recommended by the system documentation. This includes all connection, port, virus, and data or authorized process restriction systems. • Any other pre-election system security measures listed in the documentation are followed including setup of additional hardware or software not covered above. Please also see the Documentation section of the Security Test Case within Appendix A.
Readiness Testing and Poll Verification	Verification of Common Standards for Readiness Testing ensures that: • Voting machines or vote recording and data processing equipment, precinct and central count equipment are properly prepared for an election, and collect data that verifies equipment readiness • Status and data reports from each set of equipment can be obtained • The correct installation and interface of all system equipment • Hardware and software function correctly • Consolidated data reports at the polling place and higher jurisdictional levels can be generated • There is Segregation of test data from actual voting data, either procedurally or by hardware/software features

Test Detail	Test Methodology
Test Case Name	**PRI02 Closed Primary**
	When resident test software, external devices, and special purpose test software may be connected or installed in the voting device to simulate operator and voter functions provided the following standards are verified to ensure that: • These elements are capable of being tested separately, and shall be proven to be reliable verification tools prior to their use • These elements are incapable of altering or introducing any residual effect on the intended operation of the voting device during any succeeding test and operational phase (V1: 2.3.4, 2.3.4.1) Vendor documentation is reviewed, evaluated and used to create steps that ensure all voting systems and equipment function properly before and during an election. Verification of these steps provide a formal record of the following: (V1:2.3.5) • The election's identification data • The identification of all equipment units • The identification of the polling place • The identification of all ballot formats • The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain only zeros) • A list of all ballot fields that can be used to invoke special voting options • Other information needed to confirm the readiness of the equipment, and to accommodate administrative reporting requirements To prepare voting devices to accept voted ballots, all voting systems are verified to ensure that they provide the capability to test each device prior to opening. This verifies that each is operating correctly. The tests include: • Confirmation that there are no hardware or software failures • Confirm that the device is ready to be activated for accepting votes • Confirmation that the test data is separate from voting data without impact to the testing Prior to Opening the polls, verification at the Central Location is performed to ensure that vote counting and vote consolidation equipment and software function properly. Any system used in a central count environment provides a printed record of the following: (V1:2.3.6) • The election's identification data • The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain all zeros) • Other information needed to ensure the readiness of the equipment and to accommodate administrative reporting requirements Verification is performed to ensure the following: • A list of all ballot fields is created (V1: 3.2.4.2.1) • The voting device is ready to accept votes (V1:3.2.4.3.1)

Test Detail	Test Methodology
Test Case Name	**PRI02 Closed Primary**
Voting: **Opening the Polls Verification**	Verification of the Readiness checklist is performed, ensuring that it is complete. Vendor documentation is reviewed, evaluated and used to create steps that ensure all voting systems and equipment perform voting functions properly. These steps are created, using the guidelines listed in VSS volume 1, section 2.4. Verification of these steps provide a formal record of the following: • Opening the polls • Casting a ballot Additionally, verification ensures that all DRE systems support: • Activating the ballot • Augmenting the election counter • Augmenting the life-cycle counter If necessary, any issues, failures, or unexpected results and their required corrective action(s) are identified and recorded here. (V1:2.4) Verification of Opening Polls for Precinct Count Systems (paper based) ensures: • An internal test of diagnostic capability to verify that all of the polling place tests specified in section 2.3.5 have been successfully completed • Automatic disabling any device that has not been tested until it has been tested. (V1: 2.4.1.1) • A means of verifying that ballot marking devices are properly prepared and ready for use • A voting booth or similar facility, in which the voter may mark the ballot in secrecy • Secure receptacles for holding voted ballots (V1: 2.4.1.2.1) • Activating the ballot counting device • Verifying the device has been correctly activated and is functioning properly • Identifying device failure and corrective action needed (V1: 2.4.1.2.2) Verification of Opening Polls for Precinct Count Systems (DRE) ensures that: • A security seal, password, or a data code recognition capability to prevent the inadvertent or unauthorized actuation of the poll-opening function • A means of enforcing the execution of steps in the proper sequence • A means of verifying the system as been activated correctly • A means of identifying system failure and any corrective action needed (V1: 2.4.1.3) Verification of Activating the Ballot (DRE) ensures that the system: • Enables election officials to control the content of the ballot presented to the voter, whether presented in printed form or electronic display, such that each voter is permitted to record votes only in contests in which that voter is authorized to vote • Allows each eligible voter to cast a ballot • Prevents a voter from casting more than one ballot in the same election

Test Detail	Test Methodology
Test Case Name	**PRI02 Closed Primary**
	• 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 of a telecommunications connection within the polling place or between the polling place and any other location. (Vol. 1: 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); and • 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; and • Allows an authorized election official to turn off the capabilities defined above (V1: 2.4.3.2.2) Additionally, verification is performed to ensure that all DRE systems: • Prohibit the voter from accessing or viewing any information on the display

Test Detail	Test Methodology
Test Case Name	**PRI02 Closed Primary**
	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; • Prevent modification of the voter's vote after the ballot is cast; • Provide a capability to retrieve ballot images in a form readable by humans (in accordance with the requirements of Section 2.2.2.2 and 2.2.4.2) • Increment the proper ballot position registers or counters • Protect the secrecy of the vote throughout the voting process • Prohibit access to voted ballots until after the close of polls • Provide the ability for election officials to submit test ballots for use in verifying the end-to-end integrity of the system • Isolate test ballots such that they are accounted for accurately in vote counts and are not reflect in official vote counts for specific candidates or measures (V1: 2.4.3.3)
Voting: **Required functionality verifications**	Vendor documentation is reviewed, evaluated and used to create Vote Data or the test 'voters' for this test case. This Vote Data is created in matrix form and is used to ensure vote accuracy based on common standards listed in VSS volume 1, section 2.2.2.1. Each 'voter' in the Vote Data Matrix votes the ballot. A SysTest employee performs this manually.

Test Detail	Test Methodology
Test Case Name	**PRI02 Closed Primary**
	The different combinations of candidates selected by each voter in the Vote Data Matrix validates the system's ability to: • Record the election precincts/splits, contests, candidates, and issues exactly as defined by election officials • Record the appropriate options for ballot content, verifying the appropriate contests/issues are displayed as determined in election creation • Record the appropriate options for casting and recording votes across a range of voting options • Record each vote precisely as indicated by the voter and be able to produce an accurate report of all votes cast • Include control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) to demonstrate that the system has been designed for accuracy • Provide software that monitors the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected The process for casting a ballot is defined in detail in individual test case steps. These cases, steps, and verification criteria are created using the requirements stated in the VSS volume 1, section 2.4.3 and section 4.5. Additionally, the Vendor documentation is evaluated and used to enhance the testing procedures. The standards used for validation consist of the following sections: • Common Standards (V1:2.4.3.1) • Paper-Based Systems Standards (V1:2.4.3.2) • DRE Systems Standards (V1:2.4.3.3) • Vote Secrecy (DRE Systems) (V1:4.5) Backup files are made and hard copies printed for all DRE systems to record and retain redundant copies of the original ballot image (V1: 2.2.2.2, 2.2.4.2) System auditing and functional testing is performed in order to validate vote data, prescient counts, central counts, audit records and error logs. Verification is performed on the error logs based on the standards listed in the VSS volume 1 section 2.2.5. The test ballots are design with formats and voting patterns sufficient to verify performance of the test election programs. Ballots are cast in a number sufficient to demonstrate proper processing, error handling, and generation of audit data as specified in Volume I, Sections 2 and 4. Test case steps are performed during the Functionality Testing in Parallel with Hardware Testing for Precinct Count Systems to verify voting functions defined in Vol. 1: 2.4 and 2.5 of voting equipment and precinct counting equipment. Verification ensures that: • Preparation of the election programs: o Verify resident firmware, if any o Prepare software (including firmware) to simulate all ballot format and logic options for which the system will be used

Test Detail	Test Methodology
Test Case Name	**PRI02 Closed Primary**
	o Verify program memory device content o Obtain and design test ballots with formats and voting patterns sufficient to verify performance of the test election programs • Procedures to program precinct ballot counters: o Install program and data memory devices, or verify presence if resident o Verify operational status of hardware • Procedures to simulate opening of the polls: o Perform procedures required to prepare hardware for election operations o Obtain a zero report or other evidence that data memory has been cleared o Verify audit record of pre-election operations o Perform procedures required to open the polling place and enable ballot counting • Procedures to simulate counting ballots cast test ballots in a number sufficient to demonstrate proper processing, error handling, and generation of audit data • Procedures to simulate closing of polls: o Perform hardware operations required to disable ballot counting and close polls o Obtain data reports and verify correctness o Obtain audit log and verify correctness (V2: 3.3, 3.3.1) Test case steps are performed during the Functionality Testing in Parallel with Hardware Testing for Central Count Systems to verify voting functions defined in Vol. 1: 2.4 and 2.5. Verification ensures that: • Procedures to prepare election programs: o Verify resident firmware, if any o Prepare software (including firmware) to simulate all ballot format and logic options for which the system will be used, and to enable 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)

Test Detail	Test Methodology
Test Case Name	**PRI02 Closed Primary**
	Integrity measures ensure the physical stability and function of the vote recording and counting processes. Verification is performed to ensure that both Common Standards and DRE Systems Standards are followed. (V1:2.2.4) Common Standards are used to ensure system integrity by validating that the voting system: (2.2.4.1) • Protects, by a means compatible with these Standards, against a single point of failure that would prevent further voting at the polling place • Protects against the interruption of electronic power • Protects against generated or induced electromagnetic radiation • Protects against ambient temperature and humidity fluctuations • Protects against the failure of any data input or storage device • Protects against any attempt at improper data entry or retrieval • Records and report the date and time of normal and abnormal events • Maintains a permanent record of all original audit data that cannot be modified or overridden but may be augmented by designated authorized officials in order to adjust for errors or omissions (e.g. during the canvassing process.) • Detect and record every event, including the occurrence of an error condition that the system cannot overcome, and time-dependent or programmed events that occur without the intervention of the voter or a polling place operator • Include built-in measurement, self-test, and diagnostic software and hardware for detecting and reporting the system's status and degree of operability DRE Systems Standards are used to ensure system integrity by validating that the voting system: (V1:2.2.4.2) • Maintains a record of each ballot cast using a process and storage location that differs from the main vote detection, interpretation, processing, and reporting path • Provides a capability to retrieve ballot images in a form readable by humans. Audit records are prepared for all testing phases of election operations using devices designed to be controlled by the jurisdiction or its contractors. These records rely upon automated audit data acquisition and machine-generated reports, with manual input of some information. These records address the ballot preparation and election definition phase, system readiness tests, and voting and ballot-counting operations. Individual test cases and steps contain instructions on how and when to generate and validate this information. (V1:2.2.5.2, 4.4) All voting systems are evaluated and verified to ensure that they meet the following requirements for time, sequence and preservation of Audit Records: • Except where noted, systems provide the capability to create and maintain a real-time audit record • All systems include a real-time clock as part of the system's hardware • All audit record entries include the time-and-date stamp • The audit record are active whenever the system is in an operating mode • The generation of audit record entries are not terminated or altered by program control, or by the intervention of any person • Once the system has been activated for any function, the system preserves the contents of the audit record during any interruption of power to the system

Test Detail	Test Methodology
Test Case Name	**PRI02 Closed Primary**
	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-based systems: (V1:3.2.5.1.2)

Test Detail	Test Methodology
Test Case Name	**PRI02 Closed Primary**
	• Outstack the ballot, or • Stop the ballot reader and display a message prompting the election official or designee to remove the ballot, or • Mark the ballot with an identifying mark to facilitate its later identification. Exception Handling (Precinct Count) refers to the handling of ballots for a precinct count system when they are unreadable or when some condition is detected requiring that the cards be segregated from normally processed ballots for human review. All paper based precinct count systems are validated to ensure that the following can be accomplished: (V1:3.2.5.1.3) • An unreadable or blank ballot - return the ballot and provide a message prompting the voter to examine the ballot • Ballot with a write-in vote - segregate the ballot or mark the ballot with an identifying mark to facilitate its later identification • A ballot with an overvote the system: o Provides a capability to identify an overvoted ballot o Returns the ballot o Provides an indication prompting the voter to examine the ballot; o Allows the voter to submit the ballot with the overvote o Provides a means for an authorized election official to deactivate this capability entirely and by contest • In response to a ballot with an undervote the system: o Provides a capability to identify an undervoted ballot o Returns the ballot o Provides an indication prompting the voter to examine the ballot o Allows the voter to submit the ballot with the undervote o Provides a means for an authorized election official to deactivate this capability Processing speed is verified for DRE voting systems to ensure that they: • Operate at a speed sufficient to respond to any operator and voter input without perceptible delay (no more than three seconds) • 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) Note: For Provisional/Challenged ballots, the vendor supports tabulation of these ballots at Central Count Party affiliation is identified on the ballots *where appropriate*
Voting: Optional functionality verifications	The functionality listed above in "**Variables: Voting Variations"** is verified here.

Test Detail	Test Methodology
Test Case Name	**PRI02 Closed Primary**
Post-Vote: **Closing the Polls**	Vendor documentation is reviewed, evaluated and used to create steps that ensure that all voting systems and equipment perform voting functions properly for all Post-Voting Functions. These steps are created, using the guidelines listed in VSS volum1, section 2.5. Verification of these steps provide a formal record of the following: • All systems provide capabilities to accumulate and report results for the jurisdiction and to generate audit trails • Precinct count systems provide a means to close the polling place including generating appropriate reports • The standards for closing the polling place are specific to precinct count systems. The system provides the means for: (V1:2.5.1) o Preventing the further casting of ballots once the polling place has closed o Providing an internal test that verifies that the prescribed closing procedure has been followed, and that the device status is normal o Incorporating a visible indication of system status o Producing a diagnostic test record that verifies the sequence of events, and indicates that the extraction of voting data has been activated o Precluding the unauthorized reopening of the polls once the poll closing has been completed for that election • All systems provide a means to consolidate vote data from all polling places, and optionally from other sources such as absentee ballots, provisional ballots, and voted ballots requiring human review (e.g., write-in votes). (V1:2.5.2) • All systems are able to create reports summarizing the data on multiple levels. (V1:2.5.3) • *If applicable*, the voting systems offer the capability to make unofficial results available to external organizations such as the news media, political party officials, and others. Although this capability is not required, systems that make unofficial results available: (V1:2.5.4) o Provide only aggregated results, and not data from individual ballots o Provide no access path from unofficial electronic reports or files to the storage devices for official data o Clearly indicate on each report or file that the results it contains are unofficial
Post-Vote: **Vote Count Verification**	After all voting listed in the Vote Data Matrix is performed, the election data is examined and all counts are validated on the individual voter level, the voting machine level, the precinct level and the central count level. This verification ensures that the system is correctly tabulating all data and is accurately recording cast ballots, including provisional. (V1:2.2.8.1, 2.3.6, 2.5, 3.2.3.1, 3.2.5.2,3.2.6.2.2, 3.2.4.3.3) This tabulation sometimes includes verification of the following: • Ensure undervotes are counted as cast votes • Separate accumulation of Undervotes and Paper Overvotes • Ensure Overvotes are counted on paper ballots and tally correctly

Test Detail	Test Methodology
Test Case Name	**PRI02 Closed Primary**
Post-Vote: **Security**	Post-Vote - Security: • System username/password authentication and other access controls are set up according to system documentation guidelines for all devices being tested. • Any/all unnecessary processes are disabled and/or required process control measures noted in the documentation are followed. • All COTS and vendor subsystems used for system security are configured and active as recommended by the system documentation. This includes all connection, port, virus, auditing capability, data or authorized process restriction systems. • Any other system security measures listed in the documentation are followed including setup of additional hardware or software not covered above. Please also see the Documentation section of the Security Test Case within Appendix A.
Post-Vote: **System Audit and Data Retention**	All applicable system reports are produced and verified at this point. The requirements listed in the VSS volume 1 are followed for verifying Data and Document Retention. These include the following: • Data and Document Retention (V1:4.3) • Audit Record Data (V1:4.4) Additionally, the guidelines listed in the VSS volume 1, section 3.2.8.2, are used to validate Data Report Generation.
Results are Observed	Review the outcome of the test(s) against the expected result(s): • **Accept**: expected results is observed • **Reject:** expected result is NOT observed • **Not Testable (NT)**: rejection of a previous test step prevents validation of this step or this was tested in another test case • **Not Applicable (NA):** not applicable to the current test scope or to the component under review • **Not Supported (NS)**: not supported in the current test scope
Record Observations and all input/outputs for each election	All information used in processing the test case is captured. This includes: inputs, outputs, deviations and any other item that may impact the validation of the test case. Any failure of the test against the EAC guidelines is reported and implies failure of the system. Failures are reported as Defect Issues in the Discrepancy Report and are provided to the manufacturer. Before the final Certification Test Report is issued, manufacturers are given the opportunity to correct all discrepancies. If the manufacturer submits corrections, retests are performed. Issues that do not impact the failure of the requirements but could be considered defects are logged as Informational Issues on the Discrepancy Report. It is the manufacturer's option to address these issues.

Test Detail	Test Methodology
Test Case Name	**GEN03 (Usability and Accessibility)**
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	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 Usability and Accessibility.
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 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
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

Test Detail	Test Methodology
Test Case Name	**GEN03 (Usability and Accessibility)**
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 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 bility to select from a range of voting options to conform to the laws of

Test Detail	Test Methodology
Test Case Name	**GEN03 (Usability and Accessibility)**
	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 • Is visible to designated election officials (V1: 2.2.9) Additionally, verification is done to ensure that Ballot boxes and ballot transfer boxes, which serve as secure containers for the storage and transportation of voted ballots, adhere to standards. (V1:3.2.4.2.6) For each iteration that the election is run: • All supplies necessary for testing are retrieved. • Verification is performed on the System to ensure that the correct versions of software, firmware and hardware, election and ballot is installed and set up as defined in the user documentation • A supervisory level access 'user' and password' is created or available • The Readiness Check List is completed if applicable • The date and tester(s) are documented Testers are informed that the test environment must remain static, if not, no changes shall occur without documentation in the test record and the authorization of the project manager.
Documentation: **Test Data & Test Results**	For each iteration that the election is run: • Capture all voting steps in order to maintain repeatability of the test • Record election, ballot, and vote data fields on the corresponding worksheet tabs • Save all worksheet tabs for all iterations of the test case • Record results of test run by entering 'Accept/Reject' on the Test Results Matrix • Provide comments when observing deviations, discrepancies or notable observations • Log discrepancies on the Discrepancy Report
Pre-vote: **Ballot Preparation**	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

Test Detail	Test Methodology
Test Case Name	**GEN03 (Usability and Accessibility)**
procedures verifications	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 purpose • For marksense systems, ensures that the timing marks align properly with the vote response fields (V1: 2.3.1.1.2) Verification of Ballot Production common standards ensures that: • The electronic display or paper ballot is capable of rendering an image of the ballot in any of the languages required by The Voting Rights Act of 1965, as amended, and as supported by the vendor • The electronic display or paper ballot does not show any advertising or commercial logos unless specifically provided for in State law. Electronic displays shall not provide connection to such material through a hyperlink • The ballot conforms to the vendor specifications for type of paper stock, weight, size, shape used to record votes, folding, bleed through, and ink for printing if paper ballots are used as part of the voting system (V1: 2.3.1.3, 2.3.1.3.1) For paper based recording, verification is performed to ensure the following: • A ballot can be accurately/securely defined and formatted (V1: 3.2.4.2) • A ballot can be accurately/securely programmed and installed into the appropriate media (V1:3.2.4.2.5) • The system Ignores, and extraneous perforations, smudges, and folds (V1:3.2.5.2.b) During the election definition and ballot preparation process, verification is performed to ensure that the system audits the preparation of the baseline ballot formats and modifications to them, a description of these modifications, and corresponding dates. The log is to include: • The allowable number of selections for an office or issue • The combinations of voting patterns permitted or required by the jurisdiction • The inclusion or exclusion of offices or issues as the result of multiple districting within the polling place

Test Detail	Test Methodology
Test Case Name	**GEN03 (Usability and Accessibility)**
	• 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: **Preparation - Security**	System Preparation - Security: • System username/password authentication and other access controls are set up according to system documentation guidelines for all devices being tested. • Any/all unnecessary processes are disabled and/or required process control measures noted in the documentation are followed. • All COTS and vendor subsystems used for system security are configured and active as recommended by the system documentation. This includes all connection, port, virus, and data or authorized process restriction systems. • Any other pre-election system security measures listed in the documentation are followed including setup of additional hardware or software not covered above. Please also see the Documentation section of the Security Test Case within Appendix A.
Readiness Testing and Poll Verification	Verification of Common Standards for Readiness Testing ensures that: • Voting machines or vote recording and data processing equipment, precinct and central count equipment are properly prepared for an election, and collect data that verifies equipment readiness • Status and data reports from each set of equipment can be obtained • The correct installation and interface of all system equipment • Hardware and software function correctly • Consolidated data reports at the polling place and higher jurisdictional levels can be generated • There is Segregation of test data from actual voting data, either procedurally or by hardware/software features When resident test software, external devices, and special purpose test software may be connected or installed in the voting device to simulate operator and voter functions provided the following standards are verified to ensure that: • These elements are capable of being tested separately, and shall be proven to be reliable verification tools prior to their use

Test Detail	Test Methodology
Test Case Name	**GEN03 (Usability and Accessibility)**
	• These elements are incapable of altering or introducing any residual effect on the intended operation of the voting device during any succeeding test and operational phase (V1: 2.3.4, 2.3.4.1) Vendor documentation is reviewed, evaluated and used to create steps that ensure all voting systems and equipment function properly before and during an election. Verification of these steps provide a formal record of the following: (V1:2.3.5) • The election's identification data • The identification of all equipment units • The identification of the polling place • The identification of all ballot formats • The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain only zeros) • A list of all ballot fields that can be used to invoke special voting options • Other information needed to confirm the readiness of the equipment, and to accommodate administrative reporting requirements To prepare voting devices to accept voted ballots, all voting systems are verified to ensure that they provide the capability to test each device prior to opening. This verifies that each is operating correctly. The tests include: • Confirmation that there are no hardware or software failures • Confirm that the device is ready to be activated for accepting votes • Confirmation that the test data is separate from voting data without impact to the testing Prior to Opening the polls, verification at the Central Location is performed to ensure that vote counting and vote consolidation equipment and software function properly. Any system used in a central count environment provides a printed record of the following**:** (V1:2.3.6) • The election's identification data • The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain all zeros) • Other information needed to ensure the readiness of the equipment and to accommodate administrative reporting requirements Verification is performed to ensure the following: • A list of all ballot fields is created (V1: 3.2.4.2.1) • The voting device is ready to accept votes (V1:3.2.4.3.1)
Voting: **Opening the Polls Verification**	Verification of the Readiness checklist is performed, ensuring that it is complete. Vendor documentation is reviewed, evaluated and used to create steps that ensure all voting systems and equipment perform voting functions properly. These steps are created, using the guidelines listed in VSS volume 1, section 2.4. Verification of these steps provide a formal record of the following: • Opening the polls • Casting a ballot

Test Detail	Test Methodology
Test Case Name	**GEN03 (Usability and Accessibility)**
	Additionally, verification ensures that all DRE systems support: • Activating the ballot • Augmenting the election counter • Augmenting the life-cycle counter If necessary, any issues, failures, or unexpected results and their required corrective action(s) are identified and recorded here. (V1: 2.4) Verification of Opening Polls for Precinct Count Systems (paper based) ensures: • An internal test of diagnostic capability to verify that all of the polling place tests specified in section 2.3.5 have been successfully completed • Automatic disabling any device that has not been tested until it has been tested. (V1: 2.4.1.1) • A means of verifying that ballot marking devices are properly prepared and ready for use • A voting booth or similar facility, in which the voter may mark the ballot in secrecy • Secure receptacles for holding voted ballots (V1: 2.4.1.2.1) • Activating the ballot counting device • Verifying the device has been correctly activated and is functioning properly • Identifying device failure and corrective action needed (V1: 2.4.1.2.2) Verification of Opening Polls for Precinct Count Systems (DRE) ensures that: • A security seal, password, or a data code recognition capability to prevent the inadvertent or unauthorized actuation of the poll-opening function • A means of enforcing the execution of steps in the proper sequence • A means of verifying the system as been activated correctly • A means of identifying system failure and any corrective action needed (V1: 2.4.1.3) Verification of Activating the Ballot (DRE) ensures that the system: • Enables election officials to control the content of the ballot presented to the voter, whether presented in printed form or electronic display, such that each voter is permitted to record votes only in contests in which that voter is authorized to vote • Allows each eligible voter to cast a ballot • Prevents a voter from casting more than one ballot in the same election • Activates the casting of a ballot in a general election • Enables the selection of the ballot that is appropriate to the party affiliation declared by the voter in a primary election • Activates all portions of the ballot upon which the voter is entitled to vote • Disables all portions of the ballot upon which the voter is not entitled to vote (V1: 2.4.2) Verification of Casting a Ballot Common Standards ensures that the system: • Verifies that additional functional capabilities that enable accessibility to

Test Detail	Test Methodology
Test Case Name	**GEN03 (Usability and Accessibility)**
	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 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); and • 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; and • Allows an authorized election official to turn off the capabilities defined above (V1: 2.4.3.2.2) Additionally, verification is performed to ensure that all DRE systems: • Prohibit the voter from accessing or viewing any information on the display screen that has not been authorized by election officials and preprogrammed into the voting system (i.e., no potential for display of external information or linking to other information sources) • Enable the voter to easily identify the selection button or switch, or the active area of the ballot display that is associated with each candidate or ballot measure response • Allow the voter to select his or her preferences on the ballot in any legal number and combination

Test Detail	Test Methodology
Test Case Name	**GEN03 (Usability and Accessibility)**
	• Indicate that a selection has been made or canceled • Indicate to the voter when no selection, or an insufficient number of selections, has been made in a contest • Prevent the voter from overvoting • Notify the voter when the selection of candidates and measures is completed • Allow the voter, before the ballot is cast, to review his or her choices and, if the voter desires, to delete or change his or her choices before the ballot is cast • For electronic image displays, prompt the voter to confirm the voter's choices before casting his or her ballot, signifying to the voter that casting the ballot is irrevocable and directing the voter to confirm the voter's intention to cast the ballot • Notify the voter after the vote has been stored successfully that the ballot has been cast • Notify the voter that the ballot has not been cast successfully if it is not stored successfully, including storage of the ballot image, and provide clear instruction as to the steps the voter should take to cast his or her ballot should this event occur • Provide sufficient computational performance to provide responses back to each voter entry in no more than three seconds • Ensure that the votes stored accurately represent the actual votes cast; • Prevent modification of the voter's vote after the ballot is cast; • Provide a capability to retrieve ballot images in a form readable by humans (in accordance with the requirements of Section 2.2.2.2 and 2.2.4.2) • Increment the proper ballot position registers or counters • Protect the secrecy of the vote throughout the voting process • Prohibit access to voted ballots until after the close of polls • Provide the ability for election officials to submit test ballots for use in verifying the end-to-end integrity of the system • Isolate test ballots such that they are accounted for accurately in vote counts and are not reflect in official vote counts for specific candidates or measures (V1: 2.4.3.3)
Voting: **Required functionality verifications**	Vendor documentation is reviewed, evaluated and used to create Vote Data or the test 'voters' for this test case. This Vote Data is created in matrix form and is used to ensure vote accuracy based on common standards listed in VSS volume 1, section 2.2.2.1. Each 'voter' in the Vote Data Matrix votes the ballot. A SysTest employee performs this manually. The different combinations of candidates selected by each voter in the Vote Data Matrix validates the system's ability to: • Record the election precincts/splits, contests, candidates, and issues exactly as defined by election officials • Record the appropriate options for ballot content, verifying the appropriate contests/issues are displayed as determined in election creation • Record the appropriate options for casting and recording votes across a range

Test Detail	Test Methodology
Test Case Name	**GEN03 (Usability and Accessibility)**
	of voting options • Record each vote precisely as indicated by the voter and be able to produce an accurate report of all votes cast • Include control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) to demonstrate that the system has been designed for accuracy • Provide software that monitors the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected The process for casting a ballot is defined in detail in individual test case steps. These cases, steps, and verification criteria are created using the requirements stated in the VSS volume 1, section 2.4.3 and section 4.5. Additionally, the Vendor documentation is evaluated and used to enhance the testing procedures. The standards used for validation consist of the following sections: • Common Standards (V1:2.4.3.1) • Paper-Based Systems Standards (V1:2.4.3.2) • DRE Systems Standards (V1:2.4.3.3) • Vote Secrecy (DRE Systems) (V1:4.5) Backup files are made and hard copies printed for all DRE systems to record and retain redundant copies of the original ballot image (V1: 2.2.2.2, 2.2.4.2) System auditing and functional testing is performed in order to validate vote data, prescient counts, central counts, audit records and error logs. Verification is performed on the error logs based on the standards listed in the VSS volume 1 section 2.2.5. The test ballots are design with formats and voting patterns sufficient to verify performance of the test election programs. Ballots are cast in a number sufficient to demonstrate proper processing, error handling, and generation of audit data as specified in Volume I, Sections 2 and 4. Test case steps are performed during the Functionality Testing in Parallel with Hardware Testing for Precinct Count Systems to verify voting functions defined in Vol. 1: 2.4 and 2.5 of voting equipment and precinct counting equipment. Verification ensures that: • Preparation of the election programs: o Verify resident firmware, if any o Prepare software (including firmware) to simulate all ballot format and logic options for which the system will be used o Verify program memory device content o Obtain and design test ballots with formats and voting patterns sufficient to verify performance of the test election programs • Procedures to program precinct ballot counters: o Install program and data memory devices, or verify presence if resident o Verify operational status of hardware • Procedures to simulate opening of the polls: o Perform procedures required to prepare hardware for election

Test Detail	Test Methodology
Test Case Name	**GEN03 (Usability and Accessibility)**
	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) Common Standards are used to ensure system integrity by validating that the voting system: (2.2.4.1) • Protects, by a means compatible with these Standards, against a single point of failure that would prevent further voting at the polling place

Test Detail	Test Methodology
Test Case Name	**GEN03 (Usability and Accessibility)**
	• Protects against the interruption of electronic power • Protects against generated or induced electromagnetic radiation • Protects against ambient temperature and humidity fluctuations • Protects against the failure of any data input or storage device • Protects against any attempt at improper data entry or retrieval • Records and report the date and time of normal and abnormal events • Maintains a permanent record of all original audit data that cannot be modified or overridden but may be augmented by designated authorized officials in order to adjust for errors or omissions (e.g. during the canvassing process.) • Detect and record every event, including the occurrence of an error condition that the system cannot overcome, and time-dependent or programmed events that occur without the intervention of the voter or a polling place operator • Include built-in measurement, self-test, and diagnostic software and hardware for detecting and reporting the system's status and degree of operability DRE Systems Standards are used to ensure system integrity by validating that the voting system: (V1:2.2.4.2) • Maintains a record of each ballot cast using a process and storage location that differs from the main vote detection, interpretation, processing, and reporting path • Provides a capability to retrieve ballot images in a form readable by humans. Audit records are prepared for all testing phases of election operations using devices designed to be controlled by the jurisdiction or its contractors. These records rely upon automated audit data acquisition and machine-generated reports, with manual input of some information. These records address the ballot preparation and election definition phase, system readiness tests, and voting and ballot-counting operations. Individual test cases and steps contain instructions on how and when to generate and validate this information. (V1:2.2.5.2, 4.4) All voting systems are evaluated and verified to ensure that they meet the following requirements for time, sequence and preservation of Audit Records: • Except where noted, systems provide the capability to create and maintain a real-time audit record • All systems include a real-time clock as part of the system's hardware • All audit record entries include the time-and-date stamp • The audit record are active whenever the system is in an operating mode • The generation of audit record entries are not terminated or altered by program control, or by the intervention of any person • Once the system has been activated for any function, the system preserves the contents of the audit record during any interruption of power to the system until processing and data reporting have been completed • The system is capable of printing a copy of the audit record (V1:2.2.5.2.1, 3.2.7, 3.2.7.2) All voting systems are evaluated and verified to ensure that they meet the following requirements for Error Messages: • The system generates, stores, and reports to the user all error messages as they occur

Test Detail	Test Methodology
Test Case Name	**GEN03 (Usability and Accessibility)**
	• 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-based systems: (V1:3.2.5.1.2) • Outstack the ballot, or • Stop the ballot reader and display a message prompting the election official or designee to remove the ballot, or • Mark the ballot with an identifying mark to facilitate its later identification. Exception Handling (Precinct Count) refers to the handling of ballots for a precinct

Test Detail	Test Methodology
Test Case Name	**GEN03 (Usability and Accessibility)**
	count system when they are unreadable or when some condition is detected requiring that the cards be segregated from normally processed ballots for human review. All paper based precinct count systems are validated to ensure that the following can be accomplished: (V1:3.2.5.1.3) • An unreadable or blank ballot - return the ballot and provide a message prompting the voter to examine the ballot • Ballot with a write-in vote - segregate the ballot or mark the ballot with an identifying mark to facilitate its later identification • A ballot with an overvote the system: o Provides a capability to identify an overvoted ballot o Returns the ballot o Provides an indication prompting the voter to examine the ballot; o Allows the voter to submit the ballot with the overvote o Provides a means for an authorized election official to deactivate this capability entirely and by contest • In response to a ballot with an undervote the system: o Provides a capability to identify an undervoted ballot o Returns the ballot o Provides an indication prompting the voter to examine the ballot o Allows the voter to submit the ballot with the undervote o Provides a means for an authorized election official to deactivate this capability Processing speed is verified for DRE voting systems to ensure that they: • Operate at a speed sufficient to respond to any operator and voter input without perceptible delay (no more than three seconds) • 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) Note: For Provisional/Challenged ballots, the vendor supports tabulation of these ballots at Central Count
Voting: Optional functionality verifications	The functionality listed above in "**Variables: Voting Variations"** is verified here.
Post-Vote: **Closing the Polls**	Vendor documentation is reviewed, evaluated and used to create steps that ensure that all voting systems and equipment perform voting functions properly for all Post-Voting Functions. These steps are created, using the guidelines listed in VSS volum1, section 2.5. Verification of these steps provide a formal record of the following: • All systems provide capabilities to accumulate and report results for the jurisdiction and to generate audit trails • Precinct count systems provide a means to close the polling place including generating appropriate reports

Test Detail	Test Methodology
Test Case Name	**GEN03 (Usability and Accessibility)**
	• The standards for closing the polling place are specific to precinct count systems. The system provides the means for: (V1:2.5.1) o Preventing the further casting of ballots once the polling place has closed o Providing an internal test that verifies that the prescribed closing procedure has been followed, and that the device status is normal o Incorporating a visible indication of system status o Producing a diagnostic test record that verifies the sequence of events, and indicates that the extraction of voting data has been activated o Precluding the unauthorized reopening of the polls once the poll closing has been completed for that election • All systems provide a means to consolidate vote data from all polling places, and optionally from other sources such as absentee ballots, provisional ballots, and voted ballots requiring human review (e.g., write-in votes). (V1:2.5.2) • All systems are able to create reports summarizing the data on multiple levels. (V1:2.5.3) • *If applicable*, the voting systems offer the capability to make unofficial results available to external organizations such as the news media, political party officials, and others. Although this capability is not required, systems that make unofficial results available: (V1:2.5.4) o Provide only aggregated results, and not data from individual ballots o Provide no access path from unofficial electronic reports or files to the storage devices for official data o Clearly indicate on each report or file that the results it contains are unofficial
Accessibility verifications	The Standards provide requirements for voting systems to meet the accessibility needs of a broad range of voters with disabilities. The vendor must either configure all of the system's voting stations to meet the accessibility specifications or must design a unique station that conforms to the accessibility requirements and is part of the overall voting system configuration. Mimicking the voter with disabilities, verification is done to ensure that: • The voter can perform the complete voting experience independently and that their experience is similar to a non-disabled voter • The ballot is not visible to others • The ballot information for each voter is not available to unauthorized persons • The integrity of the ballot information is maintained similarly to non-disabled ballot information (V1: 2.2.7) To facilitate accessibility, all voting systems must meet Common Standards, as illustrated in Figures 2-1 through 2-4 listed in the VSS. (V1: 2.2.7.1) These Common Standards include: • Reach • Obstruction

Test Detail	Test Methodology
Test Case Name	**GEN03 (Usability and Accessibility)**
	• Protrusion • Operable controls • ADA standards Mimicking the voter with disabilities, measurements are taken, according to the guidelines listed in the VSS, to ensure that disabled voter accessibility meets the necessary guidelines. Additionally verification of DRE voting systems ensures that they provide, as part of their configuration, the capability to provide access to voters with a broad range of disabilities. The DRE standards, listed in the VSS, are followed and used to verify each applicable voting machine. When necessary, measuring devices are used for validation. This can include pressure and dB meters, rulers and stopwatches. (V1: 2.2.7.2)
Usability verifications	Usability verification addresses the design of the voting system and it's ability to meet the needs of the voters, that is, to ensure that the interfaces between the voter and the system are easy to use and minimize voter errors. The following areas are focused on in this step: • Information displays, e.g., presentations of contests, candidates, propositions, and instructions • Vote input fields, e.g., the location where the voter indicates his or her selection • Navigation aids, e.g., the way that voters "move" from one part of the system to another The guidelines listed in the VSS Volume 1, Appendix C and section 3.4.9, are followed in order to verify: • General Principles (V1: Appendix C.2) • Overall Design and Layout of the Voter Workspace (V1: Appendix C.3) • Ballot Legibility and Understandability (V1: Appendix C.4) • Information Grouping (V1: Appendix C.5) • Voting Input Fields (V1: Appendix C.6) • Navigation and Manipulation of Ballots (V1: Appendix C.7) • Preventing and Minimizing Voter Errors (V1: Appendix C.8) • Help and System Failure (V1: Appendix C.9) • Voter Familiarization and Training (V1: Appendix C.10)
Post-Vote: **Vote Count Verification**	After all voting listed in the Vote Data Matrix is performed, the election data is examined and all counts are validated on the individual voter level, the voting machine level, the precinct level and the central count level. This verification ensures that the system is correctly tabulating all data and is accurately recording cast ballots, including provisional. (V1:2.2.8.1, 2.3.6, 2.5, 3.2.3.1, 3.2.5.2,3.2.6.2.2, 3.2.4.3.3) This tabulation sometimes includes verification of the following: • Ensure undervotes are counted as cast votes • Separate accumulation of Undervotes and Paper Overvotes • Ensure Overvotes are counted on paper ballots and tally correctly

Test Detail	Test Methodology
Test Case Name	**GEN03 (Usability and Accessibility)**
Post-Vote: **Security**	Post-Vote - Security: • System username/password authentication and other access controls are set up according to system documentation guidelines for all devices being tested. • Any/all unnecessary processes are disabled and/or required process control measures noted in the documentation are followed. • All COTS and vendor subsystems used for system security are configured and active as recommended by the system documentation. This includes all connection, port, virus, auditing capability, data or authorized process restriction systems. • Any other system security measures listed in the documentation are followed including setup of additional hardware or software not covered above. Please also see the Documentation section of the Security Test Case within Appendix A.
Post-Vote: **System Audit and Data Retention**	All applicable system reports are produced and verified at this point. The requirements listed in the VSS volume 1 are followed for verifying Data and Document Retention. These include the following: • Data and Document Retention (V1:4.3) • Audit Record Data (V1:4.4) Additionally, the guidelines listed in the VSS volume 1, section 3.2.8.2, are used to validate Data Report Generation.
Results are Observed	Review the outcome of the test(s) against the expected result(s): • **Accept**: expected results is observed • **Reject:** expected result is NOT observed • **Not Testable (NT)**: rejection of a previous test step prevents validation of this step or this was tested in another test case • **Not Applicable (NA):** not applicable to the current test scope or to the component under review • **Not Supported (NS)**: not supported in the current test scope
Record Observations and all input/outputs for each election	All information used in processing the test case is captured. This includes: inputs, outputs, deviations and any other item that may impact the validation of the test case. Any failure of the test against the EAC guidelines is reported and implies failure of the system. Failures are reported as Defect Issues in the Discrepancy Report and are provided to the manufacturer. Before the final Certification Test Report is issued, manufacturers are given the opportunity to correct all discrepancies. If the manufacturer submits corrections, retests are performed. Issues that do not impact the failure of the requirements but could be considered defects are logged as Informational Issues on the Discrepancy Report. It is the manufacturer's option to address these issues.

Test Detail	Test Methodology
Test Case Name	**Readiness Test**
Scope	A functional test that uses The 2002 Voting System Standards (VSS) guidelines to validate Readiness throughout the entire voting system. (V1:2.3.4)
Objective	The object of this test case is to verify equipment and system readiness to ensure that the voting system functions properly, to confirm that the system equipment has been properly intergraded, and to obtain equipment status reports. (V1:2.3.4)
Standards Documents	Voting System Standards 2002, vol. 1 Voting System Standards 2002, vol. 2 Specific standards are noted in following steps.
A listing of the applicable voting system machines	**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 Refer to the following tables for complete descriptions: ➢ Matrix of Required Software/Firmware ➢ Matrix of Required Hardware
Pre-requisites and initialization of the test case	This testing is to be executed on initial testing and each time the system is to be shut down and restarted.
Documentation of Test Data & Test Results	For each iteration that the election is run: • Capture all voting steps in order to maintain repeatability of the test • Record election, ballot, and vote data fields on the corresponding worksheet tabs • Save all worksheet tabs for all iterations of the test case • Record results of test run by entering 'Accept/Reject' on the Test Results Matrix • Provide comments when observing deviations, discrepancies or notable observations • Log discrepancies on the Discrepancy Report
System Preparation - Security	System Preparation - Security: • System username/password authentication and other access controls are set up according to system documentation guidelines

Test Detail	Test Methodology
Test Case Name	**Readiness Test**
	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 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**

Test Detail	Test Methodology
Test Case Name	**Readiness Test**
	Unity Version 4.0 Release Date: August 2007 **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.

Test Detail	Test Methodology
Test Case Name	**Readiness Test**
	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
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 and/or VSSG guidelines. It also describes Access controls **Source Code Review** - Source Code Review insures source code meets VSS and/or VVSG 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 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.
Variables: Voting Variations	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 **DS200** - intElect DS200 Ballot Scanner **iVotronic** - iVotronic DRE (12 & 15) **M650** - Model 650 Optical Scan central Count Counter

Test Detail	Test Methodology
Test Case Name	**Security**
	Refer to the following tables for complete descriptions: ➢ Matrix of Required Software/Firmware ➢ Matrix of Required Hardware
Role	In this section of the Security test case, SysTest Labs validates that the vendor has implemented adequate controls to ensure an adequate amount of security is in place, via physical testing methods. Privileges are not allowed to be: • Exceeded (V1:6.2.1.2c) • Changed to Run Reports Voters are inhibited from: • Accessing Equipment Before Polls Open • Running Reports Changes to Privileges are Prohibited for IDs and Passwords Thus Preventing Unauthorized Report Printing, Results Transmission, Results Downloading and Resetting of Elections Voter equipment access or keys are limited to ensure: • Only the User interface is accessible • Only a single vote may be cast • Closed Polls are secure • Counts are not available to voters • Unauthorized Accounts from System Functions Fraudulent Ballots are not accepted by the system ensuring only valid ballots are counted
Access	In this section of the Security test case, SysTest Labs validates that the vendor has implemented adequate controls to ensure an adequate amount of security is in place, via physical testing methods. 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 Security	In this section of the Security test case, SysTest Labs validates that the vendor has implemented adequate controls to ensure an adequate amount of security is in place, via physical testing methods. • System security is achieved through a combination of technical capabilities and sound administrative practices. To ensure security, the system: Vol1, 2.2.1

Test Detail	Test Methodology
Test Case Name	**Security**
	o Provides system functions that are executable only in the intended manner and order, and only under the intended conditions. o Uses the system's control logic to prevent a system function from executing if any preconditions to the function have not been met. o Provides safeguards to protect against tampering during system repair, or interventions in system operations, in response to system failure. o Provides security provisions that are compatible with the procedures and administrative tasks involved in equipment preparation, testing, and operation. o If access to a system function is to be restricted or controlled, the system incorporates a means of implementing this capability. o Provides documentation of mandatory administrative procedures for effective system security • The voting system may use a local or remote data network. Should such a network be used in a jurisdiction, all components of the network do comply with the telecommunications requirements described in Section 5 of the Standards and the Security requirements as described in Section 6. Vol 1, 3.2.2.15
System Log	In this section of the Security test case, SysTest Labs validates that the vendor has implemented adequate controls to ensure an adequate amount of security is in place, via physical testing methods. Verification of System Log Activity is performed to ensure: • Error Activity provided by the system is complete, applicable, and appropriate (V1:4.4.3) • Voting Activity is captured correctly (V1:4.4.3.d) • Log(s) have the needed protection to validate that the information is secure (V1:4.4.3)
Software Security	• Software security validation ensures that the firmware has been shown to be inaccessible to activation or control (V1:6.4.1.c) • Verify the Separation of Election Specific Firmware and Operating System are stored (V1:6.4.1.d)
Data Integrity	In this section of the Security test case, SysTest Labs validates that the vendor has implemented adequate controls to ensure an adequate amount of security is in place, via physical testing methods. • The system meets the following requirements for installation of software, including hardware with imbedded firmware: V1.6.4.1

Test Detail	Test Methodology
Test Case Name	**Security**
	o 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 o 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 • Transmission of data shall ensure that receipt of valid vote records is verified at the receiving stations (V1:6.5.2) • Transmission of Cast Ballots During Voting Error Detection, Recovery and Retransmission • Transmission of Cast Ballots During Voting Integrity Checks • Transmission Verification Checks • 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)
Telecommunications & Data Transmission	In this section of the Security test case, SysTest Labs validates that the vendor has implemented adequate controls to ensure an adequate amount of security is in place, via physical testing methods. • The system transmits data over public telecommunications networks, and as such: V1.6.6.1 o Preserves the secrecy of a voter's ballot choices, and prevents anyone from violating ballot privacy • Encrypted Transmissions (V1:6.5.3.a) • Encryption Specification Verification • Session Hijacking • Monitoring and Responding to External Threats (V1:6.5.4.3) • Shared Operating Environment (V1:6.5.5)
Telecommunications	In this section of the Security test case, SysTest Labs validates that the vendor has implemented adequate controls to ensure an adequate amount of security is in place, via physical testing methods. • Security for Transmissions (V1:6.6) • Unauthorized Tool • Virus • Threat Reception and Storage Prevention (V1:6.5.4.2) • Remote Access Disabled • User Account Restriction From Remote Access Settings • Routers and/or Firewalls
Threat Protection	In this section of the Security test case, SysTest Labs validates that the vendor has implemented adequate controls to ensure an adequate amount of security is in place, via physical testing methods. • Memory Threat & Virus Scanning Mechanisms (1-6.5.4.2) • Rootkit Scanning Mechanisms

Test Detail	Test Methodology
Test Case Name	**Security**
Audit Log	In this section of the Security test case, SysTest Labs validates that the vendor has implemented adequate controls to ensure an adequate amount of security is in place, via physical testing methods. • Audit logs and data files cannot be altered through the use of an alternate boot sequence without detection, and the test will consist of attempting to boot the devices using alternative media during boot sequences. Audit logs and data files cannot be altered through the use of editing tools without detection. The test will consist of attempting to edit the audit log to confirm that the system either: • Does not allow edits of the audit log or data files, or • Detects and reports all attempts at editing the audit log or data files
Data Protection	Logical Isolation of Voting System Software & Data (V1:6.5.5.b)
Role	In this section of the Security test case, SysTest Labs validates that the vendor has implemented adequate controls to ensure an adequate amount of security is in place, via physical testing methods. • 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 • Password Required for Each System Software Component (V1:6.5.5.c) • Password Required for Each System Data Component • Password Required for Each System Data Component • Hardware Key Required for Each System Hardware Component • Each Type of User Account Can Only Perform Intended Functions
Data Protection	In this section of the Security test case, SysTest Labs validates that the vendor has implemented adequate controls to ensure an adequate amount of security is in place, via physical testing methods. • Access Control Lists Preclude Data Leakage (V1:6.5.5.d) • Routers and Firewalls Preclude Data Leakage • Electronic Policies Prevent Copy of Data • Voting System Access to Incomplete Election Returns (V1:6.5.6)
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: • 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)

Test Detail	Test Methodology
Test Case Name	**Security**
	o Software access controls documentation o Hardware access controls documentation o Communications documentation o Effective password management documentation o Protection abilities of a particular operating system documentation o General characteristics of supervisory access privileges documentation o Segregation of Duties documentation o Any additional relevant characteristics • The voting system vendor: (V1:6.2.1.2) o Identifies each person, to whom access is granted, and the specific functions and data to which each person holds authorized access. o specifies whether an individual's authorization is limited to a specific time, time interval, or phase of the voting our counting operation • 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) o Use of data and user authorization o Program unit ownership and other regional boundaries o One-end or two-end port protection devices o Security kernels o Computer-generated password keys o Special protocols o Message encryption o Controlled access security • The vendor defines and provides a detailed description of the methods used to prevent unauthorized access to the access control capabilities of the system itself. (V1.6.2.2) • 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) o Allow the immediate detection of tampering with vote casting devices and precinct ballot counters o Control physical access to a telecommunications link if such a link is used • The Vendor develops and documents, in detail, the measures to be taken in a central counting environment. These measures include

Test Detail	Test Methodology
Test Case Name	**Security**
	physical and procedural controls related to the: (V1:6.3.2) o Handling of ballot boxes o Preparing of ballots for counting o Counting operations o Reporting data • The system meets the following requirements for installation of software, including hardware with embedded firmware: V1.6.4.1 o 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 o 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 o After initiation of election day testing, no source code or compilers or assemblers are resident or accessible • 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 • 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 • 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 • 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 o The vendor implements an encryption standard currently documented and validated for use by an agency of the U.S. Federal Government

Test Detail	Test Methodology
Test Case Name	**Security**
	o Provides a means to detect the presence of an intrusive process, such as an Intrusion Detection System • 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 • 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 o Operating systems o Communications routers o Modem drivers o Dial-up networking software • 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 o Detect the presence of a threat in a transmission o Remove the threat from infected files/data o Prevent against storage of the threat anywhere on the receiving device o Provide the capability to confirm that no threats are stored in system memory and in connected storage media o Provide data to the system audit log indicating the detection of a threat and the processing performed • 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 • 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 o 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) o Evaluate the threats and, if any, proposed responses o Develop responsive updates to the system and/or corrective procedures o 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

Test Detail	Test Methodology
Test Case Name	Security
	o 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 o Address threats emerging too late to correct the system at least one month before the election, including o Provide prompt, emergency notification to the ITA and the affected states and user jurisdictions o Assist client jurisdictions directly, or advising them through detailed written procedures, to disable the public telecommunications mode of the system o After the election, modify the system to address the threat; submitting the modified system to an ITA and appropriate state certification authority for approval, and assisting client jurisdictions directly, or advising them through detailed written procedure, to update their systems and/or to implement the corrective procedures after approval • 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 o Uses security procedures and logging records to control access to system functions o Partitions or compartmentalizes voting system functions from other concurrent functions at least logically, and preferably physically as well o Controls system access by means of passwords, and restriction of account access to necessary functions only; o Has capabilities in place to control the flow of information, precluding data leakage through shared system resources • 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 o 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 o Uses voting system software and its security environment is designed such that data, which is accessible to interactive

Test Detail	Test Methodology
Test Case Name	**Security**
	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: ♦ The output file or database has no provision for write-access back to the system ♦ 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 • The system transmits data over public telecommunications networks such that: V1.6.6.1 o Digital signatures are employed for all communications between the vote server and other devices that communicate with the server over the network o At least two authorized election officials are required to activate any critical operation regarding the processing of ballots transmitted over a public communications network, i.e. the passwords or cryptographic keys of at least two employees are required to perform processing of votes
External Access	In this section of the Security test case, SysTest Labs validates that the vendor has implemented adequate controls to ensure an adequate amount of security is in place, via physical testing methods. • 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

<table>
<tr><th>Test Detail</th><th>Test Methodology</th></tr>
<tr><td>Test Case Name</td><td>Telecommunications</td></tr>
<tr><td></td><td>detailed in the table below.

Operational, Exception Handling and Security Test Case Classifications:
<table>
<tr><th>Test Id</th><th>Test Class</th><th>Telecommunication Test Class Description</th></tr>
<tr><td></td><td>Operational Test</td><td></td></tr>
<tr><td>.1a</td><td>Manual</td><td>Manual initiate transfer - Valid Receiver</td></tr>
<tr><td>.1b</td><td>Auto</td><td>Auto initiate transfer - Valid Receiver</td></tr>
<tr><td></td><td>Negative Test</td><td></td></tr>
<tr><td>.2a</td><td>Invalid</td><td>Initiate transfer - Invalid Receiver</td></tr>
<tr><td>.2b</td><td>No receiver</td><td>Initiate transfer - No Receiver</td></tr>
<tr><td>.2c</td><td>Cancel</td><td>Initiate transfer - Cancel Session</td></tr>
<tr><td>.2d</td><td>Interrupt</td><td>Initiate transfer - Interrupt Session</td></tr>
<tr><td>.2z</td><td>Resume</td><td>Resume transfer</td></tr>
<tr><td></td><td>Security Test</td><td></td></tr>
<tr><td>.3a</td><td>Intrude</td><td>Threat / Intrusion Detection</td></tr>
<tr><td>.3b</td><td>Remove</td><td>Threat Removal</td></tr>
<tr><td>.3c</td><td>Store</td><td>Threat Storage Prevention</td></tr>
<tr><td>.3d</td><td>Log</td><td>Log entries - threats or intrusions detected and resulting actions</td></tr>
<tr><td>.3e</td><td>Signed</td><td>Digital signature, encryption</td></tr>
<tr><td>.3f</td><td>Authorize</td><td>Dual authorization / cryptographic keys employed</td></tr>
</table></td></tr>
<tr><td>Pre-requisites and initialization of the test case</td><td>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</td></tr>
<tr><td>Test Verifications</td><td>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</td></tr>
</table>

Test Detail	Test Methodology
Test Case Name	Telecommunications
	vendor documentation. (V1: 5.1.1) 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

Test Detail	Test Methodology
Test Case Name	Telecommunications
	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; • 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;

Test Detail	Test Methodology
Test Case Name	**Telecommunications**
	• Prevent against storage of the threat anywhere on the receiving device; • Provide the capability to confirm that no threats are stored in system memory and in connected storage media; and • Provide data to the system audit log indicating the detection of a threat and the processing performed. • Validate the use of multiple forms of protective software as needed to provide capabilities for the full range of products used by the voting system. 15. Verify Vendor documentation to ensure conformance of Monitoring and Responding to External Threats to which their voting systems are vulnerable. This documentation shall provide a detailed description, including scheduling information, of the procedures the vendor will use to: (V1: 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

Test Detail	Test Methodology
Test Case Name	**Telecommunications**
	• 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 • **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**
Scope	A functional test that uses The 2002 Voting System Standards (VSS) guidelines to validate the individual ballot positions in terms of a maximum error rate while processing a specified volume of data. (V2:4.7.1.1)
Objective	The object of this test is to verify that the voting system can accurately and reliably print ballots incorporating a minimum 1,549,703 ballot positions (including voted and non-voted positions) and that these ballots can be mechanically/electronically tabulated without error.
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	**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 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

Test Detail	Test Methodology
Test Case Name	**Accuracy**
	• 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 bility 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 • Is visible to designated election officials (V1: 2.2.9) Additionally, verification is done to ensure that Ballot boxes and ballot transfer boxes, which serve as secure containers for the storage and transportation of voted ballots, adhere to standards. (V1:3.2.4.2.6) For each iteration that the election is run: • All supplies necessary for testing are retrieved. • Verification is performed on the System to ensure that the correct versions of software, firmware and hardware, election and ballot is installed and set up as defined in the user documentation • A supervisory level access 'user' and password' is created or available • The Readiness Check List is completed if applicable • The date and tester(s) are documented Testers are informed that the test environment must remain static, if not, no changes shall occur without documentation in the test record and the authorization of the project manager.

Test Detail	Test Methodology
Test Case Name	**Accuracy**
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
Pre-vote: Ballot Preparation procedures verifications	Installation and Election databases can be accurately/securely defined and formatted

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
	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

Test Detail	Test Methodology					
Test Case Name	Accuracy					
	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
				Even Marked	0	0
				Blank (unmarked)	80	5920
				All-Fill marked	0	0
		Number of Ballot Positions	264	Number of Ballot Positions	21120	1562880

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

Test Detail	Test Methodology
Test Case Name	**Accuracy**
	• Other information needed to confirm the readiness of the equipment, and to accommodate administrative reporting requirements To prepare voting devices to accept voted ballots, all voting systems are verified to ensure that they provide the capability to test each device prior to opening. This verifies that each is operating correctly. The tests include: • Confirmation that there are no hardware or software failures • Confirm that the device is ready to be activated for accepting votes • Confirmation that the test data is separate from voting data without impact to the testing Prior to Opening the polls, verification at the Central Location is performed to ensure that vote counting and vote consolidation equipment and software function properly. Any system used in a central count environment provides a printed record of the following: (V1:2.3.6) • The election's identification data • The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain all zeros) • Other information needed to ensure the readiness of the equipment and to accommodate administrative reporting requirements Verification is performed to ensure the following: • A list of all ballot fields is created (V1: 3.2.4.2.1) • The voting device is ready to accept votes (V1:3.2.4.3.1)
Voting: **Opening the Polls Verification**	Verification of the Readiness checklist is performed, ensuring that it is complete. Vendor documentation is reviewed, evaluated and used to create steps that ensure all voting systems and equipment perform voting functions properly. These steps are created, using the guidelines listed in VSS volume 1, section 2.4. Verification of these steps provide a formal record of the following: • Opening the polls • Casting a ballot Additionally, verification ensures that all DRE systems support: • Activating the ballot • Augmenting the election counter • Augmenting the life-cycle counter If necessary, any issues, failures, or unexpected results and their required corrective action(s) are identified and recorded here. (V1: 2.4) Verification of Opening Polls for Precinct Count Systems (paper based) ensures: • An internal test of diagnostic capability to verify that all of the polling place tests specified in section 2.3.5 have been successfully completed • Automatic disabling any device that has not been tested until it has been

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

Test Detail	Test Methodology
Test Case Name	**Accuracy**
	voters to resume voting once the voting system has reverted to back-up power; and • Provides the capability for voters to continue casting ballots in the event of a failure of a telecommunications connection within the polling place or between the polling place and any other location. (Vol. 1: 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; and • Allows an authorized election official to turn off the capabilities defined above (V1: 2.4.3.2.2) Additionally, verification is performed to ensure that all DRE systems: • Prohibit the voter from accessing or viewing any information on the display screen that has not been authorized by election officials and preprogrammed into the voting system (i.e., no potential for display of external information or linking to other information sources) • Enable the voter to easily identify the selection button or switch, or the active area of the ballot display that is associated with each candidate or ballot measure response • Allow the voter to select his or her preferences on the ballot in any legal number and combination • Indicate that a selection has been made or canceled • Indicate to the voter when no selection, or an insufficient number of selections, has been made in a contest • Prevent the voter from overvoting • Notify the voter when the selection of candidates and measures is completed • Allow the voter, before the ballot is cast, to review his or her choices and, if the voter desires, to delete or change his or her choices before the ballot is cast • For electronic image displays, prompt the voter to confirm the voter's choices before casting his or her ballot, signifying to the voter that casting the ballot is irrevocable and directing the voter to confirm the voter's intention to cast the ballot • Notify the voter after the vote has been stored successfully that the ballot

Test Detail	Test Methodology
Test Case Name	**Accuracy**
	has been cast • Notify the voter that the ballot has not been cast successfully if it is not stored successfully, including storage of the ballot image, and provide clear instruction as to the steps the voter should take to cast his or her ballot should this event occur • Provide sufficient computational performance to provide responses back to each voter entry in no more than three seconds • Ensure that the votes stored accurately represent the actual votes cast; • Prevent modification of the voter's vote after the ballot is cast; • Provide a capability to retrieve ballot images in a form readable by humans (in accordance with the requirements of 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: **Opening the Polls Verification**	Verification of the Readiness checklist is performed, ensuring that it is complete. Vendor documentation is reviewed, evaluated and used to create steps that ensure all voting systems and equipment perform voting functions properly. These steps are created, using the guidelines listed in VSS volume 1, section 2.4. Verification of these steps provide a formal record of the following: • Opening the polls • Casting a ballot Additionally, verification ensures that all DRE systems support: • Activating the ballot • Augmenting the election counter • Augmenting the life-cycle counter If necessary, any issues, failures, or unexpected results and their required corrective action(s) are identified and recorded here. **(**V1: 2.4) Verification of Opening Polls for Precinct Count Systems (paper based) ensures: • An internal test of diagnostic capability to verify that all of the polling place tests specified in section 2.3.5 have been successfully completed • Automatic disabling any device that has not been tested until it has been tested. (V1: 2.4.1.1) • A means of verifying that ballot marking devices are properly prepared and ready for use • A voting booth or similar facility, in which the voter may mark the ballot in

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

Test Detail	Test Methodology
Test Case Name	**Accuracy**
	failure of a telecommunications connection within the polling place or between the polling place and any other location. (Vol. 1: 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); and • 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; and • Allows an authorized election official to turn off the capabilities defined above (V1: 2.4.3.2.2) Additionally, verification is performed to ensure that all DRE systems: • Prohibit the voter from accessing or viewing any information on the display screen that has not been authorized by election officials and preprogrammed into the voting system (i.e., no potential for display of external information or linking to other information sources) • Enable the voter to easily identify the selection button or switch, or the active area of the ballot display that is associated with each candidate or ballot measure response • Allow the voter to select his or her preferences on the ballot in any legal number and combination • Indicate that a selection has been made or canceled • Indicate to the voter when no selection, or an insufficient number of selections, has been made in a contest • Prevent the voter from overvoting • Notify the voter when the selection of candidates and measures is completed • Allow the voter, before the ballot is cast, to review his or her choices and, if the voter desires, to delete or change his or her choices before the ballot is cast • For electronic image displays, prompt the voter to confirm the voter's choices before casting his or her ballot, signifying to the voter that casting the ballot is irrevocable and directing the voter to confirm the voter's intention to cast the ballot • Notify the voter after the vote has been stored successfully that the ballot has been cast • Notify the voter that the ballot has not been cast successfully if it is not stored successfully, including storage of the ballot image, and provide clear

Test Detail	Test Methodology
Test Case Name	**Accuracy**
	instruction as to the steps the voter should take to cast his or her ballot should this event occur • Provide sufficient computational performance to provide responses back to each voter entry in no more than three seconds • Ensure that the votes stored accurately represent the actual votes cast; • Prevent modification of the voter's vote after the ballot is cast; • Provide a capability to retrieve ballot images in a form readable by humans (in accordance with the requirements of 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) Verify that all potential ballot positions are active and able to be voted (V1: 2.3.4.2)
Accuracy: Error Rate	Voting system accuracy addresses the accuracy of data for each of the individual ballot positions that could be selected by a voter, including the positions that are not selected. For a voting system, accuracy is defined as the ability of the system to capture, record, store, consolidate and report the specific selections and absence of selections, made by the voter for each ballot position without error. Required accuracy is defined in terms of an error rate that for testing purposes represents the maximum number of errors allowed while processing a specified volume of data. (V1:3.2.1) For all systems, the total number of ballots to be processed by each precinct counting device during these tests reflects the maximum number of active voting positions and the maximum number of ballot styles that the vendor's TDP claims the system can support. (V2:6.2.3, 3.2.6.1.1) The error rate determines the accuracy test vote position processing volume: • Reject: one error before counting 26,997 consecutive ballot positions correctly • Accept: 1,549,703 (or more) consecutive ballot positions are read correctly • If there is one error with more than 26,997 ballot positions but less than 1,549,703 correctly read, continue until another 1,576,701 consecutive ballot positions are counted without error (i.e. Accept: 3,126,404 with one error) 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

Test Detail	Test Methodology
Test Case Name	**Accuracy**
	• 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
Post-Vote: **Closing the Polls**	Vendor documentation is reviewed, evaluated and used to create steps that ensure that all voting systems and equipment perform voting functions properly for all Post-Voting Functions. These steps are created, using the guidelines listed in VSS volum1, section 2.5. Verification of these steps provide a formal record of the following: • All systems provide capabilities to accumulate and report results for the jurisdiction and to generate audit trails • Precinct count systems provide a means to close the polling place including generating appropriate reports • The standards for closing the polling place are specific to precinct count systems. The system provides the means for: (V1:2.5.1) o Preventing the further casting of ballots once the polling place has closed o Providing an internal test that verifies that the prescribed closing procedure has been followed, and that the device status is normal o Incorporating a visible indication of system status o Producing a diagnostic test record that verifies the sequence of events, and indicates that the extraction of voting data has been activated o Precluding the unauthorized reopening of the polls once the poll closing has been completed for that election • All systems provide a means to consolidate vote data from all polling places, and optionally from other sources such as absentee ballots, provisional ballots, and voted ballots requiring human review (e.g., write-in votes). (V1:2.5.2) • All systems are able to create reports summarizing the data on multiple levels. (V1:2.5.3) • *If applicable*, the voting systems offer the capability to make unofficial results available to external organizations such as the news media, political party officials, and others. Although this capability is not required, systems that make unofficial results available: (V1:2.5.4) o Provide only aggregated results, and not data from individual ballots o Provide no access path from unofficial electronic reports or files to the storage devices for official data o Clearly indicate on each report or file that the results it contains are unofficial

Test Detail	Test Methodology
Test Case Name	**Accuracy**
Post-Vote: **Vote Count Verification**	After all voting listed in the Vote Data Matrix is performed, the election data is examined and all counts are validated on the individual voter level, the voting machine level, the precinct level and the central count level. This verification ensures that the system is correctly tabulating all data and is accurately recording cast ballots, including provisional. (V1:2.2.8.1, 2.3.6, 2.5, 3.2.3.1, 3.2.5.2,3.2.6.2.2, 3.2.4.3.3) This tabulation sometimes includes verification of the following: • Ensure undervotes are counted as cast votes • Separate accumulation of Undervotes and Paper Overvotes • Ensure Overvotes are counted on paper ballots and tally correctly
Post-Vote: **Security**	Post-Vote - Security: • System username/password authentication and other access controls are set up according to system documentation guidelines for all devices being tested. • Any/all unnecessary processes are disabled and/or required process control measures noted in the documentation are followed. • All COTS and vendor subsystems used for system security are configured and active as recommended by the system documentation. This includes all connection, port, virus, auditing capability, data or authorized process restriction systems. • Any other system security measures listed in the documentation are followed including setup of additional hardware or software not covered above. Please also see the Documentation section of the Security Test Case within Appendix A.
Post-Vote: **System Audit and Data Retention**	All applicable system reports are produced and verified at this point. The requirements listed in the VSS volume 1 are followed for verifying Data and Document Retention. These include the following: • Data and Document Retention (V1:4.3) • Audit Record Data (V1:4.4) Additionally, the guidelines listed in the VSS volume 1, section 3.2.8.2, are used to validate Data Report Generation.
Results are Observed	Review the outcome of the test(s) against the expected result(s): • **Accept**: expected results is observed • **Reject:** expected result is NOT observed • **Not Testable (NT)**: rejection of a previous test step prevents validation of this step or this was tested in another test case • **Not Applicable (NA):** not applicable to the current test scope or to the component under review • **Not Supported (NS)**: not supported in the current test scope

Test Detail	Test Methodology
Test Case Name	**Accuracy**
Record Observations and all input/outputs for each election	All information used in processing the test case is captured. This includes: inputs, outputs, deviations and any other item that may impact the validation of the test case. Any failure of the test against the EAC guidelines is reported and implies failure of the system. Failures are reported as Defect Issues in the Discrepancy Report and are provided to the manufacturer. Before the final Certification Test Report is issued, manufacturers are given the opportunity to correct all discrepancies. If the manufacturer submits corrections, retests are performed. Issues that do not impact the failure of the requirements but could be considered defects are logged as Informational Issues on the Discrepancy Report. It is the manufacturer's option to address these issues.

Approval Signatures

SysTest Labs:

James M Nilius
Vice President, Compliance Services
February 18, 2008

Client:

Sue Munguia
Director of Certification
February 18, 2008

End of Certification Test Plan