Election Assistance Commission
Voting System Certification Testing

Certification Test Plan

Document Number 06-V-DB-058-CTP-01, Rev 11
October 20, 2008

Prepared for:

Vendor Name	Premier Election Solutions, Inc.
Vendor System	Premier Election Solutions, Inc. ASSURE® 1.2 Voting System
EAC Application No.	DBD0701
Vendor Address	1253 Allen Station Parkway P.O. Box 1019 Allen, TX 75013

Prepared by:

SysTest labs®

216 16th Street Mall
Suite 700
Denver, CO 80202

NVLAP®
NVLAP LAB CODE 200733-0

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

Revision History

Date	Description of Revision	Author	Revision No.
5/24/07	Draft Initial Test Plan – SysTest Labs internal distribution and review	K. Swift, J. Garcia, B. Barkey	Rev 01
6/27/07	Draft Initial Test Plan – SysTest Labs internal distribution and review	D. George, B. Barkey	Rev 02
7/25/07	Initial submission to the EAC	B. Barkey	Rev 03
11/05/07	Updates to Rev 03 based on feedback from the EAC dated 9/06/2007	B. Barkey	Rev 04
12/28/07	Updates to Rev 04 based on feedback from the EAC dated 12/04/2007	B. Barkey, B. Phillips, M. Hilgert, J. Garcia	Rev 05
1/31/2008	Updates to Rev 05 based on feedback from the EAC dated 1/28/2008	B. Barkey, M. Hilgert, M. Santos, J. Diffendaffer	Rev 06
2/18/2008	Updates to Rev 06 based on software version updates, the removal of AVPM II, and corrected VSS references in the Security test case.	M. Hilgert	Rev 07
4/01/2008	Updates to Rev 07 to include information on additional hardware and accuracy testing required by the EAC. This includes hardware test plans and test matrix.	B. Barkey	Rev 08
4/29/2008	Updates to Rev 08 to remove the EMP component from the system configuration.	B. Barkey, M. Hilgert, M. Santos, L. Hoppert	Rev 09
9/26/2008	Updates to Rev 09 coincide with the *Premier ASSURE 1.2 Application for Voting System Testing - Amendment 6* submission to the EAC, along with additional functional changes made by Premier. **Note:** All changes or added sections in this document relating to the above changes are highlighted in yellow. Product names have been corrected to sanctioned product names for accuracy in Figure 1 and Tables 2,3,4 & 5 (these corrections are not highlighted).	M. Hilgert, D. George, M. Santos, B. Barkey	Rev 10
10/20/2008	Added appendix “B” to address RFI’s and NOC’s	M. Santos	Rev 11

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 Premier Election Solutions (Premier) ASSURE 1.2 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.

This test plan:

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

SysTest Labs will provide certification testing on the Premier ASSURE 1.2 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 ASSURE 1.2 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 Premier's System Test & Verification Specification and all of Premier's completed testing to Premier'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, and software, firmware, hardware and system test configurations
- Generation of test cases that ensure that the voting system meets all applicable VSS requirements, appropriate portions of HAVA, and associated Vendor specific requirements
- Traceability and tracking of test cases to VSS requirements, appropriate portions of HAVA, requirements established by the EAC and associated Vendor specific requirements

- Software, Firmware, System, and Hardware test execution
- Reporting of all test results

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

1.1 Certification Test Plan Attachments

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

Attachment A – List of Technical Data Package (TDP) Deliverables – (UPDATED)

Attachment B – Premier Hardware Test Matrix and Notations

Attachment C – List of Source Code Files Reviewed – PROPRIETARY – (UPDATED)

Attachment D – Trace of SysTest Labs' Test Cases to VSS, version 2002

Attachment E-1 – Document Discrepancies Discovered to Date

Attachment E-2 – Functional Discrepancies Discovered to Date

Attachment E-3 – Source Code Discrepancies Discovered to Date - PROPRIETARY

Attachment F – Hardware Test Plans

Attachment G – Hardware Testing Results from Hardware Test Laboratories

1.2 Scope of the ASSURE 1.2 System

This section provides a brief overview of the scope of the Premier ASSURE 1.2 voting system components.

Please note that each of the items listed in Table 1 – Summary of ASSURE 1.2 System Components and Figure 1, ASSURE 1.2 Product Overview are explicitly defined in Table 3 and Table 4. 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 Premier in the TDP items delivered to both SysTest Labs and the EAC.

Table 1 – Summary of ASSURE 1.2 System Components

Software/Firmware	Hardware
Global Election Management System (GEMS®)	PC w/ MS Windows XP/2000/2003 (COTS)
AccuVote®-OS Precinct Count (AccuVote-OS PC)	AccuVote-OS Models A, B, C, D (2002)
AccuVote-OS Central Count (AccuVote-OS CC)	AccuVote-OS Models A, B, C, D (2002) with optional AccuFeed Model A
AccuVote-OSX	AccuVote-OSX Model A (2002) with BootLoader and WinCE 500
BallotStation	AccuVote-TS R6 Model A, B (2002) with BootLoader and WinCE 300 Optional: • Optical Scan Accumulator Adapter (OSAA) Model A (2002) • Universal American Disabilities Association Interface Device (UAID™) Model A (2002)
	AccuVote-TSX Model A, B, C, D (2002) with BootLoader and WinCE 410 Optional: • AccuView Printer® Module (AVPM) Model A (2002) • Optical Scan Accumulator Adapter (OSAA) Model A (2002) • Universal American Disabilities Association Interface Device (UAID™) Model A (2002)
Key Card Tool (KCT)	PC w/ MS Windows 2003/XP (COTS)
VCProgrammer	PC w/ MS Windows 2003/XP (COTS)
Voter Card Encoder (VCE)	Voter Card Encoder (COTS)
ExpressPoll® CardWriter	ExpressPoll 2000 (COTS)
	ExpressPoll 4000 (COTS)
	ExpressPoll 5000 (COTS)
ASSURE Security Manager	PC w/ MS Windows XP (COTS)
Premier Central Scan (PCS)	PC w/ MS Windows XP (COTS)
	AccuVote-OS Model A, B, C, D (2002)
	DRS PhotoScribe PS900 iM2 (COTS) DRS PhotoScribe PS960 (COTS)
AVPM	AVPM Model A
AutoMARK Information Management System (AIMS)	PC w/ MS Windows XP (COTS)
Voter Assist Terminal (VAT)	VAT A100, A200, A300 with WinCE 5.0.0.17

GEMS is a software application used to create the election, lay out the ballots, download the election data to the voting devices, upload the results and produce the final results reports.

AIMS imports the election data created in GEMS and then displays the appropriate ballot information on the VAT, which is an ADA (Americans with Disabilities Act) electronic ballot marking device.

The polling place devices consist of ExpressPoll CardWriter 2000, 4000, and 5000. The ExpressPoll units run EZRoster electronic poll book application to create Voter Cards for the AccuVote-TS R6 and AccuVote-TSX. The ExpressPoll units will be operated on a standalone basis, without any active connection to other devices.

The Voter Card Encoder (VCE) is a small hand-held device that is used to create Voter Cards for the AccuVote-TS R6/TSX. AccuVote-OS and OSX are mark-sense precinct count scanners. With Central Count firmware installed, the AccuVote-OS can be used at the central counting location for the election. PCS is a central tally application that is supported by a variety of scanners, including the DRS PS900 iM2, DRS PS960, and AccuVote-OS with Central Count firmware installed.

1.2.1 Enhancements and Changes for Premier Assure 1.2 (added section)

Premier has provided release notes and change logs to SysTest Labs that include the changes listed in the Amendment 6 submission to the EAC along with additional minor changes. SysTest Labs conducted analysis on all enhancements and changes included in the release notes and change logs to assess the impact of the enhancement or change and identify the applicable testing that will be required for the Assure 1.2 test effort.

The enhancements/changes have been grouped into the following areas based on the analysis:

- New Functionality (Non system level)
- ABasic Reporting
- EMS (System level)
- Tabulation Device (System level)
- Source Code Review
- Trusted Build Process
- Operating System and installation

New Functionality (Non system level)

New Functionality (Non system level) enhancements are defined as enhancements that do not require a full system level test in order to validate. These enhancements are grouped into a New Functionality test case. This New Functionality test case will be created, along with smaller tests, and designed to provide the necessary level of validation; the re-running of a standard system level test case (eg. GEN or PRI) will not be required.

ABasic Reporting

ABasic Reporting enhancements/changes are defined as any enhancement/change that affect the reporting on the individual voting system devices or overall system reporting. All enhancements/changes to the ABasic reporting and reports at the device level will be validated in standard tests (e.g., GEN or PRI). All EMS report changes will be validated at the end of each system level test as part of the overall validation process.

EMS (System level)

EMS enhancements/ changes are defined as any enhancement or change that directly or indirectly affect the creation/layout of election data or ballots, data transmission from or to the EMS, and central tallying. All EMS (GEMS) enhancements/changes will be validated in regression testing of GEN01, GEN02, and GEN03. An analysis of each EMS enhancement/change has been conducted along with what parts of the overall system are being impacted to identify the level of regression testing needed. Based on this analysis the appropriate validation methods will be created in the test case in addition to detailed test steps.

Tabulation Device (System level)

Tabulation device enhancements/changes are defined as any enhancement or change to a device that directly or indirectly may affect the tabulation of votes. All tabulation device enhancements/changes will be validated in regression testing of GEN01, GEN02, and GEN03.

Source Code Review

Source Code Review enhancements/changes are defined as any enhancement or change that can be validated through Source Code Review and does not require functional testing. All Source Code Review enhancements/changes will be validated through the Source Code Review process.

Trusted Build Process

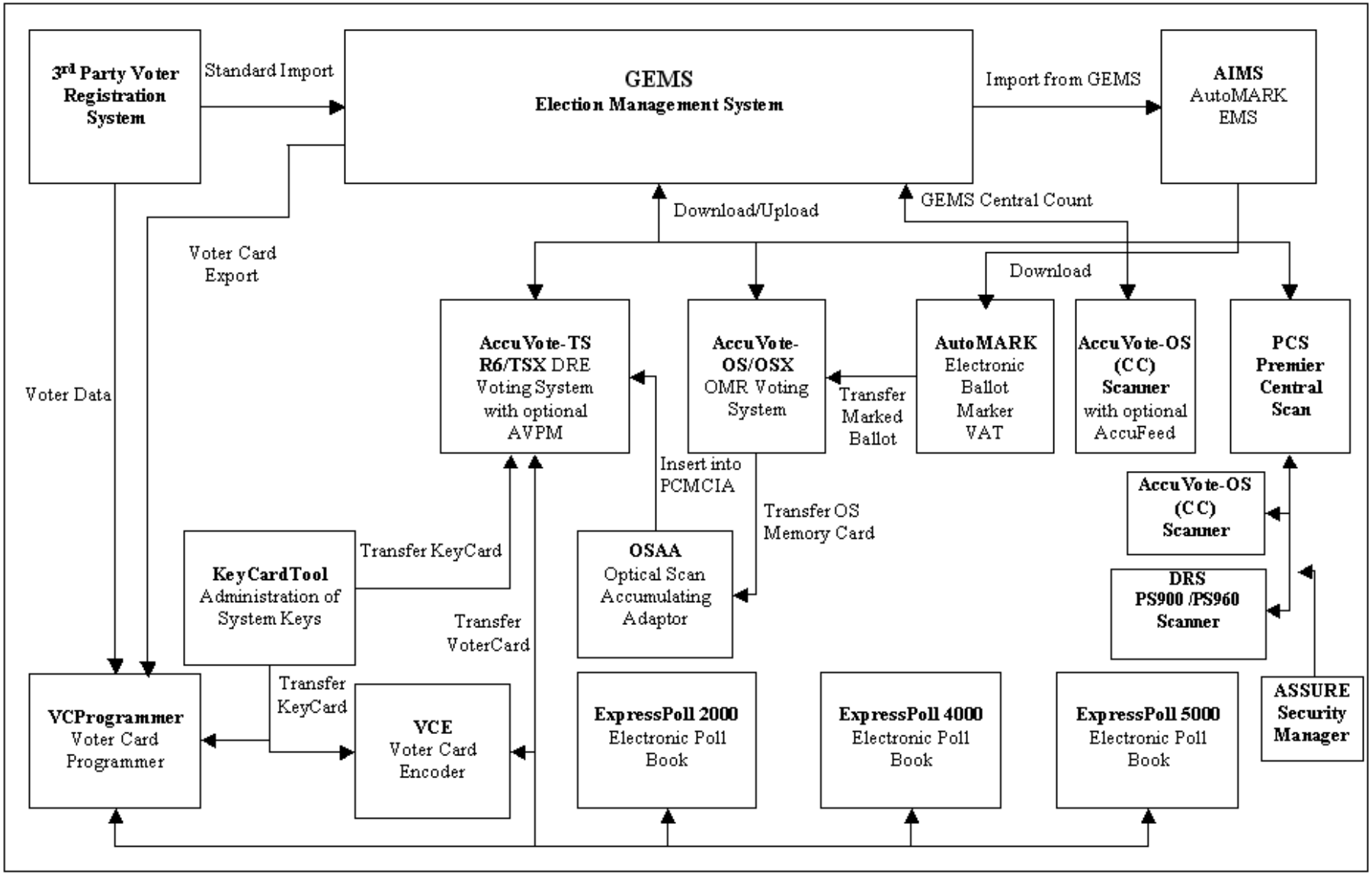
Trusted Build Process enhancements/changes are defined as any enhancement or change to the trusted build process that does not require Source Code Review or functional testing for validation. All Trusted Build Process enhancements will be validated during the Trusted Build process.

Operating System and Installation

Operating System and Installation enhancements/changes are defined as any enhancement or change that affects the installation process or Operating System level. All enhancements/changes that impact these areas will be validated in the installation or operating system upgrade processes.

Note: A detailed matrix of all changes and corresponding test cases will be provided to the EAC for review.

Figure 1 ASSURE 1.2 Product Overview



1.3 Applicable Standards

1.3.1 Applicable Voting System Standards

All testing will determine whether or not the ASSURE 1.2 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. NIST NVLAP Handbook 150-22: 2007
4. EAC Testing and Certification Program Manual, United States Election Assistance Commission, 2006
5. DRAFT – VSTL Accreditation Program Manual DRAFT

1.4 References

1. IEEE Standard for Software Quality Assurance Plans IEEE Std 730-1998, October 20th, 1998.
2. IEEE Standard for Software Configuration Management Plans IEEE Std 828-1998, June 25th, 1998.
3. IEEE Standard for Software Test Documentation IEEE Std 829-1998, December 16th, 1998.
4. IEEE Recommended Practice for Software Requirements Specifications IEEE Std 830-1998, October 20th, 1998.
5. IEEE Standard for Software Unit Testing IEEE Std 1008-1987, December 29th, 1986.
6. IEEE Standard for Software Verification and Validation IEEE Std 1012-1998, July 20th, 1998.
7. ISO 17025
8. SysTest Labs Quality System Manual, Revision 1.0, November 3, 2006.

[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

The following terms and definitions are used throughout this document:

Table 2 – Terms, Abbreviations and Definitions

Term	Abbreviation	Definition
AccuView Printer® Module	AVPM	The AVPM firmware is used to control the take-up motor on the AVPM device.
AccuVote Optical Scan	AccuVote-OS or AVOS	Premier's Optical Scan voting equipment
AccuVote Touch Screen	AccuVote-TS	Premier's Touch Screen Direct Recording Electronic (DRE) voting equipment, AccuVote-TS R6 and AccuVote-TSX.
AutoMARK Information Management System	AIMS	The AIMS software is used to prepare the data for the AutoMARK electronic ballot marker. The AIMS software imports election data from GEMS and allows the user to modify it as necessary for the AutoMARK EBM device.
BootLoader	BL	The BootLoader (BL) is used by the AccuVote-TS R6/AccuVote-TSX/AccuVote-OSX to startup the system, validate the WinCE image and then start Windows CE.
Compact Flash	CF	CF Cards are used in ATS VAT ballot marking devices, and with the ExpressPoll CardWriter.
Direct Recording Electronic	DRE	Touch Screen voting device.
ExpressPoll CardWriter		The ExpressPoll 2000, 4000, and 5000 are small devices that can run the EZRoster electronic poll book application. They also provide the functionality, through the CardWriter software, to be able to create Voter Access Cards for use by the AccuVote-TS R6/ AccuVote-TSX devices.
Global Election Management System	GEMS	GEMS is Premier Election Solutions' Election Management System. This product is used to enter jurisdiction information (district, precincts, languages, etc.) as well as election specific information (races, candidates, voter groups (parties), etc. GEMS is also used to lay out the ballots, download the election data to the voting devices, upload the results and produce the final results reports.
Premier Central Scan	PCS	PCS is a central count software application that downloads the election information from GEMS, scans and tallies ballots, and then uploads the results to GEMS.
Optical Scan Accumulator Adapter	OSAA	OSAA (Optical Scan Accumulator Adapter) is used to accumulate AccuVote-OS results on an AccuVote-TS R6/AccuVote-TSX unit. The OSAA adapter is inserted into the AccuVote-TS R6/ AccuVote-TSX PCMCIA slot and allows the AccuVote-OS memory cards to be read by the AccuVote-TS R6/AccuVote-TSX device.
Technical Data Package	TDP	Functional Requirements, Specifications, End-user documentation, Procedures, System Overview, Configuration Management Plan, Quality Assurance Program, and manuals for each of the required

Term	Abbreviation	Definition
		hardware, software, firmware components of the ASSURE 1.2 voting system.
Universal ADA Interface Device	UAID	The Universal ADA Interface Device (UAID) facilitates accessibility features to further enhance the ability of physically challenged voters to independently and privately make candidate selections and cast ballots.
VCProgrammer		VCProgrammer is a PC based application that is used to create Voter Access Cards for the AccuVote-TS R6/AccuVote-TSX. VCProgrammer can be integrated with 3rd party Voter Registration Systems to allow those systems to create the Voter Access Cards. The VCProgrammer uses a file that is exported from GEMS. When used with a voter registration system, it also requires the data provided by the VR system to create the Voter Access Cards.
Voter Assist Terminal	VAT	The AutoMARK VAT device is used to allow voters to electronically mark a ballot that will be scanned by the AccuVote-OS device. The AutoMARK VAT supports audio ballot as well as visual ballot marking.
Voter Card Encoder	VCE	VCE (Voter Card Encoder) is a small hand-held device that is used to create Voter Access Cards. The VCE is loaded with master Voter Access Card Images and then allows the user to create new Voter Access Cards from those masters.
Key Card Tool	KCT	KCT (Key Card Tool) is a software application that uses a smart card reader to create security keys, Central Administrator cards, and Supervisor cards to be used with Premier components.

2 PRE-CERTIFICATION TESTS

2.1 Pre-Certification Assessment Activities

SysTest Labs has completed an assessment of all initial deliveries of the Technical Data Package, including Functional Requirements, Specifications, End-user documentation, Procedures, System Overview, Configuration Management Plan, Quality Assurance Program, and manuals for each of the required hardware, software, firmware components of the ASSURE 1.2 voting system. For a complete list of all items included in the TDP, please refer to Attachment A. Any subsequent re-deliveries of the TDP items will be solely the result of fixes to discrepancies identified in the FCA, PCA, or test execution activities.

2.1.1 Physical Configuration Audit

2.1.1.1 Document Review

SysTest Labs conducted a PCA review of all documents submitted for review in the initial delivery of the Premier ASSURE 1.2 TDP. These included:

- Functional Requirements
- Design Specifications
- Procedures for User Acceptance Testing
- System Overview
- Configuration Management Plan
- Quality Assurance Program

Each document included in the initial delivery of the Premier ASSURE 1.2 voting system TDP was reviewed for compliance to the VSS, version 2002, Volume 2, Section 6.6. Any subsequent re-reviews of TDP items will be the result of fixes to discrepancies identified in the PCA Document Review activity.

2.1.1.2 Source Code Review

The Premier Election Solutions ASSURE 1.2 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 in the initial delivery of the Premier ASSURE 1.2 voting system TDP. The coding languages for the ASSURE 1.2 voting system include the following:

- C/C++
- VB.NET
- C#

Tools used by SysTest Labs for the source code review include the following:

- **Practiline Line Counter** – a commercial application used to determine the counts of executable and comment lines
- **Module Finder** – a SysTest proprietary application used to parse module names from C/C++ and VB code and populate the resulting module names into the review work documents

- **ExamDiff Pro** – a commercial application used to compare revised code to previously reviewed code
- **KEdit** – a commercial text editor application running a SysTest proprietary macro used to parse module names from Cobol code and populate the identified module names into the review document

Each source code module included in the initial delivery of the Premier ASSURE 1.2 voting system TDP was reviewed for compliance to the VSS, version 2002, Volume 2, Section 6.6. Any subsequent re-reviews of source code will be the result of fixes to discrepancies identified in the PCA Source Code Review activity. Please refer to Attachment C – List of Source Code Files Reviewed–PROPRIETARY for a listing of source code submitted for review as of this writing.

2.1.1.3 Trusted Build

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

- Interviews – Key vendor staff are interviewed to evaluate processes and process conformance in the areas of configuration management and quality assurance.
- Preparation for the Trusted Build - Obtaining and reviewing Premier's procedure for constructing the build platform, verifying the target build platform, and acquiring the necessary materials.
- Execution of the Trusted Build – SysTest Labs will perform the Trusted Build using our step-by-step build procedure. SysTest Labs records and ascertains the following items throughout the build process:
    - Build environment images at various key points
    - Build environment and file hashes at various key points
    - Build environment hardware characteristics
    - Build results from code compilation
    - Final software install files
- Deliverables to Vendor and Testing – Upon completion of the Trusted Build, certain items are sent to the vendor and SysTest Labs' test group. The final result will be a compact disk containing the following:
    - Final software install files
    - Hash values to validate install files
- Final Record Keeping and Archiving Procedures – At the conclusion of the Trusted Build process, SysTest Labs completes all final record keeping and archiving procedures at SysTest Labs' facility. In addition, at this time, we will generate the final media that is submitted to the EAC's approved software repository.
- COTS Operating systems and software used in testing will be verified as authentic for the Trusted Build environment as well as equipment under test. For equipment under test, operating system installations are performed by or witnessed by SysTest Labs

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

2.1.2 Functional Configuration Audit

2.1.2.1 Review of Vendor's Completed Test Cases and Results

SysTest Labs conducted an FCA review of the ASSURE 1.2 test cases delivered as part of the initial delivery of the Premier ASSURE 1.2 voting system TDP. These test cases are designed and executed by Premier for QA and testing of the ASSURE 1.2 voting system. The ASSURE 1.2 test cases were reviewed to determine the scope of testing and conformance to the VSS, version 2002, 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 VSTLs dated December 19, 2007 (please refer to item 1, in Section 1.3.2). The memorandum specifically directs "…any VSTL currently testing a system from one of the manufacturers listed in these reports to review the State reports to see what, if any, items might require a closer look during Federal certification testing." SysTest Labs will review the findings against the VSS, version 2002 requirements, appropriate portions of HAVA, and associated vendor-specific requirements.

2.1.3 Hardware Environmental Testing Assessment

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

- Testing was performed no earlier than January 1, 2005
- 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 and NIST HANDBOOK 150-22: 2007.

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 Premier 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 Premier in a series of iterative discrepancy reports for resolution. All PCA Document Review discrepancies must be corrected by Premier 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 E.1 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 Premier ASSURE 1.2 certification began in November 2006, and is expected to be completed by October of 2008, or earlier. All discrepancies that were encountered during the PCA Source Code Review to date were provided to Premier in a series of iterative discrepancy reports for resolution. All PCA Source Code Review discrepancies must be corrected by Premier 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 E-3 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 from those reviews.

2.2.1.3 Trusted Build

Trusted Builds were performed at both the Vancouver, B.C. offices of Premier Election Solutions, and at the SysTest Labs office in Denver. The first Trusted Build was completed September 7, 2007 in Vancouver, and it resulted in the Trusted Build platform PC, which was used for Trusted Builds of Premier products. Subsequently a separate Trusted Build platform PC was built at the SysTest site for Trusted Builds of the ATS products.

Trusted Builds were then performed with Premier and ATS products, as described under Section 2.1.1 above, on the respective build platforms PCs in order to provide the compiled software and firmware installation packages to be used in the certification testing.

Since source code review has not been fully completed, there will be an additional Trusted Build required. This Trusted Build will be completed and will follow SysTest Labs' Trusted Build process.

2.2.2 Functional Configuration Audit

2.2.2.1 Review of Vendor's Completed Test Cases and Results

SysTest Labs has determined that the initial delivery of the Premier ASSURE 1.2 voting system TDP test cases and subsequent test results are consistent with the VSS, version 2002. All discrepancies in the test cases and test results that were encountered during the FCA were provided to Premier in a series of iterative discrepancy reports for resolution. All discrepancies were corrected by Premier and re-reviewed to ensure that each was fixed per the requirements of the VSS, version 2002. All discrepancies that were encountered during the FCA will be included in the Certification Test Report. Should Premier be required to fix and retest any discrepancies reported by SysTest Labs during the FCA or PCA activities, Premier will re-deliver updated test cases and test results for review by SysTest Labs to the VSS, version 2002.

For all required functions that were identified as not tested or insufficiently tested, SysTest Labs has designed and developed tests cases and will develop a complete set of test data and test procedures. The test cases have been added to SysTest Labs' list of VSTL Test Cases for ASSURE 1.2 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 Premier's ASSURE 1.2 test cases as described below in Section 4 under Sampling Methodology
- SysTest Labs' Gen01 test case
- SysTest Labs' Gen02 test case
- SysTest Labs' Gen03 test case
- SysTest Labs' Pri01 test case
- SysTest Labs' Pri02 test case
- SysTest Labs' Pri03 test case
- SysTest Labs' Security test case
- SysTest Labs' Telecommunications test case
- SysTest Labs' System Accuracy test case

Please see Table 7 – Functional Testing, Table 8 – System Level and Other Functional Testing, Sections, and Appendix A – Test Cases for additional detail on the SysTest Labs test cases.

All discrepancies generated are included in Attachment E-2 as a part of this Certification Test Plan. In addition, all detailed results from the review of the Vendor completed test cases and results and all discrepancies will be included in the Certification Test Report.

2.2.2.2 Review of Ohio and Colorado Voting System Reviews

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

- A summary of the state findings for each system

- How SysTest Labs incorporated (if appropriate) these findings into the test campaign for the ASSURE 1.2 voting system
- The outcome of any additional testing deemed necessary

2.2.3 Hardware Environmental Testing Assessment

Test reports from previous hardware testing performed by accredited NVLAP or A2LA laboratories were analyzed to determine if the results could be accepted for certification (see Attachment G). If the testing met the criteria as defined in 2.1.3 above, it was considered to satisfy the requirements and is then exempted from specific tests. The testing matrix in Attachment B indicates which tests were previously performed, and it includes the name of the hardware test report from the previous accredited laboratory. Additionally, the testing matrix in Attachment B shows which accredited laboratories will be conducting the hardware tests which are now required.

Test Plans for required hardware tests are included in Attachment F to this document.

3 MATERIALS REQUIRED FOR TESTING

3.1 Software

Items identified in the table reflect all software required to perform hardware, software, security and integrated system tests. Note that the software listed with Manufacturer of Premier or ATS is software under test. Should a software version modification become necessary, an amended test plan would be produced with the new version under test listed according to Premier's revised Certification Application, which would have been submitted by Premier as appropriate.

Table 3 – Required Software and Firmware

Item	Mfr.	Version	Test Type
GEMS	Premier	1.21.1	Election Management System – Pre/Post Voting, Election Definition, Ballot Styles, Voting Results Reporting
AccuVote-OS Precinct Count	Premier	1.96.11	Voting – Ballot Scanning
AccuVote-OS Central Count	Premier	2.0.13	Voting – Central Count Ballot Scanning
AccuVote-OSX	Premier	1.2.1	Voting – Ballot Scanning
BallotStation	Premier	4.7.3	Voting – Touchscreen Voting Software
Key Card Tool	Premier	4.7.2	Pre-voting creation of Security Keys, Central Admin Cards, and Supervisor cards
VCProgrammer	Premier	4.7.2	Voter Access Card Activation for Touchscreen Voting According to Voter Registration Information
Voter Card Encoder	Premier	1.3.3	Voter Access Card Creation According to Preconfigured Ballot Styles
ExpressPoll CardWriter	Premier	1.1.6	Electronic Poll Book Function to Create Voter Access Cards for Touchscreen Voting
Premier Central Scan	Premier	2.2.1	Voting - Central Count Ballot Scanning
ASSURE Security Manager	Premier	1.2.1	Controls security & access to the Premier Central Scan (PCS) applications/devices
AutoMARK AIMS	ATS	1.3 (P) (Build 1.3.552)	Pre-Voting Interpretation of GEMS Ballot Style Data To Be Transferred to CF Cards
VAT Firmware	ATS	1.3 PVR (Build 1.3.2925)	Voting on VAT Touchscreen Ballot Marking Devices – Full Featured Version, Including Scanned Ballot Display
VAT Firmware	ATS	1.3 PAVR (Build 1.3.2925)	Voting on VAT Touchscreen Ballot Marking Devices with Audio Ballot Reporting Only

Item	Mfr.	Version	Test Type
BootLoader (BL)	Premier	1.3.10	Voting - Boots and Loads the Operating System and Application Software on the AccuVote-OSX, AccuVote-TS R6 and AccuVote-TSX Touchscreen Machines
WinCE	Premier	300.3.5	Voting – Operating System for the AccuVote-TS R6 Touchscreen Machines
WinCE	Premier	410.3.10	Voting – Operating System for the AccuVote-TSX Touchscreen Machines
WinCE	Premier	500.4.1	Voting – Ballot Scanning on the AccuVote-OSX
AVPM	Premier	3.0.3	Voting – Printing Voter Verifiable Paper Record of Voting on the AccuVote-TSX Touchscreen Machines (AVPM Model A)
ABasic Compiler	Premier	2.2.4	Voting – Facilitates Reporting of Voting Results on AccuVote-OS with GEMS
ABasic Report Files	Premier	2.2.4	Voting – Facilitates Reporting of Voting Results on AccuVote-OS with GEMS
COTS Application(s)	**Mfr**	**Version**	**ASSURE 1.2 Application**
Windows	Microsoft	XP Professional 5.1 Build:2600.xpsp_sp2_gdr.070227-2254 Service Pack 2	Host Operating System for GEMS, Key Card Tool, Premier Central Scan, VCProgrammer, ASSURE Security Manager, AIMS
Windows	Microsoft	2000 Server 5.0 Build: 2195 Service Pack 4	Host Operating System for GEMS
Windows	Microsoft	2003 Server 20070217.021455 Build: No information Service Pack 2	Host Operating System for GEMS, Key Card Tool, VCProgrammer
Windows CE	Applied Data Systems	5.0.0.17	Host Operating System for ATS VAT

3.2 Equipment (Hardware)

Equipment identified in the table reflects all hardware required to perform hardware, software, telecommunications, security and integrated system tests.

Table 4 – Required Hardware

Item	Mfr	Model	HW, O/S, FW, Version	Description of Use
AccuVote-TS R6 (DRE)	Premier	A and B with BootLoader (BL) Optional: OSAA Model A, UAID Model A, VIBS kit	O/S: WinCE 300.3.5 FW: BL 1.3.10, BallotStation 4.7.3	The AccuVote-TS R6 is a DRE device, operated by voters via a touch screen interface. It may be used with optional OSAA, UAID, and VIBS kit (Visually Impaired Ballot Station). The AccuVote-TS R6 has a built-in printer for audit reports but is not AVPM compatible.
AccuVote-TSX (DRE)	Premier	A, B, C, D with BL Optional: OSAA Model A, UAID Model A, AVPM Model A, VIBS kit	O/S: WinCE 410.3.10 FW: BL 1.3.10, BallotStation 4.7.3	The AccuVote-TSX is a Direct Recording Electronic (DRE) touchscreen voting machine. Voting is achieved by inserting a Voter Access Card into the AccuVote-TSX card reader slot, which causes a display of the voter's applicable ballot. The AccuView Printer Module (AVPM) attaches to the AccuVote-TSX unit for printing ballot records, which enable voters to verify their choices before casting their ballots.
AccuVote Optical Scan with Precinct Count firmware	Premier	A, B, C, D	FW: 1.96.11	The AccuVote Optical Scan (OS) is a mark sense ballot counting device, which can be installed with the Precinct Count (PC) firmware or the Central Count (CC) firmware. The AccuVote-OS, installed with the Precinct Count Firmware is used on a stand-alone basis and is loaded with a memory card, which is programmed with the appropriate ballot information. The memory card also contains the tallied results of ballots scanned on the AccuVote-OS.

Item	Mfr	Model	HW, O/S, FW, Version	Description of Use
AccuVote Optical Scan with Central Count firmware	Premier	A, B, C, D Optional: AccuFeed Model A	FW: 2.0.13	The AccuVote-CC (Central Count) is a mark-sense device that is used to scan ballots at a central location. The AccuVote-CC can be used with the GEMS Central Count system or in conjunction with PCS. The AccuVote-CC is the same hardware as the AccuVote-OS but using different firmware (also see the description above). The AccuFeed Model A unit provides automated multi-sheet feeding capability.
AccuVote Optical Scan OSX	Premier	A with BL	O/S: WinCE 500.4.1 FW: BL 1.3.10, OSX 1.2.1	The AccuVote-OSX is a mark sense ballot counting device (also see the AccuVote-OS description above).
Voter Card Encoder (COTS)	Spyrus		FW: 1.3.3	The Voter Card Encoder writes the voter's precinct and party combination and desired voting options (i.e., audio or visual ballot), and encodes this information to a Voter Access Card.
PhotoScribe (COTS)	Data & Research Services, PLC	PS900 iM2, PS960	O/S: Windows XP Professional 5.1 FW: PCS 2.2.1	The PhotoScribe is a high speed/volume scanner and PC. There are two models of the PhotoScribe (PS) units: PhotoScribe PS900 iM2 and the PhotoScribe PS960
ExpressPoll (COTS)	2000– Gotive 4000– Advantech 5000– Advantech	2000, 4000, 5000	FW: 1.1.6	The ExpressPoll 2000, 4000, and 5000 are small devices that can run the EZRoster electronic poll book application. They also provide the functionality, through the CardWriter software, to create Voter Access Cards for use by the AccuVote-TS R6/AccuVote-TSX devices.

Item	Mfr	Model	HW, O/S, FW, Version	Description of Use
VAT Optional: AT device (puff-sip or foot pedal)	AutoMARK	A100, A200, A300	O/S: Windows CE 5.0.0.17 (COTS) FW: 1.3.2925 PVR or 1.3.2925 PAVR AutoMARKData library: 1.3.2925 AIMS: 1.3.552 11/15/2007 Scanner: 1.48 Printer Board: 1.68 SIB: 1.43 Driver: 1.544 Hardware C++ Helper: 1.0.119 Diagnostic Log Library: 1.0.105 Scanner-Printer Library: 1.7.29 Marks Library: 1.3.2 EEPROM Access Library: 1.0.122 Operation Log Library: 1.1.2 Security Library: 1.3.2 Platform: WinCE 5.0.0 Hardware: AM1.0 Manufacturer's Data: Ricoh Electronics, Inc.	The AutoMARK Voter Assist Terminal (VAT) device allows voters to electronically mark a ballot by using the touch screen Braille keypad or an AT (Assistive Technology) device, that is scanned by the AccuVote-OS, AccuVote-OSX, and PhotoScribe devices.
AccuView Printer Module (AVPM)	Premier	Model A	3.0.3	Prints continuous voter-verifiable paper record for the AccuVote-TSX.

Item	Mfr	Model	HW, O/S, FW, Version	Description of Use
PC	COTS		O/S: Windows XP Professional 5.1	GEMS, Key Card Tool, VCProgrammer, Premier Central Scan, ASSURE Security Manager, AIMS
Server	DELL		O/S: Windows XP Professional 5.1 Windows 2000 Server 5.0 Windows 2003 20070217.021455	XP, 2000, 2003: GEMS XP, 2OO3: Key Card Tool, VCProgrammer XP: Premier Central Scan, ASSURE Security Manager
UAID (Universal ADA Interface Device) UAID Controller UAID Switch Kit (3 switches) Sip and Puff Supply Kit			N/A	The UAID (Universal American Disabilities Association Interface Device) provides either a sip and puff, or a switch interface for voters with accessibility issues to vote without assistance. The UAID provides an input box that connects to the back of an AccuVote-TS R6 or AccuVote-TSX unit. The input box may then be connected to either a sip and puff interface or switches. Each interface operates independently.
VIBS kit (headset & pad)			N/A	Provides a handheld keypad interface with the AccuVote-TSX and AccuVote-TS R6. The keypad is a 12-key telephone style layout combined with an RS-232 serial interface.

3.3 Test Materials

Items identified in the table reflect all test materials required to perform hardware, software, telecommunications, security and integrated system tests.

Table 5 – Test Materials

Item	Provided By	Description of Use
Ballots for: VAT, Premier Central Scan, AccuVote-OS and AccuVote-OSX	Premier	Ballots to be tested through mechanized or manual marking and optical scanning.
Ballot Marking Pens	Premier	Specifically recommended pens for marking ballots.
AccuVote-OS control cards	Premier	Control Cards are used to signal to the scanner the beginning and end of a stream of ballots being scanned.
AccuVote-OS keys	Premier	Keys are used to unlock and open the printer access hatch on the AccuVote-OS, and to secure the AccuVote-OS on a ballot box.
AccuVote-OS memory cards	Premier	These cards contain election definition information used for ballot scanning.
AccuVote-TS R6 and AccuVote-TSX audio voting equipment	Premier	Used for ADA accessibility for voters needing audio support, including languages other than English.
AccuVote-TS R6 and AccuVote-TSX keys	Premier	Keys are used to secure openings for memory cards and printer modules.
AccuVote-TS R6 and AccuVote-TSX memory cards	Premier	These cards contain election definition information, and they store vote data from ballot scanning.
Central Administrator cards	Premier	Created by the Key Card Tool application, these cards are used to control supervisor/administrator access to the AccuVote-OSX, AccuVote-TSX, and AccuVote-TS R6 components.
ExpressPoll flash cards	Premier	Compact Flash Cards for the ExpressPoll units contain voter registration data that activates Voter Access Cards.
Compact Flash Cards for the VAT units	AutoMARK	These memory cards contain election/ballot style information for use on the VAT.
VAT Ink Cartridges	AutoMARK	Ink cartridges are used to mark ballots in the VAT.
OSAA units	Premier	The OSAA is an adapter to transfer data between AccuVote-OS memory cards and the AccuVote-TS/TSX Touchscreen machines via the AccuVote-TSX PCMCIA card slot.
Smart card	Premier	The device is used by Key Card Tool primarily to encode security keys to Voter Access Cards and control cards, rather than authenticate these keys. VCProgrammer uses smart card reader.
Smart card readers	Premier	An external device used in conjunction with the Key Card Tool to authenticate a smart card encoded with user-defined security codes or keys.
Supervisor cards	Premier	Created by the Key Card Tool application, these cards are used to control supervisor/administrator access to the AccuVote-OSX and BallotStation.
Voter Access Cards	Premier	Used by voters to vote on the touchscreen units.
Voter Access Card Encoders	Premier	Used to create active Voter Access Cards.
Voter Access Card Encoder battery	Premier	Used to operate the Voter Access Card by battery without a live power connection.

Item	Provided By	Description of Use
Voting booth	Premier	Typically DRE voting booths are considered integral to the DRE devices, particularly the AccuVote-TSX. When we refer explicitly to voting booths, we typically refer to booths used by voters to vote mark-sense paper ballots.
Voting booth Privacy Side Curtain (door) Screen Shield	Premier	Provides voter privacy while voting.
Null Modem Adapter	SysTest	Adapts AVPM firmware loader to Trusted Build PC for firmware installation on DRE units using AVPM.
Laser Printer and USB Cable	SysTest	Laser Printer and cable used to connect to GEMS server for running testing reports.
Paper and Manila Folders	SysTest	For printing reports and organizing paperwork and test ballots.
Headset and Microphone	SysTest	For audio recording of voting information for testing to HAVA/ADA/VSS requirements.
Power Strips	SysTest	Used to provide power connections for multiple devices during testing.

3.4 Deliverable Materials

In addition to the hardware, software and materials identified in Sections 3.1, 0, and 0, Premier delivered the Technical Data Package documents as a part of ASSURE 1.2 voting system. Please see Attachment A for a list of these documents.

3.5 Proprietary Data

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

SysTest Labs' FCA Hardware Environmental Test Assessment established the baseline for hardware configuration required for testing the ASSURE 1.2 voting system. This baseline is shown in Table 4 – Required Hardware and Table 5 – 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

SysTest Labs describes and cross-references the software functions and the test case designs and conditions, per the VSS, version 2002, Subsections A.4.3.3, A.4.3.4, and A.4.3.5 in Sections 4.3.3 - 4.3.7 of this Certification Test Plan describing how each function will be tested.

4.3 Test Case Design

4.3.1 Hardware Qualitative Examination Design

Some hardware testing was performed by a previous ITA/VSTL, Wyle Labs. However, some non-operating and environmental testing (non-operating, operating, and electrical) is the responsibility of SysTest Labs for certain components as outlined in the hardware test matrix Attachment B. The new AccuVote OSX unit also requires full hardware testing. Note that the PCS DRS PhotoScribe PS900 iM2/PS960 product is based upon COTS hardware, so it will undergo the Data Accuracy Test and other Functional Testing.

SysTest Labs reviewed the results provided from the previous ITA/VSTL for overall system capabilities, pre-voting, and voting, and post-voting functions. For untested equipment and system components, SysTest Labs provided the evaluation of the overall system capabilities, pre-voting, voting, and post-voting functions. The ASSURE 1.2 system hardware is incorporated into the standard set of system-level test cases with the augmentation of validation steps specific to each function (*Vol. 2, Section A.4.3.1*).

Regarding the SysTest's hardware testing will be performed at four subcontract laboratories:

- Environmental Testing will be done at Advanced Product Testing (APT) Laboratories in Longmont, Colorado (In lieu of accreditation, APT has been audited for compliance with the appropriate sections of NIST Handbook 150-22.)
- Emissions Testing will be performed at Criterion Laboratories in Rollinsville, Colorado (NVLAP accredited laboratory)

- Safety Testing will be performed at Compliance Integrity Services (CIS) Laboratories in Longmont, Colorado (In lieu of accreditation, CIS has been audited for compliance with the appropriate sections of NIST Handbook 150-22.)
- EMC Integrity (EMCi) is an NVLAP accredited laboratory. EMCi will be used for electrical environmental tests.

In addition:

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

4.3.2 Hardware Environmental Test Case Design

Hardware environmental certification testing for conformance to Volume 1, Section 3 of the VSS, version 2002 is accomplished through a combination of current testing with previous testing performed by a laboratory contracted by Premier, Wyle Laboratories (Wyle Laboratories, Inc., 7800 Highway 20 West, Huntsville, Alabama 80806). Attachment B – Premier Hardware Test Matrix and Notations contains a table summarizing the equipment tested by Wyle and their subcontract laboratory, Nemko USA (802 North Kealy, Lewisville, TX 75057-3136). Attachment B indicates the equipment, testing, VSS Requirement Number, and reference to the lab which performed the test, or notes relating to the testing. Gaps on the Attachment B table indicate equipment and tests that are still needed. As mentioned in the previous section, Maintainability testing and Accessibility and Human Engineering Evaluation testing are required, and will be performed by SysTest Labs at its Denver facility.

The ATS VAT A300 1.3 component has undergone some changes since the testing cited above. For this reason, the following hardware testing is required for those units:

Hardware Test	VSS Section
Maintainability	Volume 2, Sec. 4.7.2
Accessibility & Human Engineering	Volume 1, Sec. 3.4.9 and Sec. 2.2.7.2
Data Accuracy Test	Volume 2, Sec. 4.7.1.1

Otherwise, the testing performed no earlier than January 1, 2005 by the previous labs, Wyle and Nemko, was accepted based upon review of the test results in relation to the VSS requirements, and based upon the accreditation of these labs (*Vol.2, Section A.4.3.2*).

The ATS VAT A100 and A200 components are also being included in this certification event, and they will be included with the A300 in Functional Testing. All three VAT units are software compatible and they will operate with the VAT Firmware Version 1.3 (P) being certified with the ASSURE 1.2 system. The A100 and A200 have been certified previously and therefore will not require additional hardware or environmental testing. The table below illustrates similarities and compatibilities among the three VAT models.

Table 6 – Comparison of AutoMARK VAT A100, A200, A300

#	Technical Feature	A 100	A 200	A 300	Comments
1	Compatible with WinCE 5.0.0.17 and VAT Firmware Version 1.3(P)	Yes	Yes	Yes	All three VAT models are firmware-compatible.
2	Identical Paper Path & Machine Function	Yes	Yes	Yes	
3	ATS Production Phase	I	II	II	Phase II machines are manufactured after March 27, 2006. Engineering Change Order required for A200. Phase II changes were made to improve efficiency and ease of assembly and service over Phase I.
4	A100/A200 vs. A300 Differences – Brand Labeling, Ink Cartridge	Other vendor labeling	Other vendor labeling	Brand neutral ink cartridge, carry case labeling, and CF card label	A100 and A200 are marketed by a competing vendor.
5	Lock/Key Differences			Unique key and lock for power switch and CF card door for Premier	
6	Access Port	Square hole	Square hole	No hole, case solid	
7	Security Seals			Two internal added, one external added	
8	Previous NASED Certification	Yes	Yes	NA	
9	Data Accuracy Test	Tested Under Previous NASED Certification	Accepted under A100 Certification without Data Accuracy Test	To be tested under Premier ASSURE 1.2 certification due to changes in Firmware Version 1.3(P)	Despite the similarity between A100, A200 and A300, Data Accuracy Tests with the Premier VAT firmware will be run on all three models.

4.3.3 Software Module Test Case Design and Data

SysTest Labs reviewed the test case design documents and data as provided by Premier Election Solutions. 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 is 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.

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

SysTest Labs will include in the Certification Test Report a listing of all COTS application files as well as all operating system files in a pre-election configuration, including related hash codes and file signatures.

4.3.4 Software Functional Test Case Design

SysTest Labs' FCA included a detailed review of the functional test case design documents and data as provided by Premier in their TDP against a detailed matrix of system functions and the test cases that exercise them. For all required functions that were identified as not tested or insufficiently tested, SysTest Labs has designed and developed test cases and will develop a complete set of test data and test procedures (procedures specific to the unique steps required to operate the ASSURE 1.2 voting system) prior to 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 Premier's ASSURE 1.2 test cases as described below in Section 4 under Sampling Methodology
- SysTest Labs' GEN01 test case
- SysTest Labs' GEN02 test case
- SysTest Labs' GEN03 test case

- SysTest Labs' PRI 01 test case
- SysTest Labs' PRI02 test case
- SysTest Labs' PRI 03 test case
- SysTest Labs' Security test case
- SysTest Labs' Telecommunications test case
- SysTest Labs' System Accuracy test case

Please see Table 7 – Functional Testing, Table 8 – System Level and Other Functional Testing, Sections 0 - 4.3.7, and Appendix A – Test Cases for additional detail on the SysTest Labs test cases.

Software Functional Testing will demonstrate that the Premier ASSURE 1.2 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 – Functional Testing.

Table 7 – 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.
Before, During & After Processing of Ballots	
b.1. Logic Test – Interpretation of Ballot Styles & recognition of precincts	Verify in Functional Tests: Verify voting variation functionality identified (Vol. 1 Section 2.2.8.2).
b.2. Accuracy Test – 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 functions a., b.4., c.1.-7., d.1.-8.
b.4. Report Generation – Produce test output data	Verify in Functional Tests: Clearing Election Totals 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 Merging Copied Election Results into the Central Count
b 5. Report Generation – Produce audit data	Verify in Functional Tests: System audit reports voting
Polling Place Functions	
c.1. Opening the polls, accepting & counting ballots	Verify in Functional Tests: Zero Reports Scan paper ballots Alerts for over votes and under votes
c.2. Monitoring equipment status	Verify in Functional Tests: Equipment status as identified in user documentation

Function	Test Methodology
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 all systems Audit messages must meet some minimum standards for information contained and clarity/usability of communication. Example: -Each audit message should contain a timestamp at the beginning of the audit trail. -The election identifier and software/firmware releases should be listed. -If the message pertains to results (i.e. inserted, added, deleted), the precinct IDs should be listed. -The number of ballots processed should be stated whenever results are uploaded into the accumulation program.
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: Writing election to media
c.8. Electronic transmission of election data to a central counting location	Verify in Functional Tests: Confirming transmission, receipt, and validity of data interactively and with reports
Central Count Functions	
d.1. Process ballot deck or PMD for >1 precinct	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 response to all voter and poll worker commands as identified in user documentation
d.4. Integration with peripherals equipment or other data processing systems	See b.3.
d.5. Generating real-time audit messages.	See b.3 and b.4.
d.6. Generating precinct-level election data reports	Verify in Functional Tests: Generation of precinct reports
d.7. Generating summary election data reports	See b.4.
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 system's 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). ASSURE 1.2 components subject to the Accuracy Test include the Premier AccuVote-OS CC, AccuVote-OS PC, AccuVote-OSX, AccuVote-TSX, AccuVote-TS R6, DRS PhotoScribe 900 iM2, and the ATS VAT A100, A200 and A300.

Note that the DRS PhotoScribe PS900 iM2 and the PhotoScribe PS960 have identical scanning capabilities and use the same PCS software; and they differ mainly in computer disk capacity. SysTest selected one of models, the PS900, for the Accuracy Test. Both models will undergo all other functional testing.

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

- Create election/ballot definition in GEMS
- Load ballot definition data onto the device being tested via a Compact Flash Card or memory card, or via electronic connection depending on the device being tested
- Generate report of the initialization process
- Display the function selections
- Open polls
- Run 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 GEMS for reporting
- Validate test results

4.3.5.1 Accuracy Testing for Changes for Premier Assure 1.2 (added section)

AccuVote-OSX accuracy test will be re-run due to the modifications to this device. The modifications included error checking on calibration of sensors and CIS heads.

AccuVote-OSX

- GEMS – **1.21.1**
- Firmware – **1.2.1**
- Ballot Type – **Ovals**
- Vote Pattern - **Diagonal**
- # of Contests – **30**
- # of Candidates – **66**
- Ballots per batch – **66**
- Vote Positions per ballot **– 1,980**
- Vote Positions per batch – **130,680**
- # of batches – **12**
- # of times a batch is run - **1**
- Total Vote Positions scanned – **1,568,160**

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 ensure that the voting system meets or exceeds the requirements in the VSS and in 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 Premier ASSURE 1.2 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 Table 7 – Functional Testing, Table 8 – System Level and Other Functional Testing, 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. Table 8 – System Level and Other Functional Testing delineates both the system level and the other software functions to be tested and how they will be tested.

Table 8 – 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
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 Premier	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

SysTest Labs reviewed the system-level and functional test case documents as provided by Premier Election Solutions. SysTest Labs took a sampling of Premier's test cases according to the guideline below.

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

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

SysTest Labs chose the following test cases from Premier's General Election Test Plan.pdf:

1. Creating a Database
22. Voting on AccuVote-TS
25. Processing Ballots in Central Count
27. Audit Reporting from GEMS

These Test Cases cover secure access and data integrity in Test Cases 1 and 22, printing audit logs to show records of action taken during the election in Test Case 27, and tabulating/verifying election results in Test Case 25. All four areas of focus are considered high-risk areas appropriate for sampling.

4.4 EAC Interpretations

This test engagement utilizes only standard VSTL test methods that conform to the EAC Testing and Certification Program Manual and the appropriate voting system standard.

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 Premier Election Solutions.

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 1, 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 will evaluate test results against the documents and software provided by Premier. 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 ASSURE 1.2 voting system. System performance shall be measured against a predicted result.

5.3 Test Data Reduction

SysTest Labs will process the test data by manually recording data in the Test Case records and SysTest Labs templates.

6 TEST PROCEDURE AND CONDITIONS

6.1 Facility Requirements

Testing will be performed on site at SysTest Labs in Colorado. All TDP and test documentation is stored in the 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. Vendor personnel are never left unattended in a voting room at any time.

Environmental hardware testing for hardware components of the ASSURE 1.2 voting system was executed at NVLAP or A2LA accredited environmental hardware testing facilities; also, reports from previous testing are included in Attachment G – Hardware Testing Results from Hardware Test Laboratories.

6.2 Test Setup

Premier's Voting System test platform will be set up, as part of the Physical Configuration Audit, in the standard configuration identified in the Premier TDP documents listed in **Attachment A – TDP Documents Delivered**. The software will be installed, versions verified and made operational. The hardware will also be set up and versions verified according to the Premier TDP documents. Once the hardware and software has 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 the table below.

Table 9 – High-Level Certification Milestones in Sequence

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, staff trained on

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

6.4 Test Operations Procedures

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

An inventory will be performed to verify the voting equipment received contains hardware and software elements as defined by 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 ASSURE 1.2 Discrepancy Report. Issues that do not conform to the requirements of the VSS, version 2002 will be marked as **Documentation Discrepancies** or **Functional Discrepancies** (a discrepancy occurs when the item under test does not meet defined requirements or specifications.). Premier must address all discrepancies prior to issuance of the Certification Report. Issues that are encountered during testing, but are not addressed by the VSS, version 2002 will be added to the Discrepancy report and noted as **Informational**. Premier has the option to address Informational issues. All responses by Premier are noted in the Discrepancy Report attachment to the Certification Report.

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 Premier's manual(s) to create election ballots, vote, and tally, for a General Election.
Variables: Voting Variations	• Ranked Order Voting (Unsupported by GEMS) • Four Districts and Two Precincts: Split Precincts (three splits per precinct) • No Rotation • Non-Partisan contest: Vote for 1 of N • Non-Partisan contest: "Vote for 1" race with a single candidate and a write-in • Non-Partisan contest: "Vote for 1" race with no declared candidates and write-ins • Non-Partisan contest: Multi-member board (N of M) • Non-Partisan contest: Proposition/Question • Partisan contest: Vote for 1 of N • Partisan contest: "Vote for 1" race with a single candidate and a write-in • Partisan contest: "Vote for 1" race with no declared candidates and write-ins • Partisan contest: Multi-member board (N of M) • Partisan contest: One party has no candidates • Slate & Group voting: one selection votes the slate • Recall Type A - Simple Yes/No question • Recall Type B - Retain is first option, followed by Replacement options for second or more
A description of the voting system type and the operational environment	• **GEMS** is the election management system application that runs on a PC using Windows XP Professional, 2000 Server, or 2003 Server. GEMS is the central election definition, ballot definition, vote tabulation, and reporting software for the ASSURE 1.2 system. GEMS also exports data to AIMS. • **AccuVote OS-PC** is an optical scanning device that has its own firmware and uses ABasic for reporting; it is intended for use in a single precinct. • **AccuVote OS-CC** is an optical scanning device that has its own firmware and uses ABasic for reporting; it is intended for use as a central counting scanner, and is able to track election results for multiple precincts or ballot styles. The AccuVote OS-CC also uses the optional AccuFeed Model A multi-ballot feeder.

Test Detail	Test Methodology
Test Case Name	**GEN01**
Standards Documents	Voting System Standards 2002, vol. 1 Voting System Standards 2002, vol. 2 Specific standards are noted in following steps
Pre-requisites and initialization of the test case	• Document the date and tester(s) • System, including the witnessed build, is installed and set up as defined in the user documentation • Define election contests, candidates, issues etc. (V1:2.2.6) • Party affiliation is identified on the ballot • Create a supervisory level access 'user' and password' • 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 • Have a Ballot Counter (V1:2.2.9, 3.2.4.2.6) • Retrieve all supplies necessary for testing • Complete Readiness check list
Documentation of 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 tabs • Save all 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 • A ballot (candidates and propositions) can be accurately/securely defined and formatted (V1:3.2.4.2) • A ballot can be accurately/securely programmed and installed into the vote card (V1:3.2.4.2.4, 3.2.4.2.5)
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, 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	**GEN01**
Testing and Poll Verification	• The election is correctly installed • Status and data reports are generated • Test data is separate from voting data without impact to the testing • Zero count report • A list of all ballot fields is created (V1:3.2.4.2.1) • No hardware/software failures • The voting device is ready to accept votes (V1:3.2.4.2.2, 3.2.4.3.1)
Pre-vote: Opening the Polls Verification	• Completed Readiness check list • Perform proper sequence of functions to open the polls • Identify any issues, failures, or unexpected results and their required corrective action(s)
Voting: Required functionality verifications	• Maintain accurate and complete audit records (V1:2.2.5.2.1, 3.2.7) • Maintain accurate and complete error and status messages (V1:2.2.5.2.2, 2.2.5.2.3, 3.2.1) • Accurately record cast ballots, including provisional (V1:2.4.3, 3.2.3.1, 3.2.5.2, 3.2.6.2.2) • DRE shall record and retain redundant copies of the original ballot image (V1:2.2.2.2, 3.2.4.3.2, 3.2.4.3.3) • Ensure undervotes are counted as cast votes • All paper-based systems shall: Protect the secrecy of the vote throughout the process (V1:2.4.3.2.1, 3.2.4.1) • Separate accumulation of Undervotes and Paper Overvotes • Ensure Overvotes are counted on paper ballots and tally correctly • Maintain integrity of Vote and Audit data • Accurate Definition, Count, Reporting for Election Day, Absentee - paper and DRE, with the results tallied, excluding and including provisional ballots (V1:2.2.2.1, 3.2.8.2) • Write-in voting: Voting position identified for write-ins (V1:3.2.5.1.3) • Correctly tabulate (V1:2.2.8.1) • Provisional/Challenged ballots - Note vendor supported tabulation of these ballots at Central Count • Overvotes (V1:3.2.5.1.3) • Undervotes (V1:3.2.5.1.3) • Blank ballots (V1:3.2.5.1.3)

Test Detail	Test Methodology
Test Case Name	**GEN01**
Voting: Optional functionality verifications	• Ranked Order Voting (Unsupported by GEMS) • Four Districts and Two Precincts: Split Precincts (three splits per precinct) • No Rotation • Non-Partisan contest: Vote for 1 of N • Non-Partisan contest: "Vote for 1" race with a single candidate and a write-in • Non-Partisan contest: "Vote for 1" race with no declared candidates and write-ins • Non-Partisan contest: Multi-member board (N of M) • Non-Partisan contest: Proposition/Question • Partisan contest: Vote for 1 of N • Partisan contest: "Vote for 1" race with a single candidate and a write-in • Partisan contest: "Vote for 1" race with no declared candidates and write-ins • Partisan contest: Multi-member board (N of M) • Partisan contest: One party has no candidates • Slate & Group voting: One selection votes the slate • Recall Type A - Simple Yes/No question • Recall Type B - Retain is first option, followed by Replacement options for second or more
Post-Vote: Closing the Polls	• Polls are properly closed • Further casting of ballots and reopening of the polls is prohibited • Device status is normal • Identify any issues, failures, or unexpected results and their required corrective action(s) • Create a test record that verifies the sequence of test events
Post-Vote: Central Count	Capture, document, and verify all counts
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, 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	**GEN01**
Post-Vote: System 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 • **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 report is issued, manufacturers are given the opportunity to correct all discrepancies • If corrections are submitted by the manufacturer, 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 Premier's manual(s) to create election ballots, vote, and tally, for a General Election: Straight Party
Variables: Voting Variations	• This is a two-page ballot election per voter • Four Districts, Seven Precincts • No Split Precincts- Ballot Rotation by Precinct • Cumulative voting ***UNSUPPORTED BY GEMS • Straight party (multi-member board) • Non-Partisan contest: Vote for 1 of N • Non-Partisan contest: "Vote for 1" race with a single candidate and a write-in • Non-Partisan contest: "Vote for 1" race with no declared candidates and write-ins • Non-Partisan contest: Multi-member board (N of M) • Non-Partisan contest: Proposition/Question • Partisan contest: Vote for 1 of N • Partisan contest: "Vote for 1" race with a single candidate and a write-in • Partisan contest: "Vote for 1" race with no declared candidates and write-ins • Partisan contest: Multi-member board (N of M) • Partisan contest: One party has no candidates • Partisan contest: Cross over to another partisan ballot • Slate & Group voting: One selection votes the slate • Recall Type A - Simple Yes/No question • Recall Type B - Retain is first option, followed by Replacement options for second or more

Test Detail	Test Methodology
Test Case Name	**GEN02 (Straight Party)**
A description of the voting system type and the operational environment	• **GEMS** – See GEN01 • **BallotStation** firmware is used for the Premier touch screen voting machines to provide the functions necessary to present the correct ballot style, accumulate vote data, accommodate disabled voters, and transfer election and voting data from and to GEMS. • **AccuVote-TSX** is the accessible touch screen voting unit which runs the BallotStation firmware application as described above, and it uses the WinCE 410 operating system and BootLoader firmware. • **AVPM** is an optional printer module that attaches to the AccuVote-TSX and provides a printed voting record on paper that may be viewed by the voter. The AVPM is driven by AVPM firmware installed on the TSX units. • **OSAA** is an adapter that fits into PCMCIA card slot of the touch screen voting machines, and it accommodates the memory cards used to transfer results from the AccuVote OS units to touch screen machine. This adapter has no software or firmware and does not store information. • **KeyCard Tool** is used to activate supervisor and administrator cards and security keys for the touch screen machines. The KeyCard Tool software application runs on a PC with Windows XP Professional. • **ExpressPoll 2000, 4000, 5000** run the ExpressPoll CardWriter firmware. These units are used to retrieve voter registration data and activate voter access cards for the touch screen voting machines. These units will be tested on a standalone basis, i.e. without active connection other devices.
Standards Documents	Voting System Standards 2002, vol. 1 Voting System Standards 2002, vol. 2 Specific standards are noted in following steps
Pre-requisites and initialization of the test case	• Document the date and tester(s) • System, including the witnessed build, is installed and set up as defined in the user documentation • Define election contests, candidates, issues etc. (V1:2.2.6) • Party affiliation is identified on the ballot • Create a supervisory level access 'user' and password' • 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 • Have a Ballot Counter (V1:2.2.9, 3.2.4.2.6) • Retrieve all supplies necessary for testing • Complete Readiness check list

Test Detail	Test Methodology
Test Case Name	**GEN02 (Straight Party)**
Documentation of 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 tabs • Save all 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 • A ballot (candidates and propositions) can be accurately/securely defined and formatted (V1:3.2.4.2) • A ballot can be accurately/securely programmed and installed into the vote card (V1:3.2.4.2.4, 3.2.4.2.5)
Pre-vote: Ballot 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, 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	• The election is correctly installed • Status and data reports are generated • Test data is separate from voting data without impact to the testing • Zero count report • A list of all ballot fields is created (V1:3.2.4.2.1) • No hardware/software failures • The voting device is ready to accept votes (V1:3.2.4.2.2, 3.2.4.3.1)
Pre-vote: Opening the Polls Verification	• Completed Readiness check list • Perform proper sequence of functions to open the polls • Identify any issues, failures, or unexpected results and their required corrective action(s)

Test Detail	Test Methodology
Test Case Name	**GEN02 (Straight Party)**
Voting: Required functionality verifications	• Maintain accurate and complete audit records (V1:2.2.5.2.1, 3.2.7) • Maintain accurate and complete error and status messages (V1:2.2.5.2.2, 2.2.5.2.3, 3.2.1) • Accurately record cast ballots, including provisional (V1:2.4.3, 3.2.3.1, 3.2.5.2, 3.2.6.2.2) • DRE shall record and retain redundant copies of the original ballot image (V1:2.2.2.2, 3.2.4.3.2, 3.2.4.3.3) • Ensure undervotes are counted as cast votes • All paper-based systems shall: Protect the secrecy of the vote throughout the process (V1:2.4.3.2.1, 3.2.4.1) • Separate accumulation of Undervotes and Paper Overvotes • Ensure Overvotes are counted on paper ballots and tally correctly • Maintain integrity of Vote and Audit data • Accurate Definition, Count, Reporting for Election Day, Absentee - paper and DRE, with the results tallied, excluding and including provisional ballots (V1:2.2.2.1, 3.2.8.2) • Write-in voting: Voting position identified for write-ins (V1:3.2.5.1.3) • Correctly tabulate (V1:2.2.8.1) • Provisional/Challenged ballots - Note vendor supported tabulation of these ballots at Central Count • Overvotes (V1:3.2.5.1.3) • Undervotes (V1:3.2.5.1.3) • Blank ballots (V1:3.2.5.1.3)
Voting: Optional functionality verifications	• This is a two-page ballot election per voter • Four Districts, Seven Precincts • No Split Precincts- Ballot Rotation by Precinct • Cumulative voting ***UNSUPPORTED BY GEMS • Straight party (multi-member board) • Non-Partisan contest: Vote for 1 of N • Non-Partisan contest: "Vote for 1" race with a single candidate and a write-in • Non-Partisan contest: "Vote for 1" race with no declared candidates and write-ins • Non-Partisan contest: Multi-member board (N of M) • Non-Partisan contest: Proposition/Question • Partisan contest: Vote for 1 of N • Partisan contest: "Vote for 1" race with a single candidate and a write-in • Partisan contest: "Vote for 1" race with no declared candidates and write-ins • Partisan contest: Multi-member board (N of M) • Partisan contest: One party has no candidates • Partisan contest: Cross over to another partisan ballot • Slate & Group voting: one selection votes the slate

Test Detail	Test Methodology
Test Case Name	**GEN02 (Straight Party)**
	• Recall Type A - Simple Yes/No question • Recall Type B - Retain is first option, followed by Replacement options for second or more
Post-Vote: Closing the Polls	• Polls are properly closed • Further casting of ballots and reopening of the polls is prohibited • Device status is normal • Identify any issues, failures, or unexpected results and their required corrective action(s) • Create a test record that verifies the sequence of test events
Post-Vote: Central Count	Capture, document, and verify all counts
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, 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.
Post-Vote: System 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 • **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 report is issued, manufacturers are given the opportunity to correct all discrepancies • If corrections are submitted by the manufacturer, 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 (Multi-Language & 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 Premier's manual(s) to create election ballots, vote, and tally, for a General Election: Multi-Language & Accessibility
Variables: Voting Variations	• Accessibility: Privacy, secrecy, and integrity demands of the FEC VSS (V1:2.2.7) • Accessibility: Common standards - reach, obstruction, protrusion, operable controls, ADA standards (V1:2.2.7.1) • Accessibility: DRE standards - Audio, headsets, FCC Part 68, ANSI C63.19-2001 Category 4, Settings (contrast, color, size, volume), touch screen, sound cues, biometrics, dexterity (V1:2.2.7.2) • One District, One Precinct • Non-Partisan contest: Vote for 1 of N • Non-Partisan contest: "Vote for 1" race with a single candidate and a write-in • Non-Partisan contest: "Vote for 1" race with no declared candidates and write-ins • Non-Partisan contest: Multi-member board (N of M) • Partisan contest: Vote for 1 of N • Partisan contest: "Vote for 1" race with a single candidate and a write-in • Partisan contest: "Vote for 1" race with no declared candidates and write-ins • Partisan contest: Multi-member board (N of M) • Partisan contest: One party has no candidates • Non-Partisan contest: Proposition/Question • Slate & Group voting: one selection votes the slate • Multi-language ballots. Languages being tested: o English (Default), Chinese (using traditional form), Filipino/Tagalog, French, Haitian Creole, Japanese, Korean, Spanish, Vietnamese • Audio Ballots • Straight Party by contest, if supported (City Council)

Test Detail	Test Methodology
Test Case Name	**GEN03 (Multi-Language & Accessibility)**
A description of the voting system type and the operational environment	• **GEMS** – See GEN01 • **AIMS** runs on a PC with Windows XP Professional and is used to import election data from GEMS and then transfer the election (i.e. ballot style) data to Compact Flash (CF) cards for use in the VAT units. • **VAT A100/A200/A300** – Voter Assist Terminals are accessible touch screen ballot marking devices. All three listed models are tested, and all three use the same VAT firmware and WinCE 5.0.0.17 (COTS) operating system. • **BallotStation** – See GEN02 • **AccuVote-TSX** – See GEN02 • **AccuVote-TS R6** is an accessible touch screen voting machine running the BallotStation application, WinCE 300 operating system, and BootLoader firmware. • **KeyCard Tool** – See GEN02
Standards Documents	Voting System Standards 2002, vol. 1 Voting System Standards 2002, vol. 2 Specific standards are noted in following steps
Pre-requisites and initialization of the test case	• Document the date and tester(s) • System, including the witnessed build, is installed and set up as defined in the user documentation • Define election contests, candidates, issues etc. (V1:2.2.6) • Party affiliation is identified on the ballot • Create a supervisory level access 'user' and password' • 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 • Have a Ballot Counter (V1:2.2.9, 3.2.4.2.6) • Retrieve all supplies necessary for testing • Complete Readiness check list
Documentation of 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 tabs • Save all 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 • A ballot (candidates and propositions) can be accurately/securely defined and formatted (V1:3.2.4.2) • A ballot can be accurately/securely programmed and installed into the vote card (V1:3.2.4.2.4, 3.2.4.2.5)

Test Detail	Test Methodology
Test Case Name	**GEN03 (Multi-Language & Accessibility)**
Pre-vote: System Preparation - Security	System Preparation - Security: • System username/password authentication and other access controls are set up according to system documentation guidelines for all devices being tested. • Any/all unnecessary processes are disabled and/or required process control measures noted in the documentation are followed. • All COTS and vendor subsystems used for system security are configured and active as recommended by the system documentation. This includes all connection, port, virus, 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	• The election is correctly installed • Status and data reports are generated • Test data is separate from voting data without impact to the testing • Zero count report • A list of all ballot fields is created (V1:3.2.4.2.1) • No hardware/software failures • The voting device is ready to accept votes (V1:3.2.4.2.2, 3.2.4.3.1)
Pre-vote: Opening the Polls Verification	• Completed Readiness check list • Perform proper sequence of functions to open the polls • Identify any issues, failures, or unexpected results and their required corrective action(s)

Test Detail	Test Methodology
Test Case Name	**GEN03 (Multi-Language & Accessibility)**
Voting: Required functionality verifications	• Maintain accurate and complete audit records (V1:2.2.5.2.1, 3.2.7) • Maintain accurate and complete error and status messages (V1:2.2.5.2.2, 2.2.5.2.3, 3.2.1) • Accurately record cast ballots, including provisional (V1:2.4.3, 3.2.3.1, 3.2.5.2, 3.2.6.2.2) • DRE shall record and retain redundant copies of the original ballot image (V1:2.2.2.2, 3.2.4.3.2, 3.2.4.3.3) • Ensure undervotes are counted as cast votes • All paper-based systems shall: Protect the secrecy of the vote throughout the process (V1:2.4.3.2.1, 3.2.4.1) • Separate accumulation of Undervotes and Paper Overvotes • Ensure Overvotes are counted on paper ballots and tally correctly • Maintain integrity of Vote and Audit data • Accurate Definition, Count, Reporting for Election Day, Absentee - paper and DRE, with the results tallied, excluding and including provisional ballots (V1:2.2.2.1, 3.2.8.2) • Write-in voting: Voting position identified for write-ins (V1:3.2.5.1.3) • Correctly tabulate (V1:2.2.8.1) • Provisional/Challenged ballots - Note vendor supported tabulation of these ballots at Central Count • Overvotes (V1:3.2.5.1.3) • Undervotes (V1:3.2.5.1.3) • Blank ballots (V1:3.2.5.1.3)

Test Detail	Test Methodology
Test Case Name	**GEN03 (Multi-Language & Accessibility)**
Voting: Optional functionality verifications	• Accessibility: Privacy, secrecy, and integrity demands of the FEC VSS (V1:2.2.7) • Accessibility: Common standards - reach, obstruction, protrusion, operable controls, ADA standards (V1:2.2.7.1) • Accessibility: DRE standards - Audio, headsets, FCC Part 68, ANSI C63.19-2001 Category 4, Settings (contrast, color, size, volume), touch screen, sound cues, biometrics, dexterity (V1:2.2.7.2) • One District, One Precinct • Non-Partisan contest: Vote for 1 of N • Non-Partisan contest: "Vote for 1" race with a single candidate and a write-in • Non-Partisan contest: "Vote for 1" race with no declared candidates and write-ins • Non-Partisan contest: Multi-member board (N of M) • Partisan contest: Vote for 1 of N • Partisan contest: "Vote for 1" race with a single candidate and a write-in • Partisan contest: "Vote for 1" race with no declared candidates and write-ins • Partisan contest: Multi-member board (N of M) • Partisan contest: One party has no candidates • Non-Partisan contest: Proposition/Question • Slate & Group voting: one selection votes the slate • Multi-language ballots. Languages being tested: o English (Default), Chinese (using traditional form), Filipino/Tagalog, French, Haitian Creole, Japanese, Korean, Spanish, Vietnamese • Audio Ballots • Straight Party by contest, if supported (City Council)
Post-Vote: Closing the Polls	• Polls are properly closed • Further casting of ballots and reopening of the polls is prohibited • Device status is normal • Identify any issues, failures, or unexpected results and their required corrective action(s) • Create a test record that verifies the sequence of test events
Post-Vote: Central Count	Capture, document, and verify all counts

Test Detail	Test Methodology
Test Case Name	**GEN03 (Multi-Language & 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, 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.
Post-Vote: System 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 • **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 report is issued, manufacturers are given the opportunity to correct all discrepancies • If corrections are submitted by the manufacturer, 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 Premier's manual(s) to create election ballots, vote, and tally, for a Primary Election: Open Primary
Variables: Voting Variations	• One District, One Precinct • Non-Partisan contest: Vote for 1 of N • Non-Partisan contest: "Vote for 1" race with a single candidate and a write-in • Non-Partisan contest: "Vote for 1" race with no declared candidates and write-ins • Non-Partisan contest: Multi-member board (N of M) • Partisan contest: Vote for 1 of N • Partisan contest: "Vote for 1" race with no declared candidates and write-ins • Partisan contest: Multi-member board (N of M) • Partisan contest: One party has no candidates • Primary Presidential Nominations: List only the nominees, not the delegates
A description of the voting system type and the operational environment	• **GEMS** – See GEN01 • **AIMS** – See GEN03 • **VAT A100/A200/A300** – See GEN03 • **PCS 900/960** is a high-speed ballot scanning device which uses PCS software running on an integrated PC with Windows XP Professional • **AccuVote OSX** is an optical scanner which uses BootLoader, ABasic, WinCE 500, and its own OSX firmware.
Standards Documents	Voting System Standards 2002, vol. 1 Voting System Standards 2002, vol. 2 Specific standards are noted in following steps

Test Detail	Test Methodology
Test Case Name	**PRI01 (Open Primary)**
Pre-requisites and initialization of the test case	• Document the date and tester(s) • System, including the witnessed build, is installed and set up as defined in the user documentation • Define election contests, candidates, issues etc. (V1:2.2.6) • Party affiliation is identified on the ballot • Create a supervisory level access 'user' and password' • 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 • Have a Ballot Counter (V1:2.2.9, 3.2.4.2.6) • Retrieve all supplies necessary for testing • Complete Readiness check list
Documentation of 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 tabs • Save all 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 • A ballot (candidates and propositions) can be accurately/securely defined and formatted (V1:3.2.4.2) • A ballot can be accurately/securely programmed and installed into the vote card (V1:3.2.4.2.4, 3.2.4.2.5)
Pre-vote: System Preparation - Security	System Preparation - Security: • System username/password authentication and other access controls are set up according to system documentation guidelines for all devices being tested. • Any/all unnecessary processes are disabled and/or required process control measures noted in the documentation are followed. • All COTS and vendor subsystems used for system security are configured and active as recommended by the system documentation. This includes all connection, port, virus, 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	**PRI01 (Open Primary)**
Testing and Poll Verification	• The election is correctly installed • Status and data reports are generated • Test data is separate from voting data without impact to the testing • Zero count report • A list of all ballot fields is created (V1:3.2.4.2.1) • No hardware/software failures • The voting device is ready to accept votes (V1:3.2.4.2.2, 3.2.4.3.1)
Pre-vote: Opening the Polls Verification	• Completed Readiness check list • Perform proper sequence of functions to open the polls • Identify any issues, failures, or unexpected results and their required corrective action(s)
Voting: Required functionality verifications	• Maintain accurate and complete audit records (V1:2.2.5.2.1, 3.2.7) • Maintain accurate and complete error and status messages (V1:2.2.5.2.2, 2.2.5.2.3, 3.2.1) • Accurately record cast ballots, including provisional (V1:2.4.3, 3.2.3.1, 3.2.5.2, 3.2.6.2.2) • DRE shall record and retain redundant copies of the original ballot image (V1:2.2.2.2, 3.2.4.3.2, 3.2.4.3.3) • Ensure undervotes are counted as cast votes • All paper-based systems shall: Protect the secrecy of the vote throughout the process (V1:2.4.3.2.1, 3.2.4.1) • Separate accumulation of Undervotes and Paper Overvotes • Ensure Overvotes are counted on paper ballots and tally correctly • Maintain integrity of Vote and Audit data • Accurate Definition, Count, Reporting for Election Day, Absentee - paper and DRE, with the results tallied, excluding and including provisional ballots (V1:2.2.2.1, 3.2.8.2) • Write-in voting: Voting position identified for write-ins (V1:3.2.5.1.3) • Correctly tabulate (V1:2.2.8.1) • Provisional/Challenged ballots - Note vendor supported tabulation of these ballots at Central Count • Overvotes (V1:3.2.5.1.3) • Undervotes (V1:3.2.5.1.3) • Blank ballots (V1:3.2.5.1.3)

Test Detail	Test Methodology
Test Case Name	**PRI01 (Open Primary)**
Voting: Optional functionality verifications	• One District, One Precinct • Non-Partisan contest: Vote for 1 of N • Non-Partisan contest: "Vote for 1" race with a single candidate and a write-in • Non-Partisan contest: "Vote for 1" race with no declared candidates and write-ins • Non-Partisan contest: Multi-member board (N of M) • Partisan contest: Vote for 1 of N • Partisan contest: "Vote for 1" race with no declared candidates and write-ins • Partisan contest: Multi-member board (N of M) • Partisan contest: One party has no candidates • Primary Presidential Nominations: List only the nominees, not the delegates
Post-Vote: Closing the Polls	• Polls are properly closed • Further casting of ballots and reopening of the polls is prohibited • Device status is normal • Identify any issues, failures, or unexpected results and their required corrective action(s) • Create a test record that verifies the sequence of test events
Post-Vote: Central Count	Capture, document, and verify all counts
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, 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.
Post-Vote: System Audit	Produce and verify available system reports

Test Detail	Test Methodology
Test Case Name	**PRI01 (Open Primary)**
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 • **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 report is issued, manufacturers are given the opportunity to correct all discrepancies • If corrections are submitted by the manufacturer, 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 Premier's manual(s) to create election ballots, vote, and tally, for a Primary Election: Closed Primary
Variables: Voting Variations	• Five Districts, Seven Precincts • No Rotation • Non-Partisan contest: Vote for 1 of N • Partisan contest: Vote for 1 of N • Partisan contest: Cross over to another partisan ballot if no declared candidate • Partisan contest: Multi-member board (N of M) • Partisan contest: One party has no candidates • Primary Presidential Delegates: A delegate slate, display of delegates with nominees • Recall Type D
A description of the voting system type and the operational environment	• **GEMS** – See GEN01 • **BallotStation** – See GEN02 • **AccuVote-TS R6** – See GEN03 • **KeyCard Tool** – See GEN02 • **OSAA** – See GEN02 • **VCProgrammer** the Voter Card Programmer is used to encode voter access cards for use with the touch screen voting machines. It runs on a PC with the Windows XP Professional operating system.
Standards Documents	Voting System Standards 2002, vol. 1 Voting System Standards 2002, vol. 2 Specific standards are noted in following steps

Test Detail	Test Methodology
Test Case Name	**PRI02 (Closed Primary)**
Pre-requisites and initialization of the test case	• Document the date and tester(s) • System, including the witnessed build, is installed and set up as defined in the user documentation • Define election contests, candidates, issues etc. (V1:2.2.6) • Party affiliation is identified on the ballot • Create a supervisory level access 'user' and password' • 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 • Have a Ballot Counter (V1:2.2.9, 3.2.4.2.6) • Retrieve all supplies necessary for testing • Complete Readiness check list
Documentation of 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 tabs • Save all 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 • A ballot (candidates and propositions) can be accurately/securely defined and formatted (V1:3.2.4.2) • A ballot can be accurately/securely programmed and installed into the vote card (V1:3.2.4.2.4, 3.2.4.2.5)
Pre-vote: System Preparation - Security	System Preparation - Security: • System username/password authentication and other access controls are set up according to system documentation guidelines for all devices being tested. • Any/all unnecessary processes are disabled and/or required process control measures noted in the documentation are followed. • All COTS and vendor subsystems used for system security are configured and active as recommended by the system documentation. This includes all connection, port, virus, 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	**PRI02 (Closed Primary)**
Testing and Poll Verification	• The election is correctly installed • Status and data reports are generated • Test data is separate from voting data without impact to the testing • Zero count report • A list of all ballot fields is created (V1:3.2.4.2.1) • No hardware/software failures • The voting device is ready to accept votes (V1:3.2.4.2.2, 3.2.4.3.1)
Pre-vote: Opening the Polls Verification	• Completed Readiness check list • Perform proper sequence of functions to open the polls • Identify any issues, failures, or unexpected results and their required corrective action(s)
Voting: Required functionality verifications	• Maintain accurate and complete audit records (V1:2.2.5.2.1, 3.2.7) • Maintain accurate and complete error and status messages (V1:2.2.5.2.2, 2.2.5.2.3, 3.2.1) • Accurately record cast ballots, including provisional (V1:2.4.3, 3.2.3.1, 3.2.5.2, 3.2.6.2.2) • DRE shall record and retain redundant copies of the original ballot image (V1:2.2.2.2, 3.2.4.3.2, 3.2.4.3.3) • Ensure undervotes are counted as cast votes • All paper-based systems shall: Protect the secrecy of the vote throughout the process (V1:2.4.3.2.1, 3.2.4.1) • Separate accumulation of Undervotes and Paper Overvotes • Ensure Overvotes are counted on paper ballots and tally correctly • Maintain integrity of Vote and Audit data • Accurate Definition, Count, Reporting for Election Day, Absentee - paper and DRE, with the results tallied, excluding and including provisional ballots (V1:2.2.2.1, 3.2.8.2) • Write-in voting: Voting position identified for write-ins (V1:3.2.5.1.3) • Correctly tabulate (V1:2.2.8.1) • Provisional/Challenged ballots - Note vendor supported tabulation of these ballots at Central Count • Overvotes (V1:3.2.5.1.3) • Undervotes (V1:3.2.5.1.3) • Blank ballots (V1:3.2.5.1.3)

Test Detail	Test Methodology
Test Case Name	**PRI02 (Closed Primary)**
Voting: Optional functionality verifications	• Five Districts, Seven Precincts • No Rotation • Non-Partisan contest: Vote for 1 of N • Partisan contest: Vote for 1 of N • Partisan contest: Cross over to another partisan ballot if no declared candidate • Partisan contest: Multi-member board (N of M) • Partisan contest: One party has no candidates • Primary Presidential Delegates: A delegate slate, display of delegates with nominees • Recall Type D
Post-Vote: Closing the Polls	• Polls are properly closed • Further casting of ballots and reopening of the polls is prohibited • Device status is normal • Identify any issues, failures, or unexpected results and their required corrective action(s) • Create a test record that verifies the sequence of test events
Post-Vote: Central Count	Capture, document, and verify all counts
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, 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.
Post-Vote: System Audit	Produce and verify available system reports

Test Detail	Test Methodology
Test Case Name	**PRI02 (Closed Primary)**
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 • **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 report is issued, manufacturers are given the opportunity to correct all discrepancies • If corrections are submitted by the manufacturer, 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	**PRI03 (Blanket 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 Premier's manual(s) to create election ballots, vote, and tally, for a Primary Election: Blanket Open Primary
Variables: Voting Variations	• One District, One Precinct • No Rotation • Non-Partisan contest: Vote for 1 of N • Non-Partisan contest: "Vote for 1" race with a single candidate and a write-in • Non-Partisan contest: "Vote for 1" race with no declared candidates and write-ins • Non-Partisan contest: Multi-member board (N of M) • Partisan contest: Vote for 1 of N • Partisan contest: "Vote for 1" race with no declared candidates and write-ins • Partisan contest: Multi-member board (N of M) • Partisan contest: One party has no candidates • Primary Presidential Nominations: List only the nominees, not the delegates
A description of the voting system type and the operational environment	• **GEMS** – See GEN01 • **BallotStation** – See GEN02 • **AccuVote-TSX** – See GEN02 • **UAID** is the Universal American Disabilities Association Interface Device, and it is tested for sip and puff and switch interfaces to the AccuVote-TSX units. This interface device has no software or firmware and does not store information. • **KeyCard Tool** – See GEN02 • **Voter Card Encoder** is a pocket-sized device used for encoding voter access cards; it is pre-programmed with ballot identification information. Voter Card Encoder uses its own firmware.
Standards Documents	Voting System Standards 2002, vol. 1 Voting System Standards 2002, vol. 2 Specific standards are noted in following steps

Test Detail	Test Methodology
Test Case Name	**PRI03 (Blanket Open Primary)**
Pre-requisites and initialization of the test case	• Document the date and tester(s) • System, including the witnessed build, is installed and set up as defined in the user documentation • Define election contests, candidates, issues etc. (V1:2.2.6) • Party affiliation is identified on the ballot • Create a supervisory level access 'user' and password' • 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 • Have a Ballot Counter (V1:2.2.9, 3.2.4.2.6) • Retrieve all supplies necessary for testing • Complete Readiness check list
Documentation of 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 tabs • Save all 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 • A ballot (candidates and propositions) can be accurately/securely defined and formatted (V1:3.2.4.2) • A ballot can be accurately/securely programmed and installed into the vote card (V1:3.2.4.2.4, 3.2.4.2.5)
Pre-vote: System Preparation - Security	System Preparation - Security: • System username/password authentication and other access controls are set up according to system documentation guidelines for all devices being tested. • Any/all unnecessary processes are disabled and/or required process control measures noted in the documentation are followed. • All COTS and vendor subsystems used for system security are configured and active as recommended by the system documentation. This includes all connection, port, virus, 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	**PRI03 (Blanket Open Primary)**
Testing and Poll Verification	• The election is correctly installed • Status and data reports are generated • Test data is separate from voting data without impact to the testing • Zero count report • A list of all ballot fields is created (V1:3.2.4.2.1) • No hardware/software failures • The voting device is ready to accept votes (V1:3.2.4.2.2, 3.2.4.3.1)
Pre-vote: Opening the Polls Verification	• Completed Readiness check list • Perform proper sequence of functions to open the polls • Identify any issues, failures, or unexpected results and their required corrective action(s)
Voting: Required functionality verifications	• Maintain accurate and complete audit records (V1:2.2.5.2.1, 3.2.7) • Maintain accurate and complete error and status messages (V1:2.2.5.2.2, 2.2.5.2.3, 3.2.1) • Accurately record cast ballots, including provisional (V1:2.4.3, 3.2.3.1, 3.2.5.2, 3.2.6.2.2) • DRE shall record and retain redundant copies of the original ballot image (V1:2.2.2.2, 3.2.4.3.2, 3.2.4.3.3) • Ensure undervotes are counted as cast votes • All paper-based systems shall: Protect the secrecy of the vote throughout the process (V1:2.4.3.2.1, 3.2.4.1) • Separate accumulation of Undervotes and Paper Overvotes • Ensure Overvotes are counted on paper ballots and tally correctly • Maintain integrity of Vote and Audit data • Accurate Definition, Count, Reporting for Election Day, Absentee - paper and DRE, with the results tallied, excluding and including provisional ballots (V1:2.2.2.1, 3.2.8.2) • Write-in voting: Voting position identified for write-ins (V1:3.2.5.1.3) • Correctly tabulate (V1:2.2.8.1) • Provisional/Challenged ballots - Note vendor supported tabulation of these ballots at Central Count • Overvotes (V1:3.2.5.1.3) • Undervotes (V1:3.2.5.1.3) • Blank ballots (V1:3.2.5.1.3)

Test Detail	Test Methodology
Test Case Name	**PRI03 (Blanket Open Primary)**
Voting: Optional functionality verifications	• One District, One Precinct • No Rotation • Non-Partisan contest: Vote for 1 of N • Non-Partisan contest: "Vote for 1" race with a single candidate and a write-in • Non-Partisan contest: "Vote for 1" race with no declared candidates and write-ins • Non-Partisan contest: Multi-member board (N of M) • Partisan contest: Vote for 1 of N • Partisan contest: "Vote for 1" race with no declared candidates and write-ins • Partisan contest: Multi-member board (N of M) • Partisan contest: One party has no candidates • Primary Presidential Nominations: List only the nominees, not the delegates
Post-Vote: Closing the Polls	• Polls are properly closed • Further casting of ballots and reopening of the polls is prohibited • Device status is normal • Identify any issues, failures, or unexpected results and their required corrective action(s) • Create a test record that verifies the sequence of test events
Post-Vote: Central Count	Capture, document, and verify all counts
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, 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.
Post-Vote: System Audit	Produce and verify available system reports

Test Detail	Test Methodology
Test Case Name	**PRI03 (Blanket Open Primary)**
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 • **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 report is issued, manufacturers are given the opportunity to correct all discrepancies • If corrections are submitted by the manufacturer, 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 level test that uses The 2002 Voting System Standards (VSS) guidelines to validate Readiness throughout the entire voting system. (V1:3.4.1)
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. (V1:3.4.1)
A listing of the applicable voting system machines	• **AVOS-PC** - AccuVote Optical Scan with Precinct Count • **AVOS-CC** - AccuVote Optical Scan with Central Count • **AVOSX** - AccuVote Optical Scan • **AccuVote-TS** - AccuVote Touch Screen • **AccuVote-TSX** - AccuVote Touch Screen • **KCT** - KeyCard Tool • **VCE** - Voter Card Encoder • **VCP** - VC Programmer • **PCS -** Premier Central Scan • **GEMS** - Global Election Management System
Standards Documents	Voting System Standards 2002, vol. 1 Voting System Standards 2002, vol. 2 Specific standards are noted in following steps
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	• Save all 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 • Provide any additional supporting documentation as needed

Test Detail	Test Methodology
Test Case Name	**Readiness Test**
System Preparation - Security	System Preparation - Security: • System username/password authentication and other access controls are set up according to system documentation guidelines for all devices being tested. • Any/all unnecessary processes are disabled and/or required process control measures noted in the documentation are followed. • All COTS and vendor subsystems used for system security are configured and active as recommended by the system documentation. This includes all connection, port, virus, 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	• 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 • 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

Test Detail	Test Methodology
Test Case Name	**Readiness Test**
Summary of Actions per Product	**AVOS-PC**: • Turn the unit off and then back on • Verify that the unit displays Testing Passed • Verify that the correct firmware version is displayed • Verify that the TOT Ballots figure is the same as prior to turning the unit off. • If in pre-election mode, print a report and verify that the results are the same as prior to turning the unit off. **AVOS-CC:** • Turn the unit off and then back on • Verify that the Correct firmware version is displayed • Verify that connecting network is displayed and then the IP address of the machine that the user was last • Connected to is displayed" • Verify that the IP address of the machine is printed to tape • Verify that you can start a deck **AVOSX:** • Turn the unit off and then back on • Verify that the system is initialized • Verify that the correct version of AVOSX firmware is displayed • Verify that the unit returns to the exact same state as it was in prior to turning the unit off. • Verify that TOT Ballot figures are the same as prior to turning the unit off. • If in pre-election mode, print a test results report and verify that the results are the same as prior to turning the unit off

Test Detail	Test Methodology
Test Case Name	**Readiness Test**
Summary of Actions per Product (cont.)	**AccuVote-TS & AccuVote-TSX:** • Turn the unit off and then back on • Verify that the system is initialized • Verify that the Ballot Station version is displayed and is accurate • Verify that the system totals are the same as prior to turning the unit off. • Verify that the election is in the same state as prior to turning the unit off. • Print the audit report and verify that the report is accurate **KCT:** • Exit out of KCT and then re-open the application • Verify that you can still create/update cards **VCE:** • Turn the unit off and then back on. • Verify that the correct firmware version is displayed • Verify that the encoder is in the same state as prior to turning it off. • Verify that the card created totals are accurate • Verify that each key that you had programmed still has the ballot stored on the card **VCP:** • Exit out of the application and then open it up again • Verify that all the ballots/report precinct combinations are still listed • Verity that the user is able to create a card. • Verify that the previously used challenge IDs are still in memory, meaning you can't create a challenged • voter card with an id that you had used prior to exiting out of VCP

Test Detail	Test Methodology
Test Case Name	**Readiness Test**
Summary of Actions per Product (cont.)	**PCS:** • Exit out of the application and then open it up again. • Login and open the workspace that you were working on • Ensure that the same run is active as was prior to exiting the application • Ensure that the Decks screen lists all the decks with the correct statuses • Ensure that all decks that were posted to GEMS still display a POSTED status • Ensure that the correct EID, version and copy # are displayed **GEMS:** • Turn the unit off and then back on (activate GEMS either from the Start menu or from the Desktop) • Verify that the installed GEMS software version has been certified for use in the appropriate jurisdiction • Verify the connection to the election database • Verify the connection to the voting device being downloaded to • Verify that the election database status is 'Set for election' Refer to Table 4 - Required Hardware for additional information on each product.
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 • **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 report is issued, manufacturers are given the opportunity to correct all discrepancies • If corrections are submitted by the manufacturer, retests are performed • Issues that do not impact the failure of the requirements but could be considered defects are logged as Informational Issues on the Discrepancy Report. It is the manufacturer's option to address these issues.

Test Detail	Test Methodology
Test Case Name	**Operational Status Check**
Scope	SysTest Labs requires the vendor to provide a comprehensive end-to-end test case(s) that they supply to their customers, such as state election officials. The Vendor may provide SysTest Labs a comprehensive checklist of test case(s) for particular states' functionality. This test may be based on the vendor's certification configuration. SysTest Labs will perform the operational status check once upon acceptance of the equipment, and once after all other testing, prior to checkout. (V2:4.6.1.5)
Objective	The object of this test case is to verify that when all tests, inspections, repairs, and adjustments have been completed, normal operation can be verified by conducting an operational status check.
Standards Documents	Voting System Standards 2002, vol. 1 Voting System Standards 2002, vol. 2 Specific standards are noted in following steps
Documentation of Test Data & Test Results	• Save all 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

Test Detail	Test Methodology
Test Case Name	**Operational Status Check**
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 • **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 report is issued, manufacturers are given the opportunity to correct all discrepancies • If corrections are submitted by the manufacturer, 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 level test which uses The 2002 Voting System Standards (VSS) guidelines to validate the individual ballot positions in terms of a maximum error rate while processing a specified volume of data. (V2:4.7.1.1)
Objective	The object of this test is to verify that the voting system can accurately and reliably print ballots incorporating a minimum 1,549,703 ballot positions (including voted and non-voted positions) and that these ballots can be mechanically/electronically tabulated without error.
Variables: Voting Variations	A ballot with the maximum number of supported parties and candidates.
A description of the voting system type and the operational environment	• **AVOS-PC** - AccuVote Optical Scan with Precinct Count • **AVOS-CC** - AccuVote Optical Scan with Central Count • **AVOSX** - AccuVote Optical Scan • **AccuVote-TS** - AccuVote Touch Screen • **AccuVote-TSX** - AccuVote Touch Screen • **KCT** - KeyCard Tool • **VCE** - Voter Card Encoder • **VCP** - VC Programmer • **PCS** - Premier Central Scan • **GEMS** - Global Election Management System
Standards Documents	Voting System Standards 2002, vol. 1 Voting System Standards 2002, vol. 2 Specific standards are noted in following steps

Test Detail	Test Methodology
Test Case Name	**Accuracy**
Pre-requisites and initialization of the test case	• Document the date and tester(s) • System, including the witnessed build, is installed and set up as defined in the user documentation • Defined election with maximum contests, candidates, issues etc. • Create a supervisory level access 'user' and password' • 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 • Have a Ballot Counter (V1:2.2.9, 3.2.4.2.6) • Retrieve all supplies necessary for testing • Complete Readiness check list
Documentation of 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 tabs • Save all 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
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, 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	**Accuracy**
Testing and Poll Verification	• The election is correctly installed • Status and data reports are generated • Test data is separate from voting data without impact to the testing • Zero count report • A list of all ballot fields is created (V1:3.2.4.2.1) • No hardware/software failures • The voting device is ready to accept votes (V1:3.2.4.2.2, 3.2.4.3.1)
Pre-vote: Opening the Polls Verification	• Completed Readiness check list • Perform proper sequence of functions to open the polls • Identify any issues, failures, or unexpected results and their required corrective action(s)
Voting: Required functionality verifications	• Maintain accurate and complete audit records (V1:2.2.5.2.1, 3.2.7) • Accurately record cast ballots (V1:2.4.3, 3.2.3.1, 3.2.5.2, 3.2.6.2.2) • Validate the data brought into the system is accurately recorded and reported • Maintain integrity of Vote and Audit data • Correctly tabulate (V1:2.2.8.1)
Accuracy: Error Rate	Maximum error rate is less than one in 10,000,000 ballot positions, with a maximum error rate of one in 500,000 ballot positions in the test process. Errors are from any source while testing a specific processing function and its related equipment. 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)
Post-Vote: Closing the Polls	• Polls are properly closed • Further casting of ballots and reopening of the polls is prohibited • Device status is normal • Identify any issues, failures, or unexpected results and their required corrective action(s) • Create a test record that verifies the sequence of test events
Post-Vote: Central Count	Capture, document, and verify all counts

Test Detail	Test Methodology
Test Case Name	**Accuracy**
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, 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.
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 • **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 report is issued, manufacturers are given the opportunity to correct all discrepancies • If corrections are submitted by the manufacturer, 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
A description of the voting system type and the operational environment	Same as Readiness Test
Standards Documents	Voting System Standards 2002, vol. 1 Voting System Standards 2002, vol. 2 Specific standards are noted in following steps

Test Detail	Test Methodology
Test Case Name	**Security**
Role	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	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	System security ensures that executables can only be run in their intended manner and order so that any other type of attempt to run the system is prohibited. (V1:2.1.1b) Additionally, executable preconditions are verified. Safeguards During Repair, Interventions or Failure are validated to ensure that tampering is not possible. Security Provision Compatibility With Procedures and Admin Tasks Incorporate a means of implementing a capability if access to a system function is to be restricted or controlled.
System Log	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)

Test Detail	Test Methodology
Test Case Name	**Security**
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	• 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
Telecommunications & Data Transmission	• 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	• 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	• Memory Threat & Virus Scanning Mechanisms (V1:6.5.4.2) • Rootkit Scanning Mechanisms
Audit Log	Audit logs and data files cannot be altered through the use of an alternate boot sequence without detection, and the test will consist of attempting to boot the devices using alternative media during boot sequences. Audit logs and data files cannot be altered through the use of editing tools without detection. The test will consist of attempting to edit the audit log to confirm that the system either: • Does not allow edits of the audit log or data files, or • Detects and reports all attempts at editing the audit log or data files
Data Protection	Logical Isolation of Voting System Software & Data (V1:6.5.5.b)
Role	• 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

Test Detail	Test Methodology
Test Case Name	**Security**
Data Protection	• 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	All vendor documentation is reviewed to validate all Vendor Access Control Policies pertaining to: • General, Software, Hardware Access controls • Communications • Effective Password management • Protection abilities of a particular operating system • General characteristics of supervisory access privileges • Segregation of duties • Vendor's access privileges • Access control measures • Physical security measures • Polling place security • Central count location security • Software security • Software and firmware installation • Protection against malicious software • Telecommunications and data transmission • Data integrity • Data interception prevention • Protection against external threats • Identification of COTS Products • Use of protective software • Monitoring and responding to external threats • Shared operating environment • Access to incomplete election returns and interactive queries • Security for transmission of official data over public communications networks • General security requirements for systems transmitting data over public networks • Voting process security for casting individual ballots over a public telecommunications networks • Documentation of mandatory security activities • Capabilities to operate during interruption of telecommunications capabilities • Any other relevant characteristics
External Access	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 level test that uses The 2002 Voting System Standards (VSS) guidelines to validate required functionality. Testing includes Telecommunications capability of the Premier voting system.
Objective	The object of this test case is to verify that the Physical, Technical, and Procedural (documentation) controls correspond correctly for Telecommunication features.
Variables: Voting Variations	• Select type of components on the components tab using the vendor documentation. (V1:5.1.1) • Voting-related transmission over a public network. (V1:5.1.2) • Data / Vote Transmission (V1:5.1.3) • Capabilities (5.2 - 5.2.5): considered basic to all data transmissions. (V1:5.2, 5.2.1, 5.2.6) • Confirmation, the system notifies the user of the successful or unsuccessful completion of the data transmission. (V1:5.2.7) • Voting systems that use telecommunications to communicate between system components and locations are subject to the same security requirements governing access to any other system hardware, software, and data function. (V1:6.5.1 - 6.5.2) • PCMCIA Cards are analyzed with Windows OS drivers to read the card. The files are then modified with a hex editor and it is verified that the system detects files have been altered. • Voting systems that use public telecommunications networks shall protect against threats. (V1:6.5.4 - 6.5.4.3) • Systems that use a shared operating environment (V1:6.5.5) • Access to Incomplete Election Returns and Interactive Queries (V1:6.5.6) • Security for Transmission of Official Data Over Public Communications Networks. Transmitting Data Over Public Network (V1:6.6, 6.6.1) • Security for Casting Individual Ballots over a Public Telecommunications Network (V1:6.6.2, 6.6.2.1) • Operate During Interruption of Telecommunications Capabilities (V1:6.6.2.2)
A description of the voting system type and the operational environment	See GEN03
Standards Documents	SEE GEN03

Test Detail	Test Methodology
Test Case Name	**Telecommunications**
Pre-requisites and initialization of the test case	SEE GEN03 Additionally, the following are performed: • Prepare device & test specific option setting • Prepare computer and device peripheral hardware options • Load firmware/data media • Validate basic device communication functionality, usability • Load voter registration - Electronic Poll Book at precincts
Documentation of Test Data & Test Results	SEE GEN03
Pre-vote: Ballot Preparation procedures verifications	SEE GEN03
Pre-vote: System Preparation - Security	SEE GEN03
Readiness Testing and Poll Verification	SEE GEN03 The election is correctly installed and Electronic Poll Book is in use
Pre-vote: Opening the Polls Verification	SEE GEN03
Voting: Required functionality verifications	SEE GEN03

Test Detail	Test Methodology
Test Case Name	**Telecommunications**
Voting: Optional functionality verifications	• Components are set up as described in the vendor documentation (V1:5.1.1) • Voting-related transmission over a public network. (V1:5.1.2) • Data / Vote Transmission (V1:5.1.3) • Capabilities (5.2 - 5.2.5): considered basic to all data transmissions. (V1:5.2, 5.2.1, 5.2.6) • Confirmation, the system notified the user of the successful or unsuccessful completion of the data transmission. (V1:5.2.7) • Voting systems that use telecommunications to communicate between system components and locations are subject to the same security requirements governing access to any other system hardware, software, and data function. (V1:6.5.1 - 6.5.2) • Voting systems that use public telecommunications networks protect against threats. (V1:6.5.4 - 6.5.4.3) • Systems that used a shared operating environment (V1:6.5.5) • Access to Incomplete Election Returns and Interactive Queries (V1:6.5.6) • * Security for Transmission of Official Data Over Public Communications Networks. Transmitting Data Over Public Network (V1:6.6, 6.6.1) • Security for Casting Individual Ballots over a Public Telecommunications Network (V1:6.6.2, 6.6.2.1) • Operate During Interruption of Telecommunications Capabilities (V1:6.6.2.2)
Post-Vote: Closing the Polls	SEE GEN03
Post-Vote: Central Count	SEE GEN03
Post-Vote: Security	SEE GEN03
Post-Vote: System Audit	SEE GEN03
Results are Observed	SEE GEN03
Record Observations and all input/outputs for each election	SEE GEN03

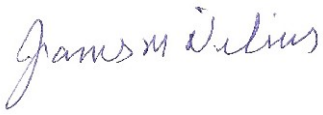
Appendix B – Request for Interpretations and Notices of Clarifications

RFI	Is Applicable?	Reason if not Applicable, high level overview if applicable
07-01	Yes	Documentation will be validated to contain required text, as listed in this RFI
07-02	Yes	This RFI determination was applied during the Source Code Review process
07-03	No	Specific to VVSG 2005
07-04	No	Specific to VVSG 2005
07-05	Yes	EAC determination was applied to Assure 1.2 system, see hardware reports in Certification Report.
07-06	Yes	EAC determination was applied to Assure 1.2 system in all system level tests
08-01	Yes	EAC determination was applied to Assure 1.2 system in hardware testing phase
08-02	Yes	Optical scan systems are subject to the backup power requirement in the Premier Assure 1.2 certification effort
08-03		This RFI has not been published yet.
08-04	No	Test Plan approved prior to effective date
08-05	Yes	EAC determination is applied to Assure 1.2 system, see vendors signed statement of compliance in Certification Report
08-06	Yes	EAC determination is applied to Assure 1.2 system that Central Count optical scan does not require 2 hr. electrical backup but does need to gracefully handle power disruption. Will be verified in separate Functional test
08-07	No	Test Plan approved prior to effective date
08-08	No	No ABCR is part of the Assure 1.2 certification effort
08-09	No	Test Plan submitted/approved prior to effective date
08-10	No	Specific to VVSG 2005
NOC	Is Applicable?	Reason if not Applicable, high level overview if applicable
07-001	Yes	Testing application was submitted in timely manner
07-002	Yes	SysTest Labs does not participate in Premier development efforts

07-003	Yes	Any state testing will be noted
07-004	Yes	Premier does list and will continue to list facilities used to manufacture or assemble voting systems
07-005	Yes	SysTest Labs will manage and oversee 3rd party testing, specifically in hardware testing, as described
08-001	Yes	Per this NOC, all Premier hardware was subjected to ESD testing, see hardware reports in Certification Report
08-002	No	This NOC applies to vendor responsibilities post certification
08-003	No	Test Plan approved prior to effective date

Approval Signatures

SysTest Labs:



James M. Nilius

Sr. VSTL Director

SysTest Labs

September 26, 2008

End of Certification Test Plan