FVAP Statement on Research Reports Related to UOCAVA System Testing

Scope and Purpose

In 2010, the Federal Voting Assistance Program (FVAP) sponsored research on the *Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA)* Pilot Program Testing Requirements (UPPTR) as adopted by the United States Election Assistance Commission (EAC). This research intended to inform the project planning and execution of the Department of Defense's legislatively mandated electronic voting demonstration (i.e., remote electronic voting) requirement, first established in the National Defense Authorization Act of 2002. In 2015, Congress eliminated this requirement; however, the resulting reports from the commissioned research remained unpublished at the time of the repeal.

In order to consider the future direction and voting system architecture surrounding a remote electronic voting system or the consideration of future pilot programs, FVAP's 2010 research objectives were 1) assess the current UPPTR as conformance standards for use by FVAP when fielding a specific voting system (i.e., electronic voting kiosk), and 2) assess the extent that the requirements would need additional security standards for a Department of Defense sponsored electronic voting solution. Although Section five of the UPPTR explores the use of penetration testing in conformance testing, FVAP's consideration of a remote electronic voting solution led to the development of a proof-of-concept approach for additional penetration testing as part of an eventual project implementation.

FVAP had four objectives for these studies: (1) evaluate portions of UPPTR that would apply to information assurance for sufficiency and clarity; (2) evaluate the value and impacts of an FVAP sponsored certification/conformance test to the UPPTR; (3) evaluate the subjective differences between the different voting system test laboratories to inform FVAP project planning; and (4) establish a viable proof-of-concept for future penetration testing as part of FVAP's overall information assurance posture.

These reports were originally intended to foster an ongoing discussion as part of the standards development process in partnership with the EAC and National Institute of Standards and Technology (NIST). As of June 2012, all mechanisms for future discussions dissolved due to changes in FVAP leadership and the lack of EAC Commissioners. Without the supporting federal advisory committees to guide the process, FVAP relied on these reports to inform its possible implementation of future pilots and the electronic voting demonstration project. These reports do not reflect the views and policies of the Department of Defense or FVAP on the concept of internet voting or its ultimate consideration of its efforts to complete the electronic voting demonstration requirement. FVAP anticipates releasing additional research by the end of 2015.

No other conclusions should be drawn beyond the findings stated in the reports and any resulting analysis should be done so in recognition of the following limitations:

Limitations on Voting System Laboratory Testing (VSTL) Report

- Vendors did not submit source code or technical data packages and no code review was performed. There was no opportunity for remediation.

- Indications of pass/fail in the test results do not indicate how well a particular system would perform during a full certification test and may be the result of test interpretation or applicability.

- No systems were presented for certification and certification was not a potential outcome. Only a small portion of the complete UPPTR was studied. Sections two and five of the UPPTR were evaluated and the remaining eight sections were not evaluated.

- The formal EAC process for voting system certification was not followed. Manufacturers are normally allowed to remediate any deficiencies found and submit the system for retesting. For this study, there was no interaction between the EAC, the manufacturer, and the Voting System Testing Laboratory. Each system was evaluated once, in a limited fashion, and the results documented.

Limitations on Penetration Test Model Design and Methodology

- These tests were only intended to serve as a proof-of-concept for the establishment of a model design and methodology for future penetration testing.

- The manufacturer names are not disclosed. The purpose behind these tests was not to evaluate any specific system, but to evaluate the requirements and the process.

- The penetration test period was limited to 72 hours, a significant limitation from expected real world conditions.

- Certain types of attacks, such as Distributed Denial of Service, social engineering, and physical tampering were not allowed. Since the time of this research, the attack profiles and methodologies have significantly changed, thus these tests should be viewed only within the context of when they were conducted.

Conclusions

FVAP found opportunities for improvement in sections two and five of the UPPTR, the core areas of focus in this research. If this research followed a full certification protocol as outlined in the EAC certification program requirements, those ambiguities identified would likely be resolved through a structured test plan and the Request for Interpretation process.

The test results from the different labs were presented in widely different formats. FVAP recommends standardization of test lab reports so relevant stakeholders can benefit from findings that do not reflect the individual styles of each test lab.

Although much of the UPPTR could be applied to remote electronic voting systems, a detailed review would be necessary to determine which requirements apply to these systems directly.

The penetration testing model revealed issues that must be addressed prior to its usage in an accreditation environment. Future consideration of penetration testing must clearly identify the requisite skills and experience of testers to ensure high confidence in the results. The penetration test methodology used during this proof-of-concept exercise also highlighted the difficulties of testing these systems in a realistic environment. Testing across public networks in such a way as to not interfere with other uses was difficult and limiting.

Expanded efforts to develop more robust penetration testing for systems used by *UOCAVA* voters should not use passive tests to assess how products perform, but should instead assess the overall ability for the supporting networks to detect and respond to threats and attacks. Penetration testing should be an ongoing process, conducted in an actively monitored environment, to determine how system operators can respond to potential intrusions.

Recommendations

With the passage of the 2015 National Defense Authorization Act and the repeal of FVAP's requirement for the conduct of an electronic voting demonstration project (i.e., remote electronic voting), the Department of Defense is no longer exploring program implementation in this area and these reports should not be used to convey a position in support of States to move forward with such technology. However, both of these reports mention a series of recommendations which may prove instructive. FVAP will work with the EAC and NIST through the standards development process provided under the *Help America Vote Act* to consider the following:

1. Integration of the individual report findings and recommendations into the consideration of future voting system standards.

2. Exploration into the viability of incorporating structured penetration testing for *UOCAVA*-related systems and qualifications for penetration testers.

Federal Voting Assistance Program (FVAP) Voting System Testing Laboratory Functionality and Security Testing

11 November 2011

FVAP.GOV
FEDERAL VOTING ASSISTANCE PROGRAM

Voting System Testing Laboratory
Functionality and Security Testing

Delivery Order # 80047-0037

Task Order # 5.1.1

Final Report

Version 2

11 November 2011

Executive Summary

In 2009, Congress passed the Military and Overseas Voters Empowerment (MOVE) Act, authorizing the Federal Voting Assistance Program (FVAP) to run pilot programs testing the ability of new or emerging technologies to better serve uniformed and overseas citizens during the voting process. The MOVE Act authorized the U.S. Election Assistance Commission (EAC) and the National Institute of Standards and Technology (NIST) to support FVAP with best practices or standards in accordance with electronic absentee voting guidelines to support the pilot programs.

The EAC published the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements (UPPTR) on August 25, 2010. Following the publication of the UPPTR the Director of FVAP initiated a test project of electronic voting systems. FVAP sought a testing effort that provided insight into:

- Suitability of the UOVAVA Pilot Program Testing Requirements (UPPTR);
- Security of electronic voting systems currently in the marketplace; and
- Comparison of Voting System Test Laboratories (VSTLs) results.

The project described in this report was to test electronic voting systems against Sections 2 (Functional Requirements) and 5 (Security) of the UPPTR, both to evaluate electronic voting systems and to evaluate the UPPTR for adequacy and testability. Two EAC-accredited VSTLs, SLI Global Solutions (SLI) of Denver, Colorado and Wyle Laboratories (Wyle) of Huntsville, Alabama conducted testing on electronic voting systems in accordance with the UPPTR as follows:

- SLI and Wyle tested five Electronic Ballot Delivery Systems (EBDS) against UPPTR Section 5; and
- SLI conducted full system testing of two Internet Voting Systems (IVS) against the non-self-certifying sections of the UPPTR, Sections 2 and 5. (Non-self-certifying requirements list the "Test Entity" as "VSTL".) The two exceptions to this are UPPTR Subsections 4.9 and 7.5. Subsection 4.9 is the evaluation of source code and Subsection 7.9 is physical configuration audit; both of these elements were excluded from this test due to time constraints of this test.

Both VSTLs reported significant limitations in the testing due to exclusions established for these tests, a list of these exclusions is in Chapter 2 of this report. Two major areas impacting the VSTLs' testing efforts were the lack of technical data packages (TDP) and the availability of source code (code that is written by a programmer in a high-level language readable by people but not computers) for the voting systems. The VSTLs reported that the lack of sufficient information and technical documentation limited their ability to define test cases and identify the requirements that could be tested. In addition, due to the lack of source code the VSTLs could not perform white-box testing (a software testing technique whereby explicit knowledge of the internal workings of the item being tested are used to select the test data, with specific knowledge of programming code being required in order to effectively examine outputs).

VSTL Testing of UPPTR Section 5 (Security)

Section 5 of the UPPTR addresses security issues divided into nine major subsections that include:

- Access Control
- Identification and Authentication
- Cryptography
- Voting System Integrity Management
- Communications Security
- Logging
- Incident Response
- Physical and Environmental Security
- Penetration Resistance

The UPPTR requirements, as written, allow for variations in interpretation. The two VSTLs interpreted the number of UPPTR requirements differently. All of UPPTR Section 5 was evaluated but rolled-up at different levels. For example UPPTR Subsection 5.6, Wyle results are reported 17 requirements, while SLI further broke the requirements down for the same section to include individual bullets creating 70 requirements.

In Section 5 of the UPPTR, SLI tested to 169 requirements and reported 147 testable as written, 15 require modification to be testable, and recommended seven for deletion. SLI recommended modifications to total of 60 requirements; however, 45 were still testable as written but recommended be modification for clarification. Wyle's tested to 99 requirements and recommended 24 of the requirements for modification for clarification and testability. See Figure 2, on page 24 of this report, for a breakdown by subsection. The VSTLs' comments and recommendations are documented in Appendix C.

The VSTLs reported their evaluation of the requirements as *Pass*, *Fail*, *Not Tested* or *N/A* (Not Applicable). SLI reported the following percentage ranges for the five EDBSs; a *Pass* rate from zero to 75%, and a *Fail* rate from zero to 100%. Additionally, SLI reported a *Not Tested* rate ranging up to 100%, and a *N/A* rate up to 43%. Wyle reported the following percentage ranges for the five EDBSs; a *Pass* rate from zero to 59%, and a *Fail* rate from zero to 67%. Additionally, Wyle reported a *Not Tested* rate ranging up to 90%, and a *N/A* rate up to 100%. See Figure 12, on page 31 of this report, for a table of these test results. The testing results to UPPTR Section 5 are discussed in Chapter 3 of this report.

SLI reported for security requirements testing of the two IVSs; *Pass* rate from zero to 75%, and a *Fail* rate from eight to 75%. Additionally, SLI reported a *Not Tested* rate ranging up to 77%, and a *N/A* rate up to 17%. See Figure 31, on page 42 of this report, for table of these test results. The testing results for the IVSs are discussed in Chapter 4 of this report.

VSTL Testing of Internet Voting Systems against UPPTR Section 2 (Functional Requirements)

Section 2 of the UPPTR addresses functional requirements of the voting systems divided into seven subsections that include:

- Accuracy
- Operating Capacities
- Pre-Voting Capabilities
- Voting Capabilities
- Post-Voting Capabilities
- Audit and Accountability
- Performance Monitoring

In Section 2 of the UPPTR, SLI tested to 123 requirements and reported 96 testable as written, 25 require modification to improve testability and recommended two for deletion. See Figure 13, on page 33 of this report, for a breakdown by subsection. SLI's comments to these UPPTR requirements are included in Appendix C. Wyle did not participate in the Section 2 Internet Voting System functional requirements testing due to cost.

For the two IVSs, SLI reported a *Pass* rate ranging from 46% to 100%, and a *Fail* rate ranging from zero to 50%. Additionally, SLI reported a *Not Tested* rate ranging from zero to 46%, and a *N/A* rate from zero to 11%; see Figure 30, on page 42 of this report, for a table of these test results. The testing results and recommended changes to UPPTR Sections 2 and 5 are discussed in Chapter 4 of this report.

Conclusion

This initial testing effort provides an evaluation of the UPPTR that will require synthesis of the recommendations and coordination with the EAC to build clearly defined electronic voting system test requirements and provide the VSTLs with better testability standards. The VSTLs have gained information on how to alter their testing methodologies and practices in order to test electronic voting systems. The testing provided the vendors feedback on their systems abilities to conform to the test requirements. The next step in testing would include a complete test of voting systems to include technical data packages review, source code reviews and trusted builds. This testing would take more time but would yield much more usable data on the requirements and the voting systems.

Table of Contents

Table of Figures

1 Introduction

1.1 Background

Under the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) of 1986, the Federal Voting Assistance Program (FVAP) assists active duty uniformed service members, their families, and United States citizens residing outside the United States in exercising their right to vote by absentee ballot when they are away from their permanent address. FVAP administers this law on behalf of the Secretary of Defense and works cooperatively with other federal agencies and state and local election officials to carry out its provisions to assist UOCAVA voters.

UOCAVA was enacted before the advent of today's global electronic communications technology, when UOCAVA voters relied solely on domestic, military, and foreign postal systems for the worldwide distribution of election materials. By the mid-1990s, it became apparent that the mail transit time and unreliable delivery posed significant barriers for many UOCAVA voters, preventing them from successfully exercising their right to vote. At the same time the internet was being widely adopted by businesses, governments and the general public; therefore, it was a natural development for FVAP and states to consider the potential of the internet as an alternative to the "by-mail" UOCAVA voting process. Over the course of the next decade, FVAP sponsored various small pilot and demonstration projects related to electronic voting.

The 2002 National Defense Authorization Act requires FVAP to carry out a demonstration project using an electronic voting system in a regularly scheduled election. In 2009, Congress passed the Military and Overseas Voters Empowerment (MOVE) Act authorizing FVAP to run pilot programs in support of this eventual demonstration project for testing the ability of new or emerging technology to better serve UOCAVA voters. The MOVE Act also directed the U.S. Election Assistance Commission (EAC) and the National Institute of Standards and Technology (NIST) to support FVAP by providing best practices, standards, and guidelines to support the pilot programs.[1]

In July 2009, the EAC convened a UOCAVA Working Group to consider how to adapt the EAC's Testing and Certification Program to accommodate UOCAVA pilot systems. It was concluded that two products were needed: a modified set of system testing requirements; and a revised testing and certification process.[2] In August 2010, the EAC published the UPPTR which is provided in Appendix B.

The UPPTR defines that all kiosk-based remote electronic pilot systems submitted for EAC certification SHALL be tested for conformance with these requirements. In UPPTR terminology, a kiosk is a terminal tasked to display information, accepts user input, and transmits information.[3]

[1] Public Law 111–84—Oct. 28, 2009. 123 STAT. 2335, SEC. 589. Technology Pilot Program., paragraph (e.)(1). Page 20.
[2] U.S. Election Assistance Commission. 2010. Uniformed and Overseas Citizens Absentee Voting Act Pilot Program Testing Requirements, August 25, 2010. Page 7. See Appendix B.
[3] Ibid, page 16 and page 134.

1.2 FVAP Initiation of the VSTL Testing

With the UPPTR published, FVAP initiated Voting System Test Laboratory (VSTL) testing to the UPPTR. Several iterations of scoping and re-scoping of the proposed VSTL testing effort occurred between October and December 2010.

The Director of FVAP and the Deputy Director for Technology Programs expressed concern about the robustness of the UPPTR and whether the requirements were sufficient for testing. This conversation sparked several ideas about how to formulate a program that would test the UPPTR, the EBDSs and IVS, and the VSTLs. There was also concern expressed about the cost of performing tests at variance with standard testing performed by VSTLs. Based on the initial information gathered, the Director decided to complete two separate tests; 1) work with up to five EBDSs and have SLI and Wyle test them to only the security portion of the UPPTR, and 2) have SLI take IVSs from two vendors and test them to the complete non-self-certifying portions of the UPPTR Sections 2 and 5.

To encourage the broadest possible participation from the vendors, testing protocols established by FVAP deviated from the standard VSTL testing. Furthermore, the published reports would have the vendors' names redacted, but that each vendor would receive a report on their system. This would help the vendors as they make changes for future iterations of their systems. The major areas were the specification that this would not be certifying test, and the exclusion of TDP and source code from the test. This is further outlined in Chapter 2 of this report.

1.3 VSTLs

Both VSTLs have experience in conducting full system certification of voting systems to the EAC 2002 Voluntary Voting System Standards (VVSS) and the 2005 Voluntary Voting System Guidelines (VVSG). The VSTLs' existing certification methodology is based on the EAC's 2005 VVSG. To date, all testing that occurs in a VSTL is based on the requirements of the 2002 VVSS or the 2005 VVSG. Each lab had to modify its methodology to accommodate the new UPPTR requirements. The UPPTR requirements are new and none of the voting system were built to meet these requirements, nor had the VSTLs previously tested against the UPPTR. This would require the VSTLs to work at adapting current methodology or producing new methods to conduct the required tests.

There are several significant differences between UOCAVA remote electronic voting systems and conventional voting systems used in polling places. Information from the statewide voter registration database is necessary to authenticate voters and determine their eligibility to vote, match them with the correct ballot style, and record voter history. Some processes handled procedurally in a polling place must be performed by a software application in a remote electronic system. Use of communications networks is necessary to connect to voters.[4]

[4] U.S. Election Assistance Commission. 2010. Uniformed and Overseas Citizens Absentee Voting Act Pilot Program Testing Requirements, August 25, 2010. Page 9. See Appendix B.

1.4 VSTL Testing

SLI and Wyle conducted testing of the electronic voting systems in accordance with the UPPTR. One objective of the project described in this report was to evaluate current requirements in UPPTR Sections 2 and 5 for testability and appropriate language. The second compares the VSTLs' reported test data. To meet these objectives, testing occurred on two types of electronic voting platforms:

- EBDS: This type of system is electronically based (either stand-alone or internet-based) and includes functionality for delivery, printing and signing the ballot. The user then has the option of submitting the ballot via postal mail, fax or email depending on the rules of their voting jurisdiction; and
- IVS: This type of system functions entirely online and includes internet-based submission of the ballot from within the system.

Chapter 2 describes the FVAP approach and defines the scope of the testing conducted by the two VSTLs. This chapter further defines the standard testing methodology for each VSTL and describes deviations from that methodology.

Chapter 3 summarizes the test results received from SLI and Wyle regarding the five EBDSs tested against the requirements of UPPTR Section 5. It also addresses the similarities and differences between the VSTL's test results.

Chapter 4 summarizes the test results received from SLI regarding the two IVSs tested against the requirements of UPPTR Sections 2 and 5.

Chapter 5 presents recommendations for changes to the UPPTR and the VSTLs and for standardizing processes and measurements for future FVAP testing, and for further testing.

2 Methodology

In order to stay within the UPPTR testing scope desired by FVAP, the VSTLs were required to tailor or eliminate elements of their standard testing methodologies. The following subchapters describe SLI's and Wyle's standard testing methodologies, FVAP's tailored approach, and resulting deviations from the standard testing activities.

2.1 EAC Certification Requirements

In standard voting system certification, registered voting system vendors and the VSTLs must adhere to the EAC Voting System Testing and Certification Program Manual. The primary purpose of this manual is to provide clear procedures to VSTLs for testing and certification of voting systems. VVSG Section 1.4, Volume II requires the VSTL to follow the general sequence to meet EAC certification. See Figure 1 for a list of standard VSTL testing activities, modifications to those standard testing activities specified by FVAP for this test, and the impacts thereof.

2.2 VSTLs' Methodologies

SLI and Wyle are currently the only two active VSTLs accredited by the EAC for voting system certification. The VSTLs' existing certification methodology is based on the EAC's 2005 VVSG.

The overall testing process includes several stages involving pre-testing, testing, and post-testing activities. National certification testing involves a series of physical tests and other examinations that are conducted in a particular sequence. This sequence is intended to maximize overall testing effectiveness, as well as ensures that testing is conducted in as efficient a manner as possible. Test anomalies and errors are communicated to the system vendor throughout the process.[5] Each VSTL has an established standard methodology that is traceable to the activities in Section 1.4 of the 2005 VVSG.

2.2.1 SLI's Standard Methodology

SLI's standard methodology defines seven lifecycle phases of testing, the work products that they develop and the activities that they perform in each phase. See the SLI Test Report in Appendix E of this report for a full description of their testing methodology.

Each of the first five phases is considered to be iterative (if an issue or discrepancy is identified, it is reported to the vendor, who is expected to resolve the issue as necessary to meet the requirement). This process generally takes several iterations and potentially involves consultation with the EAC.

SLI emphasizes that formal certification testing involves a production-level system delivered for testing. This encompassed any and all hardware, consumables, source code, and applications; a TDP; a

[5] U.S. Election Assistance Commission. 2005. Voluntary Voting System Guideline Volume II, Version 1.0. Page 8. Retrieved from: http://www.eac.gov/testing_and_certification/2005_vvsg.aspx

declaration of the functionality supported by the system; and documentation of how the system is employed by a jurisdiction.

The seven phases of SLI's standard testing model are detailed below.

2.2.1.1 SLI First Phase - Documentation Review and Test Preparation

The first phase consists of six activities:

- Receipt of the system components and applicable documentation from the vendor;
- Technical Data Package (TDP) review;
- Vendor training on the various aspects of their system;
- A comparison of the documentation against applicable requirements to verify that all needed information is appropriately conveyed;
- A source code review; and
- A test plan is created at the end of this phase that details the system variations to be tested, and how the test suites[6] will be constructed for testing the declared system functionality. The test plan development continues throughout the testing lifecycle and is completed at the end of phase five.

2.2.1.2 SLI Second Phase - System Familiarization & Readiness

The second phase encompasses the creation of a readiness test, which demonstrates the system is installed and running correctly at a basic level and prepared for testing. SLI determines the high level of content of each test suite to be executed based on the functionality of the voting system to be tested.

2.2.1.3 SLI Third Phase - Test Development

In the third phase, individual test modules are created. When brought together within a suite, these test modules will execute each piece of functionality within the system under test. Unique test modules are created as appropriate for each vendor. SLI creates new or reuses existing test modules as appropriate. Testing of the modules determine how well individual requirements are met.

[6] A test suite is a group of test modules designed to test a set of functions of a voting system or device. A test module is a small set of test steps based on a single function or scenario, such as logging into an election management system or recording a vote. Test modules are designed to be reusable components and are the basic building blocks of the test suite.

2.2.1.4 SLI Fourth Phase - Test Validation

During the fourth phase, each test module is incorporated into the respective suites. The correctness of each module is validated within each suite.[7] This phase can be iterative until all test modules within every test suite are determined to be correct in implementation. SLI performs a trusted build (a trusted build of software and/or firmware elements of the voting system is witnessed by the VSTL according to procedures established by the vendor) by following the vendor's prescribed build process to create the software binaries that will comprise the voting system.

2.2.1.5 SLI Fifth Phase - Test Execution

The fifth phase encompasses the formal execution of each test suite, as prescribed in the test plan. Test modules that were created for each vendor and suites that were built in the third phase and validated in the fourth phase would be used for testing. Ad-hoc testing could be employed if there was insufficient documentation to create test cases.

2.2.1.6 SLI Sixth Phase - Project Administration and Reporting

The Test Report is the product of the sixth phase. The VSTL would normally use the National Certification Test Report format prescribed by Section 1.4 of the VVSG.

2.2.1.7 SLI Seventh Phase - Finalization

The seventh phase concludes the test with the return of equipment to the vendor, and the archiving of test material.

2.2.1.8 SLI Test Result Definitions

SLI used the following definitions for reporting test results:

- Pass: indicates sufficient system functionality such that the requirement is considered met;
- Fail: indicates that the functionality did not meet the criteria listed for its function;
- Not Tested: indicates that while functionality should be in place to cover the requirement, either access to the functionality was not provided (for example no administrator password was given for access to the server), or documentation was insufficient for indicating where and how the functionality was implemented; and
- Not Applicable (N/A): indicates that functionality was not in place and did not apply to the system design and manufacturing. For example, if a system did not employ a Virtual Private Network (VPN) (see Subsection 5.5.1.3), this requirement was N/A.

[7] Correctness is defined as: given a known set of inputs to the module; the outputs (results) that are received are those that were expected.

2.2.2 Wyle's Standard Methodology

Wyle's standard methodology consists of three life-cycle phases. Phase one is *Test Plan / Engineering Analysis*. Phase two is *Testing*, and phase three is the *Test Report*. See the Wyle Test Plan and Test Report in Appendix F of this report.

2.2.2.1 Wyle First Phase - Test Plan and Engineering Analysis

Wyle's first phase of testing encompasses six major activities:

- Create a test plan;
- Review the TDP;
- Review source code;
- Perform a trusted build;
- Integrate the hardware; and
- Conduct functional and performance testing.

In creating the test plan, Wyle conducts an evaluation and mapping of the vendors' products, related documentation, and the UPPTR. Wyle then develops the test matrix, test cases, and the final test.

The review of the TDP, test cases are developed for three main test areas: *functional*, *penetration*, and *cryptographic*. Wyle designs individual test cases using each vendor's documentation, architectural documents and security specifications. The cryptographic test cases are designed with use cases and verification methods. During this testing the VSTL attempts to penetrate the system and scan the system and network for possible exploits. Some of these exploits may be open ports or inadequate firewalling. The VSTL uses the gathered information to write test scripts for the penetration test.

The source code is reviewed for compliance to Sections 5 and 7 (Volumes I and II) of the EAC 2005 VVSG. Wyle's procedures call for performing a trusted build with a vendor representative witnessing the build process to provide assurances that the source code reviewed and tested is the actual source code in the final build of the system. This trusted build is performed after successful review of all source code, build, and install packages in order to confirm their compliance with the EAC 2005 VVSG.

All hardware equipment is integrated according to provided system documents contained in the TDP. The reviewed and compliant source code of the trusted build is installed on the system hardware according to the TDP.

Functional and performance testing is then performed based on the EAC 2005 VVSG and the TDP. During these tests, all hardware is in the VSTL's control.

2.2.2.2 Wyle Second Phase - Testing Phase

The second phase encompasses three main test areas: *functional*, *cryptographic* and *penetration.*

The functional test focuses on inspection, review and execution as the primary test methods. Individual test cases are designed using vendor's documentation and security specifications. Each test case is defined with a written script. The test consists of executing each step of the script, recording observations and relevant data as each step completes. As the test is conducted any unexpected conditions or incorrect actions will be recorded and any suspected malfunction will be recorded as an exception report.

The cryptographic test will focus on inspection, review and execution. Cryptography will be tested for functionality, strength and NIST compliance. Systems that generate cryptographic keys internally will be tested for key management. This includes the generation method, security of the generation method, seed values and random number generation. Individual test cases have been designed using "Use Case" and verification.

The penetration test area is broken into two phases: *discovery* and *exploratory*. The discovery phase consists of performing scans while the system is running with leveraged and unleveraged credentials. These scans provide information about the ports, protocols, and hardware configurations, as well as simulating certain portions of an attack on vulnerable areas of the system. The information gathered will be provided to a certified security professional, who will analyze the results and determine the best method and types of attacks to be performed during the exploratory phase of testing.

The exploratory phase of the penetration test will have specific test cases designed and executed. These test cases are based on all information gathered during discovery, any subsequent observations made during the exploratory phase and any rules of engagement previously agreed upon by the Wyle and vendor.

2.2.2.3 Wyle Third Phase - Test Report

The third phase concludes with the preparation of a test report which includes the *Pass* / *Fail* status of each test and an analysis of the testing results.

Wyle evaluated all test results against the requirements set forth in UPPTR Section 5. Each system under test was evaluated for its performance against the referenced requirements. The acceptable range for system performance and the expected results for each test case were derived from system documentation.

2.2.2.4 Wyle Test Result Definitions

Wyle used the following definitions for reporting test results:

- Pass: The system contained the functionality documented in the UPPTR and when this functionality was tested, it passed the test;
- Fail: The system contained the functionality documented in the UPPTR and when this functionality was tested, it failed the test;
- Not Tested: The system did not contain the functionality documented in the UPPTR and therefore could not be tested or the system under test contained the functionality documented in the UPPTR; however, due to constraints (time and/or hardware provided), the system could not be tested for the UPPTR compliance; and
- Not Applicable (N/A): The system did not contain the functionality documented in the UPPTR and did not apply to EBDSs.

2.3 FVAP Approach

To encourage the broadest possible participation from the vendors, FVAP established a modified testing scope. This testing would not follow the EAC Voting System Pilot Program Testing and Certification Manual since this testing was not intended for certification. Figure 1 outlines tasks required by the VSTL standard methodology and the changes required for this UPPTR testing campaign. Inclusions are FVAP specified activities to be part of the testing. Exclusions are those activities in the VSTLs' standard methodologies omitted from the testing.

Inclusions:

- Security testing against UPPTR Section 5 EDBSs;
- Full system testing against UPPTR Sections 2 and 5 for two IVSs;
- Testing conducted only on those UPPTR requirements where the specified test entity in the UPPTR is 'VSTL' and for those requirements which contain the imperative "SHALL";
- Final test report including any discrepancies found during testing would be sent to each vendor and only a redacted report without any test discrepancies would be sent to FVAP; and
- Final test report includes the VSTLs' comments on suitability and testability of the requirements as well as any recommendations for improvement.

Exclusions:

- No self-certifying sections of the UPPTR will be tested;
- TDP will not be required from the vendors;
- No source code review will be conducted;
- A trusted build will not be performed;
- No hardware testing or review will be conducted;
- Vendors' names will not be included in the final test report;

- The vendors will not submit any system changes or fixes during the test period; and
- There would not be remediation of vendors' anomalies / failures and VSTLs would not conduct regression testing.

Appendix D outlines the activities that are required by the VSTL standard methodology for an EAC formal certification and the changes that FVAP required for this UOCAVA testing campaign. Risks to the VSTLs testing campaign are identified for those activities that were not performed.

2.4 Impact of FVAP Approach

In accordance with the inclusion and exclusion list above, both VSTLs made deviations to their standard methodologies. Figure 1 outlines the VVSG activities, FVAP modification / deviation from standard procedures, the impact on the VSTLs, and VSTL differences. The most significant of these exclusions were not requiring the vendors to provide a TDP to the VSTLs and not requiring source code reviews, activities that are required by the EAC. These two exclusions resulted in major adverse impacts on the VSTLs' ability to develop and execute test cases. The changes made to the methodology of each VSTL was driven by the insertion of the new UPPTRs, the time constraints on testing and the ability of the vendor to provide needed items and documentation. FVAP decided to exclude TDPs and code review to meet the required schedule and not force the vendors to provide items they may not have. Some of the vendor's products were newly developed.

Figure 1: VSTLs' Standard Methodology for EAC Certification and Deviations

VVSG Activities	FVAP Approach	Impact on VSTLs	VSTL Differences
a. Initial examination of the system and the technical documentation provided by the vendor to ensure that all components and documentation needed to conduct testing have been submitted, and to help determine the scope and level of effort of testing needed. TDP Review.	TDP were Not Required	Both VSTLS could not complete Phase One of their Test Methodology.	
b. Examination of the vendor's Quality Assurance Program and Configuration Management Plan.	Not Required	VSTLs did not perform this activity.	
c. Development of a detailed system test plan that reflects the scope and complexity of the system, and the status of system certification (i.e., initial certification or a recertification to incorporate modifications).		VSTLs had to develop vendor-specific test cases.	SLI did not submit test plan or test cases.
d. Code review for selected software components	Source Code was not Required.	VSTLs did not perform this activity.	

VVSG Activities	FVAP Approach	Impact on VSTLs	VSTL Differences
e. Witnessing of a system 'build' conducted by the vendor to conclusively establish the system version and components being tested.	Not Required	VSTLs did not perform this activity.	
f. Operational testing of hardware components, including environmental tests, to ensure that operational performance requirements are achieved.	Not Required	VSTLs did not have complete control of the testing environment, similar to what they normally have for kiosk-based voting systems.	
g. Functional and performance testing of hardware components.	Not Required	VSTLs did not perform this activity.	
h. System installation testing and testing of related documentation for system installation and diagnostic testing.	Not Required	VSTLs did not perform this activity.	
i. Functional and performance testing of software components.	No Change		
j. Functional and performance testing of the integrated system, including testing of the full scope of system functionality, performance tests for telecommunications and security; and examination and testing of the System Operations Manual.	Functional testing IAW UPPTR. No System Operations Manual required.	VSTLs did not perform testing of the Operational Manual.	
k. Examination of the system maintenance manual.	Not Required	VSTLs did not perform this activity.	
l. Preparation of the National Certification Test Report.	Final test report including any discrepancies found during testing would be sent to each vendor; only a redacted report without any test discrepancies would be submitted. Final test report includes the VSTL comments on suitability and testability of the requirements as well as any recommendations for improvement.	VSTLs do not provide comments for suitability and testability in a formal certification report.	Each VSTL used their own format for the test report and reported test results differently.
m. Delivery of the National Certification Test Report to the EAC.	Not Required	VSTLs did not perform this activity.	

3 Electronic Ballot Delivery Systems (EBDS) Testing Results for UPPTR Section 5 (Security)

This chapter analyzes the test results received from SLI and Wyle of five EBDSs tested against Section 5 of the UPPTR. Both labs used the same five systems for the testing; however, the vendors' names were redacted in order to maintain the vendors' anonymity. The test reports from SLI and Wyle are located at Appendices E and F of this report respectively.

For comparative analysis, the results from the five EBDSs from SLI's report, labeled as Manufacturer 3 through 7, were compared against the five EBDSs in Wyle's report, labeled as System A through E. Manufacturer 1 and 2 in SLI's report are the IVSs discussed in Chapter 4 of this report.

Section 5 of the UPPTR consists of the following subsections:

- 5.1 Access Control
- 5.2 Identification and Authentication
- 5.3 Cryptography
- 5.4 Voting System Integrity Management
- 5.5 Communications Security
- 5.6 Logging
- 5.7 Incident Response
- 5.8 Physical and Environmental Security
- 5.9 Penetration Resistance

Comparing the test results from SLI and Wyle proved challenging due to the vast differences in their final test reports. Upon receipt of the final versions of each report, a number of inconsistencies and discrepancies were found and will be discussed throughout this report.

The Wyle Test Report (Appendix F) includes a table providing information by system (labeled A, B, C, etc.) delineating which system met each result category (*Pass*, *Fail*, etc.) for each requirement in UPPTR Section 5. For example, for UPPTR 5.1.1.1 (Definitions of Roles), three systems passed and two failed. The difference between SLI and Wyle is that SLI tested to the lowest sublevel requirement, resulting in 18 and Wyle tested to only 15 requirements.

The two VSTLs submitted vastly different report formats complicating comparisons. Although both VSTLs included tables summarizing their results, SLI also provided a detailed written summary for each vendor by system against the UPPTR Subsections 5.1 through 5.9. In contrast, Wyle grouped the results into three sections: *functional* testing reported against UPPTR Subsections 5.1, 5.2, 5.4, 5.5, 5.6, and 5.7; *cryptographic* testing against Subsection 5.3; and *penetration* testing against Subsections 5.8 and 5.9. Wyle reported on all five systems for the functional and penetration testing, but it is unclear which systems(s) Wyle tested for cryptography.

The following subchapters detail the VSTLs results by subsections of the UPPTR. The figures depict the average results between all five systems from SLI's and Wyle's reports in each category (*Pass, Fail, Not Tested,* and *N/A*) and the ranges of those results by category. The ranges show the variance in results between the EDBSs and at times there are significant differences in how the EDBSs performed during testing. The subchapters also address the similarities and differences between the VSTL's test results.

Variations in the VSTLs' approach to requirements definitions and statistical reporting are worth noting. SLI reported 169 actionable requirements for Section 5 and Wyle reported 99. Wyle reported their results based on individual numbered requirements statements from Section 5, many of which contained more than one "SHALL" or "SHALL NOT".

Each VSTL received all documentation that the voting system vendors had at the time of request. There were no complete TDP received from the vendors and it was not required. As functional testing of these requirements is dependent on appropriate documentation detailing how the requirements are met, the lack of documentation may have led to variable decisions from the VSTLs about what could and could not be tested. Additionally, in several cases, the VSTLs were unable to access relevant vendor systems (voting servers or other hardware necessary for validation).

There were instances of inconsistencies within both VSTL Test Reports. The VSTLs were contacted and given opportunities to correct / edit and resubmit their reports. When the final versions were submitted, errors were still found within them and though the VSTLs acknowledged that, they were not willing to make further corrections / edits.

In Section 5 of the UPPTR, SLI tested based on 169 requirements. Of these requirements, SLI reported 147 were testable as written, 15 require modification to be testable, and recommended seven be deleted. Wyle tested to 99 requirements and recommended 24 of the requirements be modified for clarification and testability. Figure 2 provides the number, by subsection, of the UPPTR Section 5 requirements that are testable as written, need modification for better testability or deleted. The VSTLs' comments and recommendations are documented in Appendix C.

Figure 2: VSTLs' Assessment of the UPPTR Section 5 (Security)

Section 5 (Security)	SLI				Wyle			
	Requirements	Acceptable	Modify	Delete	Requirements	Acceptable	Modify	Delete
5.1 Access Control	18	17	1	0	15	5	10	0
5.2 Identification and Authentication	18	17	1	0	13	8	5	0
5.3 Cryptography	12	9	3	0	12	8	4	0
5.4 Voting System Integrity Management	8	5	3	0	7	7	0	0
5.5 Communications Security	9	7	2	0	10	10	0	0
5.6 Logging	70	66	4	0	17	12	5	0
5.7 Incident Response	2	2	0	0	2	2	0	0
5.8 Physical and Environmental Security	14	14	0	0	14	14	0	0

Section 5 (Security)	SLI				Wyle			
	Requirements	Acceptable	Modify	Delete	Requirements	Acceptable	Modify	Delete
5.9 Penetration Resistance	18	10	1	7	9	9	0	0
Total	**169**	**147**	**15**	**7**	**99**	**75**	**24**	**0**

3.1 Access Control (UPPTR 5.1)

Subsection 5.1 of the UPPTR enumerates requirements for identification of authorized system users; identification of authorized processes and devices; and the authorization or verification of those identities as prerequisites to granting access to the system processes and data. SLI reported that across the systems, appropriate access controls were in place over each defined user, role, or group; however, a majority of the systems had deficiencies in their login functions and tabulation process configurations. Wyle reported that the functional tests showed areas of deficiency, stating that across the systems tested, login functions, password functions, and log generation functions were inadequate. The VSTL test results are depicted in Figure 3.

The VSTLs made comments and recommendations on 12 of the requirements in UPPTR Subsection 5.1. The recommendations to modify the language of the UPPTR include; defining minimal level of security, specifying roles, defining required logging information, and if the requirement is at the web application level or Operating System level.

Figure 3: Access Control Test Results Averages and Ranges

UPPTR Section 5.1 Access Control	SLI				Wyle			
	Pass	Fail	Not Tested	N/A	Pass	Fail	Not Tested	N/A
Average of the 5 systems	29%	18%	53%	0%	39%	28%	13%	20%
Ranges	0-42%	0-53%	5-100%	0%	20-53%	20-33%	0-40%	20%

3.2 Identification and Authentication (UPPTR 5.2)

Subsection 5.2 of the UPPTR enumerates requirements for authorization mechanisms and their associated strengths. In several cases, the VSTLs were unable to access relevant vendor systems or credentials. For example, one system could not be tested against these requirements because the vendor was involved in a live election, and could not provide SLI access to its remote system. SLI could only test four of the five systems, and reported that across all four systems, password controls were insufficient or not verifiable, although password reset was sufficiently robust in two systems. Additionally, a majority of the systems did not provide required multifactor authentication. Wyle reported that the functional tests showed areas of deficiency, stating that across the systems tested, login functions, password functions, and log generation functions were inadequate. Figure 4 depicts the VSTL test results.

The VSTLs made comments and recommendations on nine of the requirements in UPPTR Subsection 5.2. The recommendations to modify the language of the UPPTR include; defining minimal level of authentication, specify NIST standard, and define if the password reset is to be web-based.

Figure 4: Identification and Authorization Test Results Averages and Ranges

UPPTR Section 5.2 Identification and Authorization	SLI				Wyle			
	Pass	Fail	Not Tested	N/A	Pass	Fail	Not Tested	N/A
Average of the 5 systems	17%	34%	41%	8%	40%	37%	14%	9%
Ranges	8-38%	11-46%	5-100%	8%	15-54%	15-46%	0-54%	8-15%

3.3 Cryptography (UPPTR 5.3)

Subsection 5.3 of the UPPTR enumerates requirements for cryptography, including encryption for confidentiality, authentication, and random number generation. SLI reported 70% of the requirements in this subsection as not testable. Three systems complied with the 112 bits requirement length and digital certificate generated by a top commercial Certificate Authority. The VSTL test results are depicted in Figure 5.

The VSTLs made comments and recommendations on seven of the requirements in UPPTR Subsection 5.3. The recommendations to modify the language of the UPPTR include; defining minimal level of NIST standard for cryptographic algorithms, splitting requirements that are currently combined to create discrete items, and defining an acceptable level of effort to reset the cryptographic keys to new values.

Figure 5: Cryptography Test Results Averages and Ranges

UPPTR Section 5.3 Cryptography	SLI				Wyle			
	Pass	Fail	Not Tested	N/A	Pass	Fail	Not Tested	N/A
Average of the 5 systems	25%	5%	71%	0%	8%	22%	70%	0%
Ranges	0-69%	0-23%	31-100%	0%	0-17%	17-33%	50-75%	0%

3.4 Voting System Integrity Management (UPPTR 5.4)

Subsection 5.4 of the UPPTR addresses the secure deployment and operation of the voting system, including the protection of removable media and protection against malicious software. In several cases, the VSTLs were unable to access relevant vendor systems (voting server or other hardware necessary for validation). SLI reported that only one of the systems passed any requirements and that same system experienced no failures. They also reported that three systems did not provide access to the remote server; therefore, the electronic ballot box integrity checks could not be validated. SLI tested 51% of the requirements and Wyle only tested 15%. Figure 6 depicts the VSTL test results.

The VSTLs made comments and recommendations on five of the requirements in UPPTR Subsection 5.4. The recommendations to modify the language of the UPPTR include; defining "electronic ballot box", and expanding the requirement to cover all associated devices at a kiosk location.

Figure 6: Integrity Management Test Results Averages and Ranges

UPPTR Section 5.4 Integrity Management	SLI				Wyle			
	Pass	Fail	Not Tested	N/A	Pass	Fail	Not Tested	N/A
Average of the 5 systems	11%	40%	26%	23%	9%	6%	29%	57%
Ranges	0-57%	0-71%	0-57%	0-43%	0-14%	0-14%	29%	57%

3.5 Communications Security (UPPTR 5.5)

Subsection 5.5 of the UPPTR enumerates requirements for communications security ensuring the integrity of transmitted information and protecting the voting system from external communications-based threats. SLI reported one system was not tested against any of the requirements because time ran out on the project and none of the system had VPN. Three systems implemented appropriate protocols and authentication methods and interfaces were appropriately minimized to prevent authorized access attempts. Four systems did not fully provide vote integrity to adequately fulfill the UPPTR requirements. One system did implement appropriate protocols and authentication methods. Wyle reported an average of 66% of the UPPTR requirements were not tested due to lack of access to vendor hardware for validation. The VSTL test results are depicted in Figure 7.

The VSTLs made comments and recommendations on eight of the requirements in UPPTR Subsection 5.5. The recommendations to modify the language of the UPPTR include; split data requirement to handle outbound and inbound data separately and referencing NIST requirement to clearly define strong mutual authentication requirements.

Figure 7: Communications Security Test Results Averages and Ranges

UPPTR Section 5.5 Communications Security	SLI				Wyle			
	Pass	Fail	Not Tested	N/A	Pass	Fail	Not Tested	N/A
Average of the 5 systems	34%	6%	52%	8%	18%	8%	66%	10%
Ranges	0-60%	0-10%	20-100%	0-10%	0-50%	0-20%	20-90%	10%

3.6 Logging (UPPTR 5.6)

Subsection 5.6 of the UPPTR enumerates requirements for the voting system to perform event logging for system maintenance troubleshooting, recording the history of system activity, and detecting unauthorized or malicious activity. In several cases, the VSTLs were unable to access relevant vendor systems (voting server or other hardware necessary for validation). SLI reported a vast difference in the systems for the

logging requirements and because they broke out the requirement into 70 different testing events, no two system's results were similar. Wyle tested the highest percentage of requirements over any other in subsection of the UPPTR (87%). Figure 8 depicts the VSTL test results.

The VSTLs made comments and recommendations on 15 of the requirements in UPPTR Subsection 5.6. The recommendations to modify the language of the UPPTR include; splitting default settings requirements to more discrete sub requirements, defining minimal default settings per NIST, defining the scope of "all communications," and define critical events.

Figure 8: Logging Test Results Averages and Ranges

UPPTR Section 5.6 Logging	SLI				Wyle			
	Pass	Fail	Not Tested	N/A	Pass	Fail	Not Tested	N/A
Average of the 5 systems	24%	47%	29%	0%	45%	42%	1%	12%
Ranges	12-35%	30-71%	5-47%	0%	29-59%	29-59%	0-6%	12%

3.7 Incident Response (UPPTR 5.7)

Subsection 5.7 of the UPPTR has only two requirements that the vendors document system operations or security critical events. SLI reported all the systems failed in testing; however, in their written results, SLI stated that three of the five systems were not tested because the vendors did not provide kiosk location hardware (not a requirement) and documentation was lacking, thus an inconsistence in their reporting. Wyle concluded that the two requirements were not applicable to a web based application. Figure 9 depicts the VSTL test results.

The VSTLs made comments and recommendations on both of the requirements in UPPTR Subsection 5.7. The recommendations to modify the language of the UPPTR included defining the minimum criteria for critical events.

Figure 9: Incident Response Test Results Averages and Ranges

UPPTR Section 5.7 Incident Response	SLI				Wyle			
	Pass	Fail	Not Tested	N/A	Pass	Fail	Not Tested	N/A
Average of the 5 systems	0%	100%	0%	0%	0%	0%	0%	100%
Ranges	0%	100%	0%	0%	0%	0%	0%	100%

3.8 Physical and Environmental Security (UPPTR 5.8)

Subsection 5.8 of the UPPTR enumerates requirements for physical and environmental security which includes physical access; alarms, voting capture devices, and counter security measures. SLI reported a vast difference in the systems. One system had no testing done against any of the requirements and the

other four systems tested vastly different from each other but overall, an average of only 4% of the requirements in this section passed. Because there were no requirements for documentation or kiosks, testing was limited. Wyle reported physical and environmental security under penetration testing and broke that area down into two phases; discovery and exploratory. Three systems had between 11 and 42 low risks found and one of those three systems also had eight medium risks found. One system had no detected risks and one system exposed some information that could be useful to an attacker. Figure 10 depicts the VSTL test results.

The VSTLs made comments and recommendations on fourteen of the requirements in UPPTR Subsection 5.8. The recommendations to modify the language of the UPPTR include; changing the "Test Method" for the physical port shutdown requirement to functional, enumerating the activities for access point security requirements, and rewording media protection requirement for common industry terms.

Figure 10: Test Results Averages and Ranges for Physical and Environmental

UPPTR Section 5.8 Physical and Environmental	SLI				Wyle			
	Pass	Fail	Not Tested	N/A	Pass	Fail	Not Tested	N/A
Average of the 5 systems	4%	24%	63%	9%	6%	0%	9%	86%
Ranges	0-14%	0-71%	7-93%	7-15%	0-14%	0%	0-14%	86%

3.9 Penetration Resistance (UPPTR 5.9)

Subsection 5.9 of the UPPTR enumerates requirements for penetration resistance attempts and penetration resistance test and evaluation. SLI reported penetration testing was completed and in terms of system access and interface requirements. Two vendors had 253 exploits attempted and all exploits were unsuccessful. The other three vendors were not able to provide access to back-end servers for SLI to perform penetration testing. Wyle determined that during penetration testing of the five vendors collectively, there were 75 low risk areas, eight medium risk areas, and no high risk areas. The categorization of high risks, medium risks, and low risks was done using the reporting capability of the Nessus scanning tool. A certified security professional performed vulnerability scans of the voting systems using the Nessus scanning tool. The underlying risk calculations for the report use the Common Vulnerability Scoring System (CVSS) methodology from NIST. Figure 11 on the next page depicts the VSTL test results.

The VSTLs made comments and recommendations on all of the requirements in UPPTR Subsection 5.9. The recommendations to modify the language of the UPPTR include; defining resistant levels, enumerating the activities to be tested for system access, and removing the penetration resistance test and evaluation, and move the requirement to a program manual for the VSTLs.

Figure 11: Test Results Averages and Ranges for Penetration Resistance

UPPTR Section 5.9 Penetration Resistance	SLI							
	Pass	Fail	Wyle	N/A	Pass	Fail	Not Tested	N/A
Average of the 5 systems	30%	8%	45%	17%	40%	22%	18%	20%
Ranges	0-75%	8%	0-75%	17%	11-56%	0-67%	11-22%	11-22%

3.10 Testing Summary for UPPTR Section 5

Analyzing the results of both laboratories proved to be challenging mainly due to their very different testing and reporting styles. SLI provided much more details about each system than did Wyle. Wyle encapsulated the results and grouped them into major categories not breaking them down into second and third levels (5.1, 5.2, 5.4, 5.5, 5.6, and 5.7), (5.3), and (5.8 and 5.9). Each VSTL reported each test result category (*Pass*, *Fail*, *Not Tested*, and *N/A*) differently. The interpretation of the test result categories and the UPPTR requirements lead to altering each VSTL's standard testing methodology. The differing methodologies of the two VSTLs were factors if the differences in test category reporting.

Figure 12 on the next page depicts the average percentage totals (for all five systems) and the ranges of those totals for each major subsection of the UPPTR. The *Not Tested* category is comprised of requirements not tested due to time constraints and/or unclear UPPTR requirements. The *N/A* category indicates that the functionality was either not in place and was not required for a web-based application. In some instances, the VSTLs' spreadsheet / matrix, included in their test reports, had discrepancies that led to questions of their findings. Two examples are; 1) SLI reporting a 100% *Fail* rate for all requirements in Section 5.7 with their written report stating they could not test due to hardware not provided at the kiosk location and 2) Wyle not including all of the "SHALL" requirements in Subsection 5.1.2.8.

Figure 12a provides the average VSTLs' Pass / Fail percentages by Subsection. Figure 12b provides the Pass percentage results from both VSLTs for the five systems. The five systems tested by SLI, Manufactures 3-7, are labeled SLI-1, SLI-2, etc. The five systems tested by Wyle, System s A-E, are label Wyle-A, Wyle-B, etc. The percentages vary greatly between Subsections and systems. For example, the Pass rate of SLI-3 for Subsection 5.4 was 0% and for Subsection 5.9 was 75%, while the Pass rates in Subsection 5.9 for all systems ranged from 0% to 75%.

In evaluating the VSTLs' results, based on the fact that the UPPTR was written for kiosks, the Pass / Fail results would not have changed with the requirements being modified. Both VSTLs' Pass / Fail test criteria used the definition that the functionality was available and it either satisfied the requirement or did not satisfied the requirement. The majority of the requirements that were not appropriate for EDBSs fell into the Not Applicable percentage, though some of the requirements were Not Tested and require modification in order to be testable for EDBSs.

Both VSTLs recommended modifications to the Section 5 UPPTR requirements documented in Appendix C and the VSTL's Test Reports located in Appendices E and F. SLI recommended a total of 60 requirements needed modifications and seven should be deleted. Wyle recommended a total of 51 requirements needed modifications.

Figure 12: VSTL Test Results for UPPTR Section 5 (Security)

UPPTR Section 5 Security	SLI				Wyle			
	Pass	Fail	Not Tested	N/A	Pass	Fail	Not Tested	N/A
5.1 Access Control	29%	18%	53%	0%	39%	28%	13%	20%
Range	0-42%	0-53%	5-100%	0%	20-53%	20-33%	0-40%	20%
5.2 Identification and Authentication	17%	34%	41%	8%	40%	37%	14%	9%
Range	8-38%	11-46%	5-100%	8%	15-54%	15-46%	0-54%	8-15%
5.3 Cryptography	25%	5%	71%	0%	8%	22%	70%	0%
Range	0-69%	0-23%	31-100%	0%	0-17%	17-33%	50-75%	0%
5.4 Voting System Integrity Management	11%	40%	26%	23%	9%	6%	29%	57%
Range	0-57%	0-71%	0-57%	0-43%	0-14%	0-14%	29%	57%
5.5 Communications Security	34%	6%	52%	8%	16%	8%	66%	10%
Range	0-60%	0-10%	20-100%	0-10%	0-50%	0-20%	20-90%	10%
5.6 Logging	24%	47%	29%	0%	45%	42%	1%	12%
Range	12-35%	30-71%	5-47%	0%	29-59%	29-59%	0-6%	12%
5.7 Incident Response	0%	100%	0%	0%	0%	0%	0%	100%
Range	0%	100%	0%	0%	0%	0%	0%	100%
5.8 Physical and Environmental Security	4%	24%	63%	9%	6%	0%	9%	86%
Range	0-14%	0-71%	7-93%	7-15%	0-14%	0%	0-14%	86%
5.9 Penetration Resistance	30%	8%	45%	17%	40%	22%	18%	20%
Range	0-75%	8%	0-75%	17%	11-56%	0-67%	11-22%	11-22%

Figure 13a: VSTLs' Average Pass / Fail Percentages

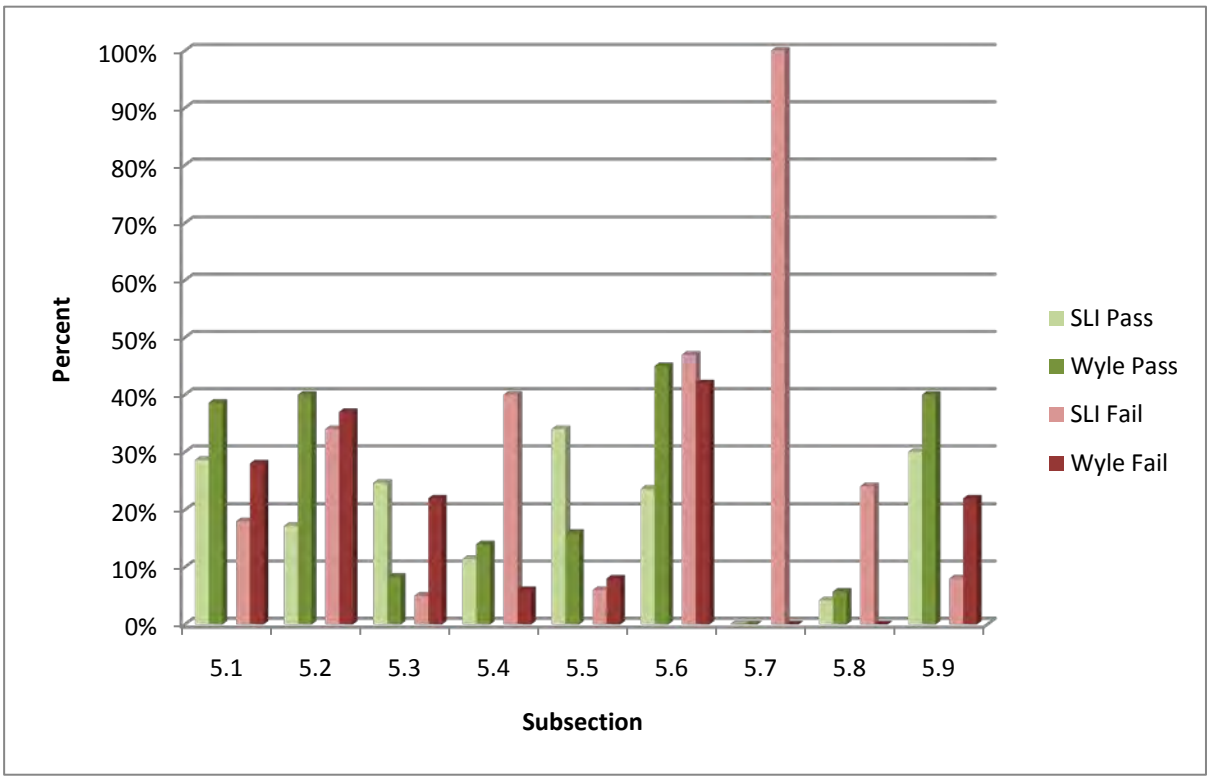
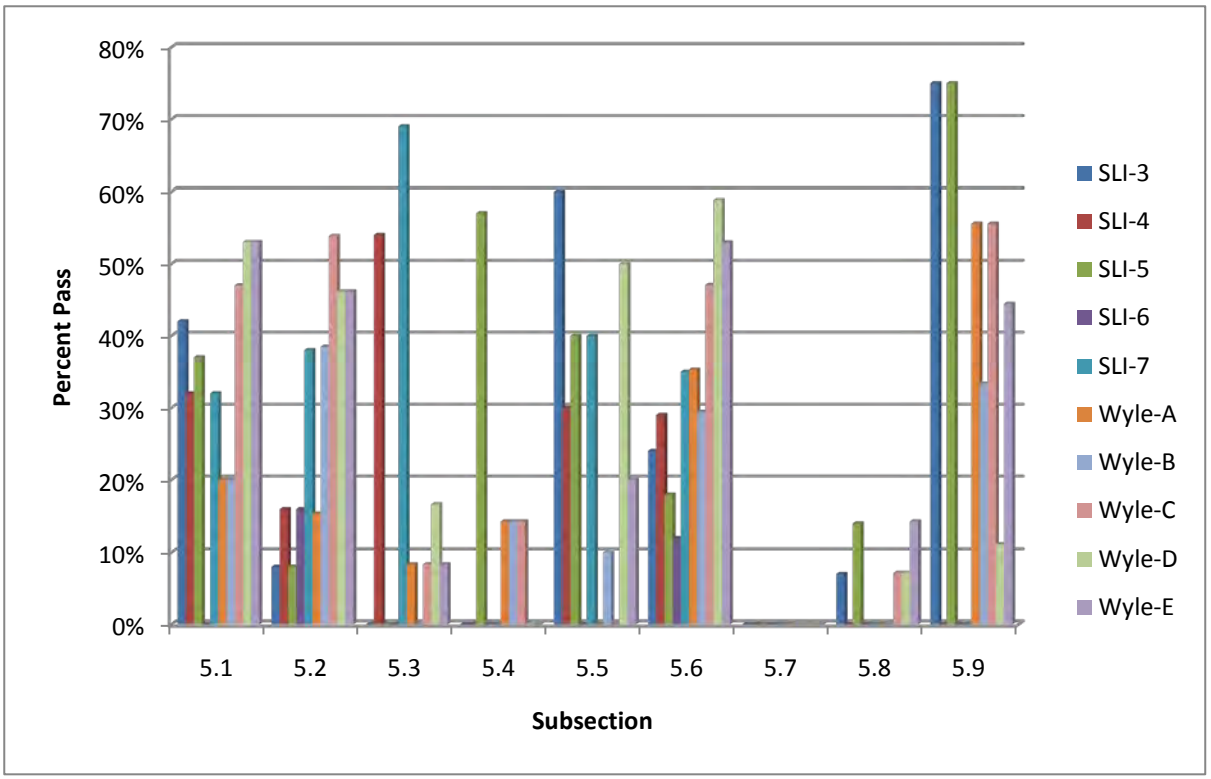


Figure 14b: Pass Percentages by System



4 Internet Voting Systems (IVS) Testing Results for UPPTR Section 2 (Functional Requirements) and Section 5 (Security)

This chapter analyses the test results performed by SLI of two systems for the requirements of Sections 2 and 5 of the UPPTR. SLI labeled the systems as "Manufacturer 1" and "Manufacturer 2" (referred to as Systems A and B in this chapter). In order to maintain their anonymity the vendor names were redacted. The SLI Test Report is located at Appendix E.

This chapter is divided into three subchapters; 4.1 reviews UPPTR Section 2; Subchapter 4.2 reviews UPPTR Section 5; and Subchapter 4.3 summarize both.

4.1 SLI's Testing Results for UPPTR Section 2 (Functional Requirements)

Testing incorporated end-to-end election scenarios testing of the functionality of the requirements of UPPTR Section 2 via a readiness test, designed to validate that the core functionality of a voting system is intact and functioning. The test created a baseline election and executed it in a basic election day scenario, which included; opening polls, voting ballots, closing polls, printing reports, transmitting results to pertinent locations unique to each system, and tallying results.

Section 2 of the UPPTR consists of the following subsections:

- 2.1 Accuracy
- 2.2 Operating Capacities
- 2.3 Pre-Voting Capabilities
- 2.4 Voting Capabilities
- 2.5 Post-Voting Capabilities
- 2.6 Audit and Accountability
- 2.7 Performance Monitoring

The test suites were customized for each voting system and conducted in conjunction with the inspection and functional testing as prescribed in the UPPTR and as applicable given the type of systems under review. The two vendors provided election creation and importation documentation relative for testing these requirements, as well as back office environments for SLI.

In Section 2 of the UPPTR, SLI tested based on 123 requirements and reported that 96 were testable as written, 25 require modification for testable, and recommended two for deletion. SLI's comments to these UPPTR requirements are included in Appendix C. The testing results and recommended changes to UPPTR Section 2 are discussed in Chapter 4 of this report. Figure 13 provides number of UPPTR requirements that are testable as written, require modification for better testability or deleted by subsection.

Figure 15: SLI's Assessment of the UPPTR Section 2 (Functional Requirement)

Section 2 (Functional Requirement)	Requirements	Testable	Modify	Delete
2.1 Accuracy	20	8	10	2
2.2 Operating Capacities	13	11	2	0
2.3 Pre-Voting Capabilities	8	8	0	0
2.4 Voting Capabilities	26	23	3	0
2.5 Post-Voting Capabilities	9	5	4	0
2.6 Audit and Accountability	44	39	5	0
2.7 Performance Monitoring	3	2	1	0
Total	**123**	**96**	**25**	**2**

4.1.1 Accuracy (UPPTR 2.1)

Subsection 2.1 of the UPPTR enumerates requirements addressing accuracy of data for each of the individual ballots selections that could be selected by a voter. Accuracy is defined as the ability of a voting system to; capture, record, store, consolidate and report the specific selections and absence of selections made by the voter on each ballot without error.

Both systems' data content accuracy was successfully verified in multiple stages, but the stages cited in the report were not consistent for both systems. However, both had consistency with write-in ballots and were confirmed at each stage. System A could be automated and tested at a high volume. For System B, it was not possible to automate the system and all testing was performed manually against the requirement of applying voting smartcards. Figure 14 depicts SLI test results.

Figure 16: Accuracy Test Results Averages

UPPTR Section 2.1 Accuracy	Pass	Fail	Not Tested	N/A
System A	88%	0%	12%	0%
System B	88%	0%	12%	0%

SLI provided comments and recommendations on portions of all 12 requirements in Subsection 2.1. The recommendations to modify the language of the UPPTR include; removing "SHALL" from the header paragraph, establishing standards for component accuracy, and changing some requirements to "Inspections".

4.1.2 Operating Capabilities (UPPTR 2.2)

Subsection 2.2 of the UPPTR enumerates requirements operating capabilities of the voting system, which includes notification and simultaneous transmissions. For System A, SLI was able to achieve high levels of data presentation to the accumulation center with the implementation of automated scripts. For System B, SLI was not able to achieve high levels of data presentation to the accumulation center without the

implementation of automated scripts, but no situation was encountered that caused issues of concern to be raised. Figure 15 compares the two systems.

Figure 17: Operating Capabilities Test Results Averages

UPPTR Section 2.2 Operating Capabilities	Pass	Fail	Not Tested	N/A
System A	75%	25%	0%	0%
System B	75%	25%	0%	0%

SLI provided comments and recommendations on portions of all four requirements. The recommendations to modify the language of the UPPTR include; change capacity requirement to meet a minimum NIST specification and changing some requirements to "Inspections".

4.1.3 Pre-Voting Capabilities (UPPTR 2.3)

Subsection 2.3 of the UPPTR enumerates requirements to import and protect election definition and provide a test mode to verify the voting system is correctly installed. System A successfully verified the capability to create / import election data, ballot instructions and election rules. Internet connectivity was required because this was a virtual testing environment. Before the ballots could be created / imported, it required secure credentials. System B imported and verified election detail successfully and ballot content was consistent with what was defined for each associated precinct. The ballot styles were also consistent with what appeared in the authentication laptop when searching on voter IDs. This system did not support the use of image files. Figure 16 compares the two systems.

Figure 18: Pre-Voting Capabilities Test Results Averages

UPPTR Section 2.3 Pre-Voting Capabilities	Pass	Fail	Not Tested	N/A
System A	50%	50%	0%	0%
System B	50%	50%	0%	0%

In this section, SLI recommended the UPPTR be modified to the activities for importing the election definitions.

4.1.4 Voting Capabilities (UPPTR 2.4)

Subsection 2.4 of the UPPTR enumerates requirements of voting capabilities during the voting period, which includes casting ballots, linking ballots to voter identification, and voting secrecy. The two systems had identical results as seen in Figure 17; however, SLI's spreadsheet (see Appendix E), cited Subsection 2.4.2.4.2 as "not testable, beyond scope" for both systems but their report did not recount any requirements as *Not Tested* in the chart located on page 48 of their report.

System A had the capability to open polls, access the ballot, verify voter selections, and cast the ballots. Voters' identities were never made available in the event logs nor could votes be viewed. System B could

cast ballots, allowed up to three changes before submission and provided a paper receipt for confirmation. The actions and voter identification were correctly encrypted.

Figure 19: Voting Capabilities Test Results Averages

UPPTR Section 2.4 Voting Capabilities	Pass	Fail	Not Tested	N/A
System A	67%	22%	0%	11%
System B	67%	22%	0%	11%

SLI provided comments and recommendations on six requirements. The recommendations to modify the language of the UPPTR include; creating a sub-requirement for voter modifying selections, splitting requirements, and requiring paper confirmation only when the ballot is cast.

4.1.5 Post-Voting Capabilities (UPPTR 2.5)

Subsection 2.5 of the UPPTR enumerates requirements for post voting capabilities which include ballot box retrieval and integrity check, and all aspects of tabulation. For System A, when voting results were successfully obtained and at no point could an individual's identity be traced to their ballot and it was not possible to determine a voter's selections before, during, or after decryption. This system encrypted with a public key; did not use a digital signature but the process did check the integrity of the ballot box. For System B, the ballot box file generated on the back office laptop was successfully signed and sealed but the system did not provide a direct application for checking the ballot box integrity, but any tampering with the encrypted file would be detected.

Figure 20: Post-Voting Capabilities Test Results Averages

UPPTR Section 2.5 Post-Voting Capabilities	Pass	Fail	Not Tested	N/A
System A	100%	0%	0%	0%
System B	100%	0%	0%	0%

SLI provided feedback on the eight requirements. The recommendations to modify the language of the UPPTR include; additional requirement for encryption, defining the term *seal*, and enumerating the activities for tabulation device connectivity.

4.1.6 Audit and Accountability (UPPTR 2.6)

Subsection 2.6 of the UPPTR enumerates requirements for audit and accountability of electronic and paper records. System A implemented significant logging but some deficiencies were noted with the write-in fields. Some of this system's tools did not implement log files preventing the recording of important events such as, poll opening / closings, internet protocol (IP) addresses of accessing systems. This system has two types of election definitions. One implements an election where the voter's choices are not transmitted to the back-end system and must be printed and faxed, emailed or mailed. The second

type of election is where the voters' choices are automatically transmitted via the internet and are not printed.

For System B, the tallying process on the back office computer successfully generated a file (a table for each precinct) that listed the number of votes for each contest. These tables could be printed but could not print the tally details. One issue was that the final tally file displayed a ballot count per precinct but did not differentiate whether they were the number received or the number counted. In addition, the final tally file did not display the number of rejected electronic cast vote records nor the sum total of ballots counted and received for all of the precincts combined. Figure 19 compares the two systems.

Figure 21: Audit and Accountability Test Results Averages

UPPTR Section 2.6 Audit and Accountability	Pass	Fail	Not Tested	N/A
System A	46%	8%	46%	0%
System B	75%	8%	17%	0%

SLI provided feedback on the 14 requirements. The recommendations to modify the language of the UPPTR include; using VVSG standard for electronic records testing and enumerating the actives for testing electronic records and multiple pages.

4.1.7 Performance Monitoring (UPPTR 2.7)

Subsection 2.7 of the UPPTR enumerates requirements for performance monitoring that includes network monitoring, tool access, and tool privacy. Neither system provided any specific application for monitoring the network. System A was left with its inherent roles access features to prevent any unauthorized monitoring. For System B, applying passive monitoring commands would not compromise either voter privacy or election integrity. Applying commands that alter network service, (e.g., stopping the web server or altering the firewall configuration) would not jeopardize voter privacy or the election integrity. Figure 20 compares the two systems.

Figure 22: Performance Monitoring Test Results Averages

UPPTR Section 2.7 Performance Monitoring	Pass	Fail	Not Tested	N/A
System A	67%	33%	0%	0%
System B	67%	33%	0%	0%

SLI's evaluation of the UPPTR language, they agreed with two requirements and recommended modification of network monitoring to provide additional detail on the level of monitoring required.

4.2 VSTL Testing Results for UPPTR Section 5 (Security)

The testing incorporated end-to-end election scenarios testing the functionality of all requirements of UPPTR Section 5 via a readiness test, designed to validate that the core functionality of a voting system is

intact and functioning. The test created a baseline election and executed it in a basic Election Day scenario that included opening polls, voting ballots, closing polls, printing reports, transmitting results to pertinent locations unique to each system, and tallying results.

Section 5 of the UPPTR consists of the following subsections:

- 5.1 Access Control
- 5.2 Identification and Authentication
- 5.3 Cryptography
- 5.4 Voting System Integrity Management
- 5.5 Communications Security
- 5.6 Logging
- 5.7 Incident Response
- 5.8 Physical and Environmental Security
- 5.9 Penetration Resistance

4.2.1 Access Control (UPPTR 5.1)

Subsection 5.1 of the UPPTR enumerates requirements for identification of authorized system users; identification of authorized processes and devices; and the authorization or verification of those identities as prerequisites to granting access to the system processes and data. Systems had appropriate access controls in place over each defined user, role, or group; however, the systems had deficiencies in their login functions and tabulation process configurations. System A had 5% *Not Tested* but the reason(s) were not documented. Figure 21 compares the two systems.

Figure 23: Access Control Test Results Averages

UPPTR Section 5.1 Access Control	Pass	Fail	Not Tested	N/A
System A	42%	53%	5%	0%
System B	84%	18%	0%	0%

4.2.2 Identification and Authentication (UPPTR 5.2)

Subsection 5.2 of the UPPTR enumerates authorization mechanisms and their associated strength must meet the minimum requirement to maintain integrity and trust. Split knowledge or dual authorization was necessary to ensure security; especially relevant for critical cryptographic key management functions. System A had 38% *Not Tested* due to the lack of documentation and the 8% *N/A* due to no VPN. System B had 8% *N/A* because of the lack of time to complete the testing. Figure 22 compares the two systems.

Figure 24: Identification and Authentication Test Results Averages

UPPTR Section 5.2 Identification and Authentication	Pass	Fail	Not Tested	N/A
System A	8%	46%	38%	8%

System B	54%	38%	8%	0%

4.2.3 Cryptography (UPPTR 5.3)

Subsection 5.3 of the UPPTR enumerates cryptography that serves several purposes which include; confidentiality, authentication, and random number generation. As seen in Figure 23, neither rated *Pass* for any of the requirements and 77% were *Not Tested*. No source code was reviewed and therefore could not test areas of the cryptography.

Figure 25: Cryptography Test Results Averages

UPPTR Section 5.3 Cryptography	Pass	Fail	Not Tested	N/A
System A	0%	23%	77%	0%
System B	0%	23%	77%	0%

4.2.4 Integrity Management (UPPTR 5.4)

Subsection 5.4 of the UPPTR addresses the secure deployment and operation of the voting system, including the protection of removable media and protection against malicious software. Functionally, neither system provided adequate transmission integrity or storage of cast vote data. Checks for malware detection or upgrade mechanisms were not sufficiently implemented on either system. For System A, cast vote storage and electronic ballot box integrity checks could be validated, but not for System B. System A had 29% *Not Tested* due to the lack of VSTL access and only System B could pass any requirements; however, the failure rate for both systems was very high. Figure 24 compares the two systems.

Figure 26: Integrity Management Test Results Averages

UPPTR Section 5.4 Integrity Management	Pass	Fail	Not Tested	N/A
System A	0%	71%	29%	0%
System B	23%	77%	0%	0%

4.2.5 Communications Security (UPPTR 5.5)

Subsection 5.5 of the UPPTR enumerates requirements for communications security ensuring the integrity of transmitted information and protecting the voting system from external communications-based threats. System A was insufficient in detailing how the data transmission integrity was protected with protocols, mutual authentication methods, or interface protections. System B was insufficient in detailing how communications security was implemented, to include the use of VPN and mutual authentication. Functionally, the VPN credentials could not be verified to meet the required standards and VPN usage precluded SLI from being able to determine how data was being encrypted. System A's 20% *Not Tested* was due to the lack of information and the 10% *N/A* was due to no VPN. System B's

60% *Not Tested* was due to VPN credentials could not be verified to meet the required standard without TDP. Figure 25 compares the two systems.

Figure 27: Communications Security Test Results Averages

UPPTR Section 5.5 Integrity Management	Pass	Fail	Not Tested	N/A
System A	60%	10%	20%	10%
System B	30%	10%	60%	0%

4.2.6 Logging (UPPTR 5.6)

Subsection 5.6 of the UPPTR enumerates requirements for the voting system to perform event logging for system maintenance troubleshooting, recording the history of system activity, and detecting unauthorized or malicious activity. Both systems were compliant with logging; logon and logoff events, abnormal shutdowns and restarts, power failures, removable media events, password changes, use of privileges and attempts to exceed privileges, access attempts to underlying resources, format of logs, maintaining voter privacy, timekeeping mechanisms, and opening and closing polls. The *Not Tested* rates were due to the VSTLs lack of access. Figure 26 compares the two systems.

Figure 28: Logging Test Results Averages

UPPTR Section 5.6 Logging	Pass	Fail	Not Tested	N/A
System A	24%	71%	5%	0%
System B	59%	29%	12%	0%

4.2.7 Incident Response (UPPTR 5.7)

Subsection 5.7 of the UPPTR enumerates requirements that the manufacturers document system operations or security critical events. No alarms were noted by either system during functional testing. System A did not provide a comprehensive list of what types of system operations or security events are critical but System B did. Figure 27 compares the two systems.

Figure 29: Incident Response Test Results Averages

UPPTR Section 5.7 Incident Response	Pass	Fail	Not Tested	N/A
System A	0%	100%	0%	0%
System B	50%	50%	0%	0%

4.2.8 Physical and Environmental (UPPTR 5.8)

Subsection 5.8 of the UPPTR enumerates requirements for physical and environmental security which includes physical access; alarms, voting capture devices, and counter security measures. Written results

for both systems were nearly identical in that during functional testing; only an authorized administrator could be re-enabled disabled ports. For System A, there was no evidence in the ability for the vote capture device to be automatically disabled if connections were broken. For System B, there was evidence in the ability for the vote capture device to be automatically disabled if connections were broken with peripheral components when the smartcard reader was removed and the system disabled the port. System A had 7% *Not Tested* because no associated kiosk and 15% *N/A* due to no peripheral devices. System B had 21% *Not Tested* because of the lack of peripheral devices. The lack of peripheral devices was reported differently for the two systems with no conclusive reason why. Figure 28 compares the two systems.

Figure 30: Physical and Environmental Test Results Averages

UPPTR Section 5.8 Physical and Environmental	Pass	Fail	Not Tested	N/A
System A	7%	71%	7%	15%
System B	50%	29%	21%	0%

4.2.9 Penetration Resistance (UPPTR 5.9)

Subsection 5.9 of the UPPTR enumerates requirements for penetration resistance attempts and penetration resistance test and evaluation. System A did not provide kiosk oriented hardware so SLI was not able to test against a hardened physical environment; however, the vendor was able to provide a local server, backend system (a suite of multiple devices) for penetration testing. Only a minimal port set was left open, and those were configured in an appropriately positive manner to prevent exploitation attempts – the system perform well. There were 215 known exploits successfully rebuffed. For system access and interfaces, 253 exploits were attempted and all rebuffed. System B provided kiosk oriented hardware and SLI was able to provide a local server, backend system for penetration testing. Only a minimal port set was left open, and those were configured in an appropriately positive manner to prevent exploitation attempts – the system performed well. There were 35 known exploits successfully rebuffed. For system access and interfaces, 35 exploits were attempted and all rebuffed. SLI reported that the testing performed on the provided equipment was successful overall in its security deployment. Figure 29 compares the two systems.

Figure 31: Penetration Resistance Test Results Averages

UPPTR Section 5.9 Penetration Resistance	Pass	Fail	Not Tested	N/A
System A	75%	8%	0%	17%
System B	75%	8%	0%	17%

4.3 VSTL Full system Testing Summary

SLI preformed full system testing on two systems against UPPTR Sections 2 and 5. Both systems contained the ability to import / create / modify election definitions, as well as conduct voting, accumulating, and tallying results.

SLI's spreadsheet at Appendix E of this report has numerous inconsistencies. The verbiage used regarding requirements that were labeled "can be met today" but test results stated "insufficient robustness" and "not tested" in Subsections 2.6.3.4 and 2.6.3.5, and in similar situations for other requirements.

Figures 30 and 31 on the next page summarize the reported results from this chapter. Figure 30 provides the results for UPPTR Section 2. Both systems had identical results, except for 2.6 (Audit and Accountability); Manufacture 1 had 46% Pass and 46% Not Tested, and Manufacture 2 had 67% Pass and 17% Not Tested. Figure 31 provides the test results for UPPTR Section 5 for both systems.

Figure 32: SLI Testing Average Results for UPPTR Section 2 (Functional Requirements)

UPPTR Section 2: Functional Requirements	Pass	Fail	Not Tested	N/A
2.1 Accuracy	88%	0%	12%	0%
2.2 Operating Capacities	75%	25%	0%	0%
2.3 Pre-Voting Capabilities	50%	50%	0%	0%
2.4 Voting Capabilities	67%	22%	0%	11%
2.5 Post-Voting Capabilities	100%	0%	0%	0%
2.6 Audit and Accountability	61%	8%	31%	0%
2.7 Performance Monitoring	67%	33%	0%	0%

Figure 33: SLI Testing Results for UPPTR Section 5 (Security)

UPPTR Section 5: Security	Manufacture 1				Manufacture 2			
	Pass	Fail	Not Tested	N/A	Pass	Fail	Not Tested	N/A

5.1 Access Control	42%	53%	5%	0%	84%	16%	0%	0%
5.2 Identification and Authentication	8%	46%	38%	8%	54%	38%	8%	0%
5.3 Cryptography	0%	23%	77%	0%	0%	23%	77%	0%
5.4 Voting System Integrity Management	0%	71%	29%	0%	23%	77%	0%	0%
5.5 Communications Security	60%	10%	20%	10%	30%	10%	60%	0%
5.6 Logging	24%	71%	5%	0%	59%	29%	12%	0%
5.7 Incident Response	0%	100%	0%	0%	50%	50%	0%	0%
5.8 Physical and Environmental Security	7%	71%	7%	15%	50%	29%	21%	0%
5.9 Penetration Resistance	75%	8%	0%	17%	75%	8%	0%	17%

5 Recommendations

This chapter covers recommendations for changes for all of the stakeholders of this test. The intent is to provide the VSTLs, the EAC and FVAP actionable information for improving their respective areas of responsibility in the testing process.

5.1 Recommendations for Changes to the UPPTR

The UPPTR contains requirements that, based on VSTL reports, need to be better defined or need more specificity. The requirements as currently written are open to interpretation by the VSTLs, vendors and other stakeholders. In formal testing efforts, the VSTLs would test systems against these UPPTR requirements. They develop test methods, test cases, and scripts to ensure that the voting system under test can meet these requirements as written. In this testing effort, VSTLs tested voting systems against the requirements in UPPTR Sections 2 and 5 only with less than formal certification requirements. Each VSTL interpreted many of the requirements differently and therefore we had different results in the testing. These requirements should be rewritten to remove any ambiguity or room for interpretation.

In UPPTR Section 5, SLI and Wyle made recommendations that 65 of the requirements be enumerated, split, modified or deleted for clarification and testability. In UPPTR Section 2, SLI made recommendations that 36 of the requirements be enumerated, split, modified or deleted for clarification and testability. The VSTLs' comments to the UPPTR are included in Appendix C. These recommendations need further analysis and synthesized into a change document for revisions to the UPPTR.

5.2 Recommendation for the VSTLs

Comparing and analyzing the VSTLs differences were found in their methodologies, breakdown and interpretation of the UPPTR requirements, method of testing and use of test cases, and results reporting. Chapter 2 of this report lays out the methodologies of each lab. The breakdown and interpretation of the UPPTR requirements can be clearly seen in the spreadsheet of each VSTL report (Appendices E and F). Wyle used a test plan but SLI did not, they did ad-hoc testing. The reports submitted by both VSTLs were very different.

Due to differences between each of the VSTL's interpretation of the UPPTR, variations in their testing methodologies, variations in definitions of *Pass* / *Fail* acceptance criteria, and variations in their need for vendor documentation for test case development, the current percentages for *Pass*, *Fail*, *Not Tested*, and *N/A* metrics are suspect and unreliable.

The EAC should publish along with the requirements the definition of all terms. That would include *Pass, Fail, Not Tested*, and *N/A.* With these definitions included in the requirements the VSTLs would have to accept them and grade the results of testing accordingly. Allowing each VSTL to interpret the requirements and how to reports the results give too much power to the VSTL. The VSTLs should also lobby the EAC for these changes as it would make reporting results more reliable and repeatable.

The requirements should not be left to interpretation. Each requirement should be written with as little ambiguity as possible. As example; UPPTR Subsection 5.1.2.1 states, "the voting system SHALL allow the administrator group or role to configure permissions and functionality for each identity". Wyle labs had a test script for this requirement whereas SLI stated it was NA. This difference in interpreting the requirements should not occur. The EAC should work with the VSTLs and NIST where applicable to attempt to write requirements that are clear and well defined.

The VSTLs described the need to remove some requirements from the UPPTR and move them to a new document called the *Program Manual*. It is recommended that the VSTLs define the Program Manual and the minimum contents for use in establishing test program scope, tailoring of the UPPTR to meet cost and schedule goals, risk assessment, assumptions and constraints, resources needed, and requirements for a specific test campaign.

The VSTLs did not test many of the requirements because the VSTLs did not have the necessary information to help them define sufficient test cases. The architectures of these electronic voting systems are significantly different from the architectures of current voting systems with which they were familiar and for which they have existing test cases for formal certification efforts. It is also recommended that the VSTLs define the minimum acceptable contents of the TDP which they will require from electronic voting system vendors to meet the requirements of the UPPTR.

Each vendor implemented their software solutions in different ways using their own development and testing methodologies. There are several self-certifying sections of the UPPTR which were not part of this current testing effort. The self-certifying sections of the UPPTR are those sections where the "Test Entity" is listed as "Manufacturer". The VSTLs should work with the vendors to help them to adopt best development and testing practices to improve the quality level of these self-certifying sections.

5.3 Recommendations for Standardizing Processes and Measurements for Future FVAP Testing

This testing effort has established an initial benchmark showing gaps in the UPPTR which need to be resolved and a rough order of magnitude measurement (percent passed) where the vendors (on average) meet these UPPTR requirements. As documented in the results section of this report, there is variation in the test results received from each of the VSTLs as well as variation in the results observed from each of the vendors.

Better testing requirements and defined test and measurement standards are recommended for a future round of VSTL testing which will build on this VSTL benchmark. One example for standardizing measurement may be to have the EAC define exactly what is meant by *Pass, Fail, Not Tested,* and *N/A*. The VSTLs should not be given the ability to formulate their own definitions to these measurable results.

The report has many examples of differing interpretation of the requirements. A requirement written in plain language with more specificity would help the VSTL in conducting tests according to the requirements. It may also help to standardize the methodologies used by the VSTLs because interpretation of the requirements would not be difficult or impossible.

The labs also had differing definitions *Pass, Fail, Not Tested,* and *N/A.* As stated above the EAC could define these terms and place them in the UPPTR. The labs would then be reporting the same results with the same meaning. This would allow for a better one-to-one comparison of results without another interpretation being made by the analyst.

Defining the exact format and of the VSTL final report would also be helpful. Having a standardize report and content would make comparing the results from each lab much simpler. A better defined report done in conjunction with the recommendations above would provide an opportunity for more precise analysis of the results and the methodology of each VSTL. Two separated reports formatted entirely differently and with the content reported in different ways leads to some time consuming analysis.

5.4 Recommendations for Further Testing

The conclusion of this initial testing effort provides a baseline for the quality of the UPPTR as written. It also provides the vendors information on their product's ability to conform to the requirements. The VSTLs gained information on how their testing methodologies and practices may need to be altered in order to test the new requirements. This information is useful but there is more work that can be done to improve the EAC requirements to which the voting systems must conform, and shape how the VSTLs test the voting systems. Below are recommended testing scenarios that may provide more actionable information for all stakeholders.

1. Conduct a complete evaluation of the VSTLs' recommendations and provide FVAP and EAC with recommendation for changes to the UPPTR.
2. The voting system vendors would then re-submit the same voting systems that were used in the first round of testing to the VSTL to have them re-tested to the updated versions of UPPTR Sections 2 and 5. A comparison of the data before and after the changes could be made. This may help the EAC to determine if the changes made were of value or perhaps there are more changes needed.
3. Take one system from a selected vendor and place the system with each of the VSTLs and have the system tested against the entire UPPTR to include TDPs, trusted builds and a line-by-line source code review. This would provide a direct comparison to the VSTLs methodologies, test scenarios, test results and how they report their findings. This data may help to determine if one of the labs provides a better product that the other or if one methodology is preferred over another. The direct comparison of the two VSTLs may help provide the EAC with data needed to ensure that the same quality of testing is performed in each lab.
4. Submit some new technologies (Smart phones, tablets, and notepads) into VSTL testing. These devices should be able to conform to the requirements of the security of UPPTR Section 5 the same as any other voting system. There may also be a possibility of testing these devices to the requirements in UPPTR Section 2. Various types and models of these technologies could be tested using the UPPTR and the data may point to one type of technology or even one model of a manufacturer to be preferred. This data may help the EAC to begin to develop new standards or

update the UPPTR to include these types of devices. The vendors would also gain useful knowledge on how these devices may be tested for certification in the future.

This is not meant to be an all-inclusive list of possible testing efforts but rather a glimpse at some of the possibilities for testing. The EAC, the voting system vendors, and the VSTLs all gain useful information about their processes, their products, and the usability of their requirements through independent testing. FVAP can benefit from the fact that they are providing useful information to its partners in the EAC and to the election technology industry.

Appendix A – Glossary

Administrator	The role responsible for installing, configuring, and managing the technical operations of the system.
Back - office	Not related to the actual voting process. Computers or operations needed to support an election; not involved in capturing a vote or tallying that vote.
Ballot	The official presentation of all of the contests to be decided in a particular election. See also ballot image, cast vote record, and paper record.
Certification	Certification is the process by which the EAC, through testing and evaluation conducted by an accredited Voting System Test Laboratory, validates that a voting system meets the requirements set forth in existing voting system testing standards (Voting System Standards [VSS] or VVSG), and performs according to the Manufacturer's specifications for the system. An EAC certification may be issued only by the EAC in accordance with the procedures presented in this Manual. Certifications issued by other bodies (e.g., the National Association of State Election Directors and State certification programs) are not EAC certifications.
Component	A discrete and identifiable element of hardware or software within a system.
Contest	A single decision being put before the voters (e.g., the selection of a candidate for office or the response to ballot questions).
COTS	Commercial Off the Shelf.
Cryptography	The protection of information by converting the information into an unreadable format.
Device	Functional unit that performs its assigned tasks as an integrated whole.
EAC	Election Assistance Commission - provides for the testing and systems certification through the Voting System Testing and Certification Program.
Electronic Ballot Delivery System	This system is electronically based (either stand alone or internet-based) and includes functionality for printing and signing the ballot. The user then has the option of submitting the ballot via postal mail, fax or email depending on the rules of their voting jurisdiction.
Election Definition	Definition of the contests and questions that will appear on the ballot for a specific election.

Election Officials	The persons responsible for administering and conducting elections.
Firmware	1) Firmware is a combination of software and hardware. Computer chips that have data or programs recorded on them are firmware. These chips commonly include the following: • ROMs (read-only memory) • PROMs (programmable read-only memory) • EPROMs (erasable programmable read-only memory) Firmware in PROM or EPROM is designed to be updated if necessary through a software update. 2) In electronic systems and computing, firmware is a term often used to denote the fixed, usually rather small, programs and/or data structures that internally control various electronic devices.
Functional	Functional testing is the determination through operational testing of whether the behavior of a system or device in specific scenarios conforms to requirements. Functional tests are derived by analyzing the requirements and the behaviors that should result from implementing those requirements.
FVAP	Federal Voting Assistance Program - assists active duty uniformed service members, their families, and overseas voters in exercising their right to vote by absentee ballot when they are away from their permanent address.
Inspection	Examination of a product design, product, process or installation and determination of its conformity with specific requirements or, on the basis of professional judgment, with general requirements.
Internet Voting System	This system functions entirely online and includes internet-based submission of the ballot from within the system.
Kiosk	A terminal tasked to display information, accepts user input, and transmits information.
Module	Structural unit of software or analogous logical design, typically containing several callable units that are tightly coupled.
MOVE	Military and Overseas Voters Empowerment Act - Passed in 2009, it clarifies the procedures for absent uniformed services and overseas voters with respect to absentee registration and voting for all Federal elections by both mail and electronically.
NIST	National Institute of Standards and Technology.
SERVE	Secure Electronic Registration and Voting Experiment.
Source Code	Software that is written by a programmer in a language readable by people but not by computers.

TDP	Technical Data Package.
Test Case (IEEE 610)	A set of test inputs, execution conditions, and expected results developed for a particular objective, such as to exercise a particular program path or to verify compliance with a specific requirement.
Test Case	A set of conditions or variables under which a tester will determine whether an application or software system is working correctly or not. A test case is usually a single step, or occasionally a sequence of steps, to test the correct behavior / functionalities, features of an application. An expected result or expected outcome is usually given.
Test Module	A small set of test steps based on a single function or scenario, such as logging into an election management system or recording a vote.
Test Procedure	A group of test modules that are implemented to perform a specific function within a test suite, such as creating an election definition, voting in a polling location, tallying and reporting results.
Test Suite	A group of test modules designed to test a set of functions of a voting system or device.
Trusted Build	A build of software and/or firmware elements of the voting system by the VSTL according to procedures established by the manufacturer. A build is the process whereby source code is converted to machine-readable binary instructions (executable code) for the computer.
Test Entity	The responsible organization for conducting UPPTR testing; can be either the VSTL or the vendor.
UOCAVA	Uniformed and Overseas Citizens Absentee Voting Act.
UPPTR	UOCAVA Pilot Program Testing Requirements.
Use Case	A description of steps or actions between a user and a software system which leads the user towards something useful. Test Cases can be derived from Use Cases.
Vendor	Entity with ownership and control over a system submitted for testing.
Vote Capture Device	Device that is used directly by a voter to vote a ballot.
Voted Ballot	Ballot that contains all of a voter's selections and has been cast.
VOI	Voting Over the Internet.
Voter Privacy	The inability of anyone to observe, or otherwise determine, what selections a voter has made.

Voting System	Equipment (including hardware, firmware, and software), materials, and documentation used to define elections and ballot styles, configure voting equipment, identify and validate voting equipment configurations, perform readiness tests, activate ballots, capture votes, count votes, generate reports, transmit election data, archive election data, and audit elections.
VSTCPM	Voting System Testing and Certification Program Manual
VSTL	Voting System Test Laboratory. Laboratories accredited by the EAC to test voting systems to EAC approved voting system standards. Each Voting System Test Laboratory (VSTL) must be accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and recommended by the National Institute of Standards Technology (NIST) before it may receive an EAC accreditation. NVLAP provides third party accreditation to testing and calibration laboratories. NVLAP is in full conformance with the standards of the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC), including ISO/IEC Guide 17025 and 17011.
VVSG	Voluntary Voting System Guidelines. Voluntary voting system standards developed, adopted, and published by the EAC. The guidelines are identified by version number and date. (Version 1.0; 2005)
VVSS	EAC 2002 Voluntary Voting System Standards.
White-Box Testing	A test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. Also known as detailed testing.
Write-In	To make a selection of an individual not listed on the ballot.

Appendix B

UOCAVA PILOT PROGRAM TESTING REQUIREMENTS

Uniformed and Overseas Citizens Absentee Voting Act Pilot Program Testing Requirements

AUGUST 25, 2010

Table of Contents

Intentionally left blank

Section 1: Overview

1.1 Background

1.1.1 UOCAVA Pilot Projects

The Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) of 1986 protects the right to vote in federal elections for this defined category of citizens. UOCAVA sets out federal and state responsibilities to assist these voters in exercising their voting rights. The Secretary of Defense is the presidential designee responsible for the federal functions of the Act. The Federal Voting Assistance Program (FVAP) administers this law on behalf of the Secretary of Defense and works cooperatively with other federal agencies and state and local election officials to carry out its provisions.

UOCAVA legislation was enacted before the advent of today's global electronic communications technology. Consequently it relied on U.S. domestic and military mail systems as well as foreign postal systems for the worldwide distribution of election materials. By the mid-1990s it became apparent that the mail transit time and unreliable delivery posed significant barriers for many UOCAVA citizens, preventing them from successfully exercising their right to vote. At the same time the Internet was being widely adopted by businesses, governments and the general public. Therefore it was a natural development for FVAP and states to consider the potential of the Internet as an alternative to the "by-mail" UOCAVA process.

FVAP sponsored Voting Over the Internet (VOI), a small pilot project for the November 2000 general election, to examine the feasibility of using Internet technology. Four states participated in this experiment, which enabled voters to use their own personal computers to securely register to vote, request and receive absentee ballots, and return their voted ballots. Following the successful completion of the VOI project, in the Fiscal Year 2002 National Defense Authorization Act (§1604 of P.L. 107-107:115 Stat.1277), Congress instructed the Secretary of Defense to carry out a larger demonstration project for the November 2002 general election. This project was to be "carried out with participation of sufficient numbers of absent uniformed services voters so that the results are statistically significant".

Since there was not sufficient time to define and implement a large project for 2002, the project was planned for implementation for the November 2004 election. Seven states agreed to participate and worked with FVAP to develop system requirements and operating procedures. However, the Secure Electronic Registration and Voting Experiment (SERVE) was cancelled before it was deployed due to concerns raised by several computer scientists. These individuals contended that the use of personal computers over the Internet could not be made secure enough for voting and consequently called for the project to be terminated. The Department of Defense, citing a lack of public confidence in the SERVE system, decided the project could not continue under these circumstances.

In response to this development, the Fiscal Year 2005 National Defense Authorization Act (§567 of P.L. 108-375;118 Stat.119) repealed the requirement for the Secretary of Defense to conduct an electronic voting demonstration project "until the first regularly scheduled general election for federal office which occurs after the Election Assistance Commission (EAC) notifies the Secretary that the Commission has established electronic absentee voting guidelines and certifies that it will assist

the Secretary in carrying out the project". Pursuant to this legislation, in September 2005, the EAC requested its voting system advisory group, the Technical Guidelines Development Committee (TGDC), to add this subject on their research agenda; however the request was declined. This effectively put all federally-sponsored projects involving electronic return of voted ballots on indefinite hold.

After the cancellation of the SERVE Project in 2004, FVAP developed and fielded the Interim Voting Assistance System (IVAS). This system provided for electronic submission of ballot requests and delivery of blank ballots using a Department of Defense secure server. The voter was notified by email when their ballot was available on the server. Then they could download and print the ballot, mark their selections and return the voted ballot by postal mail or facsimile, if their state permitted this option. Use of this system was restricted to voters enrolled in the Defense Enrollment Eligibility Reporting System (DEERS), which was the source for voter identification validation. A total of 108 counties in 9 states participated in this project. One hundred forty-nine voters submitted ballot requests and 17 voters received blank ballots.

In 2006 the capabilities of IVAS were extended to enable all UOCAVA voters to use the system for submitting ballot requests. This was used by 470 jurisdictions in 8 states. FVAP could not measure how many voters used this option. As in 2004, voters in the DEERS database could also receive blank ballots using the system. This capability was used by 103 jurisdictions in 3 states. Sixty-three voters submitted ballot requests and 29 downloaded blank ballots.

In 2008 IVAS was further modified to enable all UOCAVA voters to make ballot requests and receive blank ballots. This enhanced capability was called the Voter Registration/Ballot Delivery System. It was used by 45 jurisdictions in 11 states. Over 21,000 voters completed a ballot request form and 780 uploaded these forms to the system. One hundred twenty-four voters downloaded blank ballots.

Since the State of Florida conducts its own voting system certification process, Okaloosa County, Florida, decided to field a small pilot for the 2008 general election that would enable voters to return their voted ballots electronically. Okaloosa County set up staffed remote electronic voting locations called "kiosks" in England, Germany and Japan. These sites were equipped with vote capture devices connected by a secure communications link to a system server. Voters came to the site and used the vote capture devices to receive, mark and cast their ballots electronically. The cast ballots were encrypted and transmitted back to the system server where they were stored until the Okaloosa Canvassing Board was ready to decrypt and tabulate them at the close of the election. The kiosk workers who staffed these sites verified voter identity and eligibility using an on-line connection to the voter registration system. A paper record of each vote was printed and used to verify the electronic results when the votes were tabulated. Ninety-three voters cast their ballots using this system.

Also in 2008 the Arizona Secretary of State's office developed and implemented a web-based system to enable voters to securely return their voted ballots electronically. This system, called the Military and Overseas Voting System, is still operational. Voters can request to register to vote and/or request an absentee ballot. When a request is received, an email is sent to the voter's jurisdiction with the voter's information to prompt the local election office to send a Federal Post Card Application and/or an absentee ballot. Ballots are sent to the voter by postal mail, email or facsimile. The local election office also authorizes the voter to use the Military and Overseas Voting System to return their voted ballot. An email is generated by the system that provides the voter with instructions for returning their ballot and a password. When they receive the ballot, the voter marks their selections and scans the ballot image into a computer file. Then they log onto the system and upload the voted ballot. The system sends an email to the voter to confirm that the ballot was

received. The appropriate county official also receives an email that a ballot has been received so they can download it for processing and tabulation.

1.1.2 Testing Pilot Systems

Most states require voting systems to undergo a testing and certification process before the system may be used in an election. This provides a level of assurance that the system provides the required functionality and operates reliably and securely. The four states participating in the VOI project agreed to test that system utilizing the Department of Defense Information Technology Security Certification and Accreditation (DITSCAP) process combined with the State of Florida Division of Elections Voting Systems Certification process. The testing regimen planned for the SERVE system was a combined DITSCAP, National Association of State Election Directors (NASED), and State of Florida certification and accreditation process. The system used for Okaloosa County's remote voting pilot was tested and certified by the State of Florida Division of Elections.

Due to the nature of these new systems, existing voting system standards were not sufficient for testing specific aspects. Therefore, additional security requirements were needed to test the use of digital signatures, cryptography and secure communications protocols. The hardware and software standards, developed for DRE and optical scan systems used in polling places, also needed to be revised to reflect the characteristics of the remote voting technologies. Each of these pilot projects established a working group, comprised of election officials, security experts and test engineers, to define the additional requirements needed to supplement the existing voting system standards. Reference materials for the working groups came from various national and international sources of information technology standards, such as the Federal Information Processing Standards (FIPS), Common Criteria, and the International Standards Organization. These efforts resulted in testing requirements documents that were specific to the technical features of each of the pilot systems, which supplied the criteria for testing and certifying these particular pilot systems.

Since 2008, several states have enacted legislation enabling them to conduct electronic voting projects for UOCAVA voters, beginning with the 2010 elections. To be prepared to support the states with these projects, in July 2009 the EAC convened a UOCAVA Working Group to consider how to adapt the EAC's Testing and Certification Program to accommodate UOCAVA pilot systems. It was concluded that two products were needed: a modified set of system testing requirements; and a revised testing and certification process. It was determined that the working group would assist the EAC in drafting the testing requirements. The EAC staff would adapt the certification process to accommodate the needs of UOCAVA pilot projects and publish a Voting System Pilot System Testing and Certification Manual.

The EAC UOCAVA Working Group began with a review of the Voluntary Voting System Guidelines (VVSG) 2005; the Revision to the 2005 VVSG; and the Next Iteration to the VVSG to identify already established or proposed TGDC guidelines that would also apply to remote electronic voting systems. To fill gaps related to the introduction of technologies not covered in the VVSG and the additional security requirements associated with remote systems, VOI, SERVE and Okaloosa Project requirements documents were reviewed. In addition, FIPS and NIST Special Publications were consulted to identify federally specified information security requirements that would apply to the use of cryptography, public key infrastructure, secure communications and other security features of remote electronic voting systems.

A significant challenge for the EAC Working Group was to specify requirements that would not unduly constrain innovation in the design of UOCAVA systems. The VOI, SERVE and Okaloosa system testing requirements were tailored to test the particular system implementations developed for those projects. However, since many different designs for remote voting systems could be submitted to the EAC certification program, the EAC Working Group needed to identify generic system requirements to allow for system design flexibility. This document is the result of that effort.

1.1.3 Scope of EAC Pilot Project Testing Requirements

Pilot projects are small in scale and short in duration. Consequently, certification for pilot systems needs to be quicker and less expensive than the regular process currently used for conventional systems with an expected life of more than 10 years. Nevertheless, since actual votes will be cast on the pilot voting systems, the certification process must retain sufficient rigor to provide reasonable assurance that these systems will operate correctly and securely.

There is a fundamental dichotomy in complexity in remote voting system architectures: those where the vote capture device is controlled (e.g., provided by the election jurisdiction); and those where it is not controlled (e.g., the voter uses his own personal computer). Since the EAC planned to have the pilot certification process ready for implementation during the first half of 2010, it was decided that the EAC would focus its efforts on controlled platform architectures servicing multiple jurisdictions. This is a highly secure remote voting solution and the Okaloosa Project, which used remote kiosks with vote capture devices provided by the Supervisor of Elections office, provides an implementation example for reference. Defining requirements for this class of system architecture was determined to provide a reasonable test case that could be completed within the available timeframe. In addition, most of the core system processing functions are the same for both types of architectures, so a substantial number of requirements will carry over as this work is expanded by the TGDC to include other methods of remote electronic voting. This pilot testing requirements document will be provided to the TGDC as the basis and starting point for their research and deliberations.

1.1.4 Next Steps

While the EAC was working to ensure that the pilot certification effort was underway, legislation dealing with a number of UOCAVA voting issues was under consideration by Congress. Ultimately passed as part of the Fiscal Year 2010 National Defense Authorization Act (NDAA) (§581 of P.L. 111-84), the Military and Overseas Voters Empowerment Act contains a provision allowing the Secretary of Defense to establish one or more pilot programs to test the feasibility of new election technology for UOCAVA voters. This provision requires the EAC and the National Institute of Standards and Technology (NIST) to provide best practices or standards to support these pilot programs, “in accordance with electronic absentee voting guidelines established under” the earlier FY2005 NDAA. In December 2009, the EAC directed the TGDC to begin this work as a top research priority. The EAC expects the TGDC to make recommendations for the comprehensive set of remote electronic voting system guidelines mandated by the FY2005 NDAA. The TGDC has been tasked to consider the full range of remote voting architectures, including instances where the voter uses his own personal computer for voting.

1.2 EAC Certification Scope for UOCAVA Pilot Systems

An initial step in a system certification process is to define the boundaries of the system that will be tested and certified. There are several significant differences between UOCAVA remote electronic voting systems and conventional voting systems used in polling places. UOCAVA pilot systems operate as adjuncts to existing election administration systems in the participating jurisdictions. Pilot systems require election definition data from the local Election Management System (EMS) to set up the system for the election and define ballots. Information from the Statewide Voter Registration Database is needed to authenticate voters and determine their eligibility to vote, match them with the correct ballot style, and record voter history. Some processes that are handled procedurally in a polling place may be performed by a software application in a remote electronic system. Use of communications networks is necessary to connect to voters. Since the UOCAVA voting period currently extends for 45 days, pilot systems may be in operation for several weeks before polling place systems are activated for Election Day. Most, if not all, states prohibit tabulation of absentee ballots until after the polls are closed, so voted ballots may have to be stored on the system for several weeks. Pilot tabulation results will be integrated with the tabulation report generated by the local EMS. Consequently, there are many factors to consider when determining the scope for pilot system certification testing.

Figure 1-1 illustrates a generic process flow for remote electronic voting that does not presuppose any particular architectural solution. Even at this high level of abstraction, two alternative processing paths are needed to accommodate differences in individual state requirements. The first path, called the absentee model, has two distinguishing features. This is essentially an electronic rendering of the UOCAVA by-mail process. In this path, the voter's identity must remain linked to the cast ballot until the close of the voting period. At that time adjudication is made by the local jurisdiction on whether to accept or not accept the ballot. If the ballot is accepted, any identifiable link to the voter is removed. The now anonymous ballot is placed in the ballot box to be tabulated. If the ballot is rejected, the link is not removed and the disposition of the 'unopened' ballot is made in accordance with individual state procedures.

The second path, called the early voting model, does not maintain any association between the voter and the cast ballot. When the voter presses the 'Vote' button and receives notification that their ballot selections have been recorded, the ballot goes directly into the ballot box. There is no ballot adjudication step and therefore no need to maintain a connection between the voter and the ballot.

There are many of ways in which systems can be designed to perform these absentee functions. However, for the reasons discussed in 1.1.3, only one type of system architecture – kiosk-based remote voting -- is addressed in this document. There are four major components in kiosk-based voting systems:

1. A system server which runs the voting software, stores voted ballots, and provides system administration functions;
2. One or more kiosks which are designated remote locations that service multiple election jurisdictions are staffed by kiosk workers who verify voter identity and eligibility, and are equipped with electronic vote capture devices with printing capability.
3. A tabulation device at each participating local election office which decrypts and tabulates the ballots for that jurisdiction; and
4. Communications links which tie all the system components together.

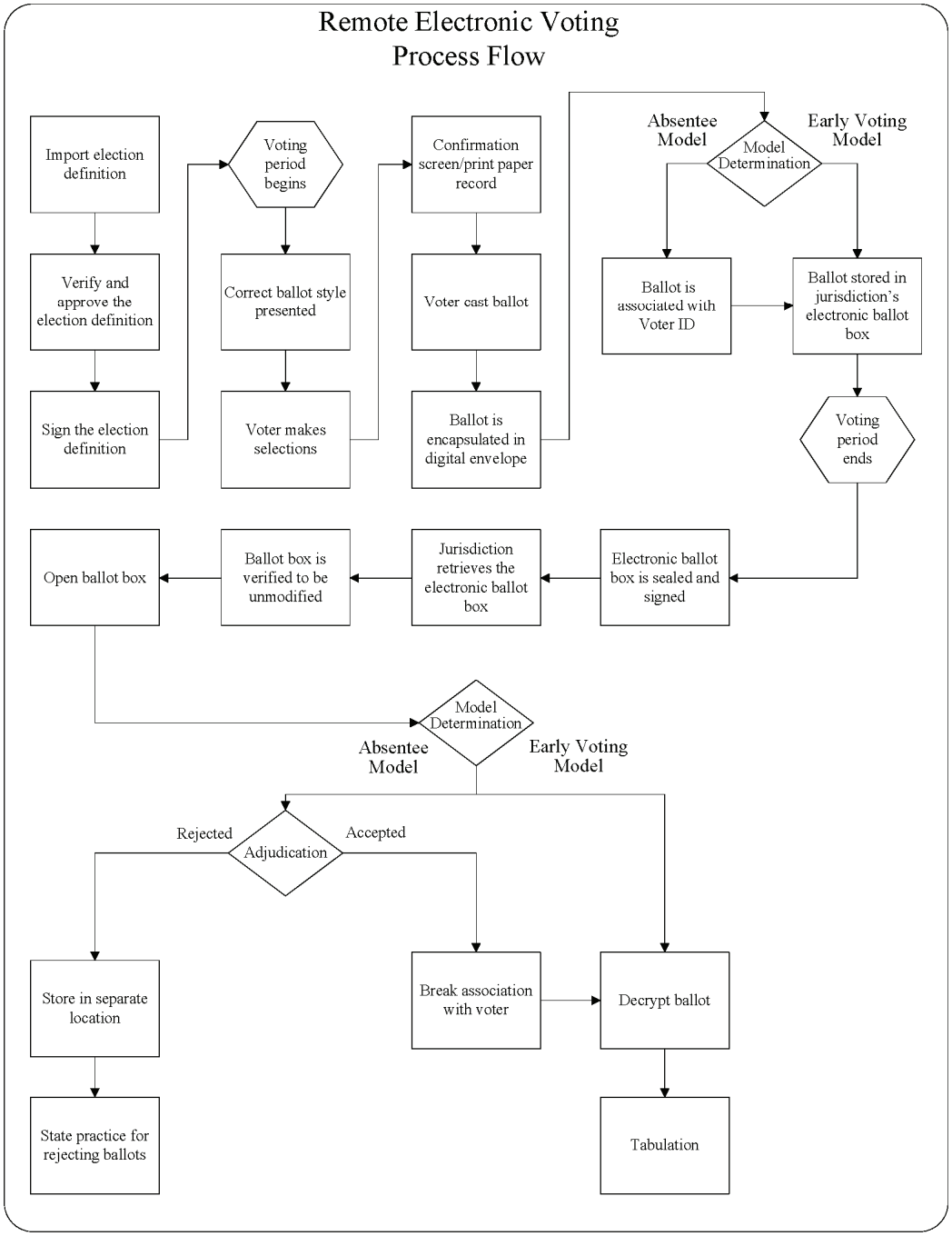
For security purposes, no vote data is permanently retained by the vote capture device. The cast ballot is transmitted to an electronic ballot box stored on the system server. The

vote capture device produces a paper record of the voter's choices that the voter can review for verification purposes. The paper records will be deposited in a secure receptacle and returned to the appropriate jurisdiction for system audit purposes. Other elements of the system architecture are not specified.

All the system components supporting the functions inside the frame in Figure 1-1 are subject to EAC pilot certification testing. Any system submitted to the EAC for pilot certification must support both the absentee and early voting models. The interfaces between the pilot system and the local EMS are not included in EAC testing. Should a pilot jurisdiction decide to develop a software wizard or other automated method to move data between the EMS and the pilot system, that jurisdiction will be responsible for validating that element. Similarly, if a jurisdiction decides to provide an automated means for kiosk workers to access voter registration data to validate voter identity and eligibility, the jurisdiction will be expected to validate its performance.

It is important to bear in mind that, although kiosk-based remote electronic voting may appear to be very similar to poll site voting, there are some very significant differences in the underlying legislative basis and the policies and procedures that flow from that. UOCAVA voting is by definition absentee voting. The process employed in UOCAVA voting pilots follows the same rules as the conventional postal delivery process. This means that the voting period could begin 45 days or more before Election Day, depending on state law. If some event, such as a law suit or an accident, causes a change in candidates in a race after the UOCAVA voting period begins, there must be a defined protocol for how to count that race in ballots that have already been cast if those voters don't have an opportunity to vote again with a replacement ballot. Since kiosks could be located in many different time zones, the system server hosting the voting application has to be available essentially 24 hours a day, seven days a week. Therefore, the electronic voting process would most likely have to be interrupted to change the ballot definition data and rerun logic and accuracy testing. Since this is an absentee voting process, provisional ballots are not available. For the same reason, there are no legally-mandated accessibility requirements. For those states following the absentee model of UOCAVA voting described above, there is a formal process to decide whether or not to accept a ballot for counting. Consequently, UOCAVA system requirements will vary somewhat from those for poll site systems.

Figure 1-1 UOCAVA Process



1.3 Conformance Clause

1.3.1 Scope and Applicability

This document defines requirements for conformance of kiosk-based remote electronic voting systems, intended for use in UOCAVA pilot programs, that manufacturers of such systems SHALL meet pursuant to EAC pilot program

certification. As described in 1.2, these systems consist minimally of a system server connected through secure communications links to a number of staffed remote kiosk locations equipped with vote capture devices. The vote capture devices display the ballot data provided by the system server to the voter and capture the electronic record of voter choices. These choices are securely transmitted back to the server for storage when the ballot is cast. The vote capture device also prints a paper record for voter verification which is retained for use in system performance validation. The system server is also connected through secure communications links to each participating local election jurisdiction to transfer the encrypted ballot file at the close of the election period. This file is manually transferred to a standalone, air-gapped tabulation device which decrypts and tabulates the ballots. The functionality of each of these components and the integrated system functional performance and security features will be tested during the certification process.

EAC pilot system certification testing will not include pilot system linkages to local voter registration and election management systems except for defined data interchange interfaces. It is the responsibility of the participating state and local jurisdictions to validate the functionality of any connections to their local systems. It should also be noted that these testing requirements only relate to the performance of system hardware and software, they do not extend to election administration procedures. However, requirements are included for system documentation and the ability to produce data needed to support procedures such as system audit.

This document also provides the framework, procedures, and requirements that voting system testing labs (VSTLs) and manufacturers responsible for the certification testing of such pilot program systems SHALL follow. The requirements and procedures in this document may also be used by states to certify kiosk-based remote electronic voting systems for their own pilot programs.

This document defines the minimum requirements for remote electronic voting systems in the context of pilot programs conducted by states and local jurisdictions and the process for testing these systems. The requirements are intended for use by:

- Designers and manufacturers of voting systems;
- VSTLs performing the analysis and testing of systems in support of the EAC certification process;
- Election officials, including officials responsible for the installation, operation, and maintenance of voting systems for UOCAVA pilot programs; and
- VSTLs and consultants performing the state certification of voting systems for pilot programs.

Minimum requirements specified in this document include:

- Functional capabilities;
- Performance characteristics, including security;
- Documentation; and
- Test evaluation criteria.

1.3.2 Conformance Framework

This section provides the framework in which conformance is defined. It identifies the entities to which these requirements apply, the relationships among the various entities, the structure of the requirements, and the terminology used to indicate conformance.

1.3.2.1 Applicable entities

The requirements, prohibitions and options specified in these requirements apply to kiosk –based remote electronic voting systems, voting system manufacturers, and VSTLs. These requirements apply to all systems submitted for pilot certification under the EAC program.

1.3.2.2 Requirements of entities

It is the voting system manufacturer that must implement these requirements and provide the necessary documentation for the system. In order to claim conformance to the requirement, the voting system manufacturer SHALL satisfy the specified requirements. The voting system manufacturer SHALL successfully complete the prescribed test campaign with an EAC VSTL in order to obtain EAC certification.

The VSTL SHALL satisfy the requirements for conducting pilot program certification testing. Additionally, as indicated in the document, certain requirements SHALL be tested by the manufacturer rather than the VSTL. The VSTL may use an operational environment emulating that used by election officials as part of their testing to ensure that the voting system can be configured and operated in a secure and reliable manner according to the manufacturer's documentation and as specified by the requirements. The VSTL SHALL coordinate and deliver the requisite documentation, including a Test Plan and a Test Report, to the EAC for review and approval.

The EAC SHALL review the test results and associated documentation from both the VSTL and the manufacturer and make a determination that all requirements have been appropriately tested and the test results are acceptable. The EAC may conduct audits of manufacturer testing to ensure its adequacy. The EAC will issue a pilot program certification number that indicates conformance of the specified system to these requirements.

1.3.3 Extensions

Extensions are additional functions, features, and/or capabilities included in a voting system that are not required by this document. To accommodate the needs of states that may impose additional requirements and to accommodate changes in technology, this document allows extensions. The use of extensions SHALL NOT contradict nor cause the nonconformance of functionality required by this document.

1.3.4 Implementation Statement

The implementation statement SHALL describe the remote electronic voting system and SHALL document the requirements that have been implemented by the voting system. It SHALL also identify optional features and capabilities supported by the voting system, as well as any extensions (i.e., additional functionality beyond what is required in this document). The implementation statement SHALL include a checklist identifying all the requirements for which a claim of conformance is made.

The implementation statement SHALL be submitted with the manufacturer's application to the EAC for pilot program certification testing. It SHALL provide a concise summary and narrative description of the voting system's capabilities. It SHALL include identifying information about the voting system, including the hardware and software components, version number and date.

1.3.5 Equivalent Configurations

1.3.5.1 Background

Under the standard EAC certification program, the scope of certification is very specific and extends only to the exact voting system configuration tested. The certificate specifically identifies each of the various configurations of the voting system's components that were tested and certified, including the Operating System (OS) version and service pack, as well as the Central Processing Unit (CPU). Any modification to the system not authorized by the EAC will void the certificate. The certificate is applicable to the system configuration that has been tested during certification and is not applicable when any modification to hardware, software or COTS products has occurred.

There is a tradeoff between requiring the exact configuration that was tested and certified to be deployed and allowing "equivalent configurations" that have been tested by the voting system manufacturer and attested to perform identically on these configurations. Requiring only exact configurations that have been certified to be deployed guarantees that the customer is using the identical system that has been tested by the VSTL, but does not allow the flexibility needed to accommodate routine and expected changes to Commercial Off the Shelf (COTS) systems. The requirements in this document are designed to allow for such flexibility.

1.3.5.2 Procedures for changes to baseline configuration

Testing for UOCAVA Pilot Certification is conducted by the VSTL and voting system manufacturer on the baseline configuration consisting of:

1. Specific hardware;
2. Major Version of operating system and third-party COTS applications.
    - Major Versions are changed when an updated version is downloaded; major versions are not considered changed when a patch is applied to fix an individual item.
    - In Microsoft Operating Systems, Major Versions would include Service Packs– New Service Packs would be considered a different Major Version.
    - Downloading patches (i.e., security) would not be considered a change to the Major Version. However, manufacturers SHALL create a log of all patches downloaded and supply them to the EAC upon request.

Any change to hardware or software (Major Versions) SHALL be regression tested by the voting system manufacturer to ensure that all requirements affected by the change have been adhered to. Regression testing SHALL be documented and legally affirmed to by the manufacturer, and accepted by the EAC. Regression testing SHALL be done by the manufacturer when the EAC certified version differs from the one being deployed in any of the following ways:

a. Any hardware is changed. However, de minimis changes, as defined in the EAC Pilot System Certification Manual, SHALL NOT undergo regression testing;

b. Any change to Major Version of the OS is made; and

c. Any major change to a third-party COTS application is made.

All regression testing by manufacturers SHALL include accuracy and reliability testing. Other tests SHALL be repeated for requirements closely related to the functionality that was modified with the hardware or software (Major Version) changes.

Any change to the voting system application not covered by 3 a, b or c SHALL undergo testing by the VSTL.

Test Reports describing the manufacturer regression testing SHALL be submitted to the EAC. The EAC may conduct random audits to ensure that the manufacturer regression testing performed was sufficient.

1.3.6 Requirements Language and Structure

1.3.6.1 Language

Understanding how language is used is a pre-requisite to understanding this document. Language in this document is divided into two categories: normative, i.e., the requirements language itself, and informative. Normative language is prescriptive and must be followed to obtain conformance to this document and ultimately EAC certification. Informative parts of this document include discussion, examples, extended explanations, and other matter that are necessary for proper understanding of the requirements and how to ensure conformance. Informative text is not prescriptive and serves to clarify requirements.

Normative language is specifically for requirements. The following keywords are used within requirements text to indicate the conformance aspects of the requirement:

- SHALL indicates a mandatory requirement to do something;
- SHALL NOT indicates a mandatory requirement not to do something.

1.3.6.2 Structure of requirements

Each remote electronic voting system requirement in this document is identified according to a hierarchical scheme in which higher-level requirements (e.g., "The requirements for formatting the TDP are general in nature; specific format details are of the manufacturer's choosing.") are supported by lower-level requirements (e.g., " The TDP SHALL include a detailed table of contents for the required documents, an abstract of each document, and a listing of each of the informational sections and appendices presented."). Thus, requirements are nested. When the nesting hierarchy has reached four levels (i.e., 1.1.1.1), further nested requirements are designated with lowercase letters, then Roman numerals. Therefore, all requirements are traceable by a distinct reference.

Some requirements are directly testable and some are not. Lower-level requirements (i.e., leaf-node requirements that have no requirements directly beneath them) are directly testable. Higher-level requirements (i.e., requirements with directly testable requirements beneath them) are not directly testable. Higher-level requirements are included because: (1) they are testable indirectly insofar as their lower-level requirements are testable; and (2) they often provide the structure and rationale for the lower level requirements. Satisfying all the lower-level requirements will result in satisfying the corresponding higher-level requirement. Thus, VSTLs need to only directly test lower-level requirements, not higher-level requirements. However, if non-conformance with a higher-level requirement is determined through any other means (e.g., OEVT testing, inspection) then the voting system is deemed not to conform to that higher-level requirement.

1.4 Effective Date

The UOCAVA Pilot Program Testing Requirements SHALL become effective for pilot certification testing upon adoption by the EAC. At that time, all kiosk-based remote electronic pilot systems submitted for EAC certification SHALL be tested for conformance with these requirements.

These requirements are voluntary in that each of the states can decide whether to require the voting systems used in pilot programs for their state to have an EAC certification. States may decide to adopt these requirements in whole or in part at any time, irrespective of the effective date. In addition, states may specify additional requirements that pilot voting systems used in their jurisdictions must meet. The EAC certification program does not, in any way, pre-empt the ability of the states to have their own voting system certification process.

Section 2: Functional Requirements

2.1 Accuracy

Voting system accuracy addresses the accuracy of data for each of the individual ballot selections that could be selected by a voter, including the positions that are not selected. Accuracy is defined as the ability of the voting system to capture, record, store, consolidate and report the specific selections and absence of selections, made by the voter on each ballot without error.

For each processing function in the following list, the voting system SHALL achieve a target error rate of no more than one in 10,000,000 ballot positions, with a maximum acceptable error rate in the test process of one in 500,000 ballot positions. Types of functions include:

- Recording voter selections
- Recording voter selections into ballot image storage independently from voting data storage; and
- Consolidation of vote selection data from multiple voting sites to generate jurisdiction-wide vote totals.

2.1.1 Components and Hardware

2.1.1.1 Component accuracy

Memory hardware, such as semiconductor devices and magnetic storage media, SHALL be accurate.

Test Method: Functional

Test Entity: VSTL

2.1.1.2 Equipment design

The design of equipment in all voting systems SHALL provide for protection against mechanical, thermal, and electromagnetic stresses that impact voting system accuracy.

Test Method: Functional

Test Entity: VSTL

2.1.1.3 Voting system accuracy

To ensure vote accuracy, all voting systems SHALL:

a. Record the election contests, candidates, and issues exactly as defined by election officials;

b. Record the appropriate options for casting and recording votes;

c. Record each vote precisely as indicated by the voter and be able to produce an accurate report of all votes cast;

d. Include control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) to demonstrate that the voting system has been designed for accuracy; and

e. Provide software that monitors the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected.

Test Method: Functional

Test Entity: VSTL

2.1.2 Environmental Range

All voting systems SHALL meet the accuracy requirements over manufacturer specified operating conditions and after storage under non-operating conditions.

Test Method: Functional

Test Entity: VSTL

2.1.3 Content of Data Verified for Accuracy

2.1.3.1 Election management system accuracy

Voting systems SHALL accurately record all election management data entered by the user, including election officials or their designees.

Test Method: Functional

Test Entity: VSTL

2.1.3.2 Recording accuracy

For recording accuracy, all voting systems SHALL:

a. Record every entry made by the user except where it violates voter privacy;

b. Accurately interpret voter selection(s) and record them correctly to memory;

c. Verify the correctness of detection of the user selections and the addition of the selections correctly to memory;

d. Verify the correctness of detection of data entered directly by the user and the addition of the selections correctly to memory; and

e. Preserve the integrity of election management data stored in memory against corruption by stray electromagnetic emissions, and internally generated spurious electrical signals.

Test Method: Functional

Test Entity: VSTL

2.1.4 Telecommunications Accuracy

The telecommunications components of all voting systems SHALL achieve a target error rate of no more than one in 10,000,000 ballot positions, with a maximum acceptable error rate in the test process of one in 500,000 ballot positions.

Test Method: Functional

Test Entity: VSTL

2.1.5 Accuracy Test Content

Voting system accuracy SHALL be verified by a specific test conducted for this objective. The overall test approach is described in Appendix C.

2.1.5.1 Simulators

If a simulator is used, it SHALL be verified independently of the voting system in order to produce ballots as specified for the accuracy testing.

Test Method: Functional

Test Entity: VSTL

2.1.5.2 Ballots

Ballots used for accuracy testing SHALL include all the supported types (i.e., rotation, alternative languages) of contests and election types (primary, general).

Test Method: Functional

Test Entity: VSTL

2.1.6 Reporting Accuracy

Processing accuracy is defined as the ability of the voting system to process stored voting data. Processing includes all operations to consolidate voting data after the voting period has ended.

The voting systems SHALL produce reports that are consistent, with no discrepancy among reports of voting data.

Test Method: Functional

Test Entity: VSTL

2.2 Operating capacities

2.2.1 Maximum Capacities

The manufacturer SHALL specify at least the following maximum operating capacities for the voting system (i.e. server, vote capture device, tabulation device, and communications links):

- Throughput,
- Memory,
- Transaction processing speed, and
- Election constraints:
    - Number of jurisdictions
    - Number of ballot styles per jurisdiction
    - Number of contests per ballot style
    - Number of candidates per contest
    - Number of voted ballots

Test Method: Functional

Test Entity: VSTL

2.2.1.1 Capacity testing

The voting system SHALL achieve the maximum operating capacities stated by the manufacturer in section 2.2.1.

Test Method: Functional

Test Entity: VSTL

2.2.2 Operating Capacity notification

The voting system SHALL provide notice when any operating capacity is approaching its limit.

Test Method: Functional

Test Entity: VSTL

2.2.3 Simultaneous Transmissions

The voting system SHALL protect against the loss of votes due to simultaneous transmissions.

Test Method: Functional

Test Entity: VSTL

2.3 Pre-Voting Capabilities

2.3.1 Import and Verify Election Definition

2.3.1.1 Import the election definition

The voting system SHALL:

a. Keep all data logically separated by, and accessible only to, the appropriate state and local jurisdictions;

b. Provide the capability to import or manually enter ballot content, ballot instructions and election rules, including all required alternative language translations from each jurisdiction;

c. Provide the capability for the each jurisdiction to verify that their election definition was imported accurately and completely;

d. Support image files (e.g., jpg or gif) and/or a handwritten signature image on the ballot so that state seals, official signatures and other graphical ballot elements may be properly displayed; and

e. Support multiple ballot styles per each local jurisdiction.

Test Method: Inspection/Functional

Test Entity: VSTL

2.3.1.2 Protect the election definition

The voting system SHALL provide a method to protect the election definition from unauthorized modification.

Test Method: Functional

Test Entity: VSTL

2.3.2 Readiness Testing

2.3.2.1 Voting system test mode

The voting system SHALL provide a test mode to verify that the voting system is correctly installed, properly configured, and all functions are operating to support pre-election readiness testing for each jurisdiction.

Test Method: Functional

Test Entity: VSTL

2.3.2.2 Test data segregation

The voting system SHALL provide the capability to zero-out or otherwise segregate test data from actual voting data.

Test Method: Functional

Test Entity: VSTL

2.4 Voting Capabilities

2.4.1 Opening the Voting Period

2.4.1.1 Accessing the ballot

The voting system SHALL:

a. Present the correct ballot style to each voter;

b. Allow the voting session to be canceled; and

c. Prevent a voter from casting more than one ballot in the same election.

Test Method: Functional

Test Entity: VSTL

2.4.2 Casting a Ballot

2.4.2.1 Record voter selections

The voting system SHALL:

a. Record the selection and non-selection of individual vote choices;

b. Record the voter's selection of candidates whose names do not appear on the ballot, if permitted under state law, and record as many write-ins as the number of candidates the voter is allowed to select;

c. Prohibit the voter from accessing or viewing any information on the display screen that has not been authorized and preprogrammed into the voting system (i.e., no potential for display of external information or linking to other information sources);

d. Allow the voter to change a vote within a contest before advancing to the next contest;

e. Provide unambiguous feedback regarding the voter’s selection, such as displaying a checkmark beside the selected option or conspicuously changing its appearance;

f. Indicate to the voter when no selection, or an insufficient number of selections, has been made for a contest (e.g., undervotes);

g. Provide the voter the opportunity to correct the ballot for an undervote before the ballot is cast;

h. Allow the voter, at the voter’s choice, to submit an undervoted ballot without correction.

i. Prevent the voter from making more than the allowable number of selections for any contest (e.g., overvotes); and

j. In the event of a failure of the main power supply external to the voting system, provide the capability for any voter who is voting at the time to complete casting a ballot, allow for the successful shutdown of the voting system without loss or degradation of the voting and audit data, and allow

voters to resume voting once the voting system has reverted to back-up power.

Test Method: Functional

Test Entity: VSTL

2.4.2.2 Verify voter selections

The voting system SHALL:

a. Produce a paper record each time the confirmation screen is displayed;

b. Generate a paper record identifier. This SHALL be a random identifier that uniquely links the paper record with the cast vote record;

c. Allow the voter to either cast the ballot or return to the vote selection process to make changes after reviewing the confirmation screen and paper record; and

d. Prompt the voter to confirm his choices before casting the ballot, signifying to the voter that casting the ballot is irrevocable and directing the voter to confirm his intention to cast the ballot.

Test Method: Functional

Test Entity: VSTL

2.4.2.3 Cast ballot

The voting system SHALL:

a. Store all cast ballots in a random order; logically separated by, and only accessible to, the appropriate state/local jurisdictions;

b. Notify the voter after the vote has been stored persistently that the ballot has been cast;

c. Notify the voter that the ballot has not been cast successfully if it is not stored successfully, and provide clear instruction as to steps the voter should take to cast his ballot should this event occur; and

d. Prohibit access to voted ballots until such time as state law allows for processing of absentee ballots.

Test Method: Functional

Test Entity: VSTL

2.4.2.4 Ballot linking to voter identification

2.4.2.4.1 Absentee model

The cast ballot SHALL be linked to the voter's identity without violating the privacy of the voter.

Test Method: Functional

Test Entity: VSTL

2.4.2.4.2 Early voting model

The cast ballot SHALL NOT be linked to the voter's identity.

Test Method: Inspection

Test Entity: VSTL

2.4.3 Vote Secrecy

2.4.3.1 Link to voter

The voting system SHALL be capable of producing a cast vote record that does not contain any information that would link the record to the voter.

Test Method: Functional

Test Entity: VSTL

2.4.3.2 Voting session records

The voting system SHALL NOT store any information related to the actions performed by the voter during the voting session.

Test Method: Functional

Test Entity: VSTL

2.5 Post Voting Capabilities

2.5.1 Ballot Box Retrieval

2.5.1.1 Seal and sign the electronic ballot box

The voting system SHALL seal and sign each jurisdiction's electronic ballot box, by means of a digital signature, to protect the integrity of its contents.

Test Method: Functional

Test Entity: VSTL

2.5.1.2 Electronic ballot box retrieval

The voting system SHALL allow each jurisdiction to retrieve its electronic ballot box.

Test Method: Functional

Test Entity: VSTL

2.5.1.3 Electronic ballot box integrity check

The voting system SHALL perform an integrity check on the electronic ballot box verifying that it has not been tampered with or modified before opening.

Test Method: Functional

Test Entity: VSTL

2.5.2 Tabulation

2.5.2.1 Tabulation device connectivity

The tabulation device SHALL be physically, electrically, and electromagnetically isolated from any other computer network.

Test Method: Inspection

Test Entity: VSTL

2.5.2.2 Open ballot box

The tabulation device SHALL allow only an authorized entity to open the ballot box.

Test Method: Functional

Test Entity: VSTL

2.5.2.3 Absentee model

2.5.2.3.1 Adjudication

The tabulation device SHALL allow the designation of electronic ballots as “accepted” or “not accepted” by an authorized entity.

Test Method: Functional

Test Entity: VSTL

2.5.2.4 Ballot decryption

The tabulation device decryption process SHALL remove all layers of encryption and breaking all correlation between the voter and the ballot, producing a record that is in clear text.

Test Method: Functional

Test Entity: VSTL

2.5.2.5 Tabulation report format

The tabulation device SHALL have the capability to generate a tabulation report of voting results in an open and non-proprietary format.

Test Method: Functional

Test Entity: VSTL

2.6 Audit and Accountability

2.6.1 Scope

This section presents requirements for the voting system to provide the capability for conducting the types of system performance verifications listed below. The intention is to provide for independent verification of the agreement of the paper record and electronic tabulation results. These audits could be conducted on the entire set of records or on a sampling basis, depending on the preferences of state/local jurisdictions:

a. Hand audit – Validation of electronic tabulation results via comparison with results of a hand tally of paper records; and

b. Comparison of ballot images and the corresponding paper records.

It should be noted that these audits are for the purpose of verifying system performance and are conducted independently from the election audits that many jurisdictions conduct to verify overall election results. It is expected that ballots cast on a UOCAVA pilot voting system will be included with ballots cast by all other means when audit samples are drawn for election results verification.

2.6.2 Electronic Records

In order to support independent auditing, a voting system SHALL be able to produce electronic records that contain the necessary information in a secure and usable manner. Typically, this includes records such as:

- Vote counts;
- Counts of ballots recorded;
- Paper record identifier;
- Event logs and other records of important events; and
- Election archive information.

The following requirements apply to records produced by the voting system for any exchange of information between devices, support of auditing procedures, or reporting of final results:

a. Requirements for electronic records to be produced by tabulation devices; and

b. Requirements for printed reports to support auditing steps.

2.6.2.1 All records capable of being exported

The voting system SHALL provide the capability to export its electronic records in an open format, such as XML, or include a utility to export log data into a publicly documented format.

Test Method: Functional

Test Entity: ***VSTL***

2.6.2.2 Ballot images

The voting system SHALL have the capability to generate ballot images in a human readable format.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.6.2.3 Ballot image content

The voting system SHALL be capable of producing a ballot image that includes:

a. Election title and date of election;

b. Jurisdiction identifier;

c. Ballot style;

d. Paper record identifier; and

e. For each contest and ballot question:

   i. The choice recorded, including write-ins; and

   ii. Information about each write-in.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.6.2.4 All records capable of being printed

The tabulation device SHALL provide the ability to produce printed forms of its electronic records. The printed forms SHALL retain all required information as specified for each record type other than digital signatures.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.6.2.5 Summary count record

The voting system SHALL produce a summary count record including the following:

a. Time and date of summary record; and

b. The following, both in total and broken down by ballot style and voting location:

   i. Number of received ballots

   ii. Number of counted ballots

   iii. Number of rejected electronic CVRs

   iv. Number of write-in votes

   v. Number of undervotes.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.6.3 Paper Records

The vote capture device is required to produce a paper record for each ballot cast. This record SHALL be available to the voter to review and verify, and SHALL be retained for later auditing or recounts, as specified by state law. Paper records provide an independent record of the voter's choices that can be used to verify the correctness of the electronic record created by the vote capture device.

2.6.3.1 Paper record creation

Each vote capture device SHALL print a human readable paper record.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.6.3.2 Paper record contents

Each paper record SHALL contain at least:

a. Election title and date of election;

b. Voting location;

c. Jurisdiction identifier;

d. Ballot style;

e. Paper record identifier; and

f. For each contest and ballot question:

   i. The recorded choice, including write-ins; and

   ii. Information about each write-in.

Test Method: ***Inspection***

Test Entity: ***VSTL***

2.6.3.3 Privacy

The vote capture device SHALL be capable of producing a paper record that does not contain any information that could link the record to the voter.

Test Method: ***Inspection***

Test Entity: ***VSTL***

2.6.3.4 Multiple pages

When a single paper record spans multiple pages, each page SHALL include the voting location, ballot style, date of election, and page number and total number of the pages (e.g., page 1 of 4).

Test Method: Functional

Test Entity: VSTL

2.6.3.5 Machine-readable part contains same information as human-readable part

If a non-human-readable encoding is used on the paper record, it SHALL contain the entirety of the human-readable information on the record.

Test Method: Inspection

Test Entity: VSTL

2.6.3.6 Format for paper record non-human-readable data

Any non-human-readable information on the paper record SHALL be presented in a non-proprietary format.

Test Method: Inspection

Test Entity: VSTL

2.6.3.7 Linking the electronic CVR to the paper record

The paper record SHALL:

a. Contain the paper record identifier; and

b. Identify whether the paper record represents the ballot that was cast.

Test Method: Inspection

Test Entity: VSTL

2.7 Performance Monitoring

2.7.1 Voting System and Network Status

2.7.1.1 Network monitoring

The system server SHALL provide for system and network monitoring during the voting period.

Test Method: Functional

Test Entity: VSTL

2.7.1.2 Tool access

The system and network monitoring functionality SHALL only be accessible to authorized personnel from restricted consoles.

Test Method: Functional

Test Entity: VSTL

2.7.1.3 Tool privacy

System and network monitoring functionality SHALL NOT have the capability to compromise voter privacy or election integrity.

Test Method: Functional

Test Entity: VSTL

Section 3: Usability, Accessibility, and Privacy Requirements

3.1 Overview

The importance of usability and accessibility in the design of voting systems has become increasingly apparent. It is not sufficient that the internal operation of these systems be correct; in addition, voters and kiosk workers must be able to use them effectively. There are some particular considerations for the design of usable and accessible voting systems:

- The voting task itself can be fairly complex; the voter may have to navigate an electronic ballot, choose multiple candidates in a single contest, or decide on abstrusely worded referenda
- Pilot projects by definition are implementing new kinds of voting systems, so there is limited opportunity for voters and kiosk workers to gain familiarity with the process
- Usability and accessibility requirements include a broad range of factors, including physical abilities, language skills, and technology experience

3.1.1 Purpose

The challenge, then, is to provide a voting system that voters can use comfortably, efficiently, and with confidence that they have cast their votes correctly. The requirements within this section are intended to serve that goal. Three broad principles motivate this section:

1. All eligible UOCAVA voters SHALL have access to the voting process without discrimination.

The voting process SHALL be accessible to individuals with disabilities. The voting process includes access to the kiosk site, instructions on how to vote, initiating the voting session, making ballot selections, review of the ballot and the paper record, final submission of the ballot, depositing the paper record in a secure receptacle, and getting help when needed.

2. Each cast ballot SHALL accurately capture the selections made by the voter.

The ballot SHALL be presented to the voter in a manner that is clear and usable. Voters should encounter no difficulty or confusion regarding the process for recording their selections.

3. The voting process SHALL preserve the secrecy of the ballot.

The voting process SHALL preclude anyone else from determining the content of a voter's ballot, without the voter's cooperation. If such a determination is made against the wishes of the voter, then his or her privacy has been violated.

All the requirements in this section have the purpose of improving the quality of interaction between voters and voting systems.

Note that these principles refer to the entire voting process. The UOCAVA Pilot Program Testing Requirements apply only to voting systems; other aspects of the

process (such as administrative rules and procedures) are outside the scope of EAC certification, but are nonetheless crucial for the full achievement of the principles.

3.1.2 Special terminology

The following terms are used frequently in this chapter; they are defined in the Glossary in Appendix A:

- Alert time
- Audio-Tactile Interface (ATI)
- Common Industry Format (CIF)
- Completed system response time
- Initial system response time
- Voter inactivity time

3.2 General Usability

The voting system SHALL support voters in the task of effectively and accurately casting their ballots. The features of the voting system SHALL not contribute to the commission of voter error within the voting session.

3.2.1 Privacy

The voting process must preclude anyone else from determining the content of a voter's ballot without the voter's cooperation. Privacy ensures that the voter can cast votes based solely on his or her own preferences without intimidation or inhibition.

3.2.1.1 Privacy at the kiosk locations

a. The vote capture device SHALL prevent others from determining the contents of a ballot.

b. The vote capture device SHALL support ballot privacy during the voting session and ballot submission.

c. During the voting session, if an audio interface to the vote capture device is provided, it SHALL be audible only to the voter.

d. The vote capture device SHALL issue all warnings in a way that preserves the privacy of the voter and the confidentiality of the ballot.

e. The vote capture device SHALL not issue a receipt to the voter that would provide proof to another of how the voter voted.

3.2.1.2 No recording of alternative format usage

When voters use non-typical ballot interfaces, such as large print or alternative languages, their anonymity may be vulnerable. To the extent possible, only the logical contents of their ballots should be recorded, not the special formats in which they were rendered.

a. No information SHALL be kept within an electronic cast voter record that identifies any alternative language feature(s) used by a voter.

b. No information SHALL be kept within an electronic cast voter record that identifies any accessibility feature(s) used by a voter.

3.2.2 Cognitive issues

The features specified in this section are intended to minimize cognitive difficulties for voters. They should always be able to operate the vote capture device and understand the effect of their actions.

a. The vote capture device SHALL provide instructions for all its valid operations.

b. The vote capture device SHALL provide a means for the voter to get help directly from the system at any time during the voting session.

c. Instructional material for the voter SHALL conform to norms and best practices for plain language.

   i. Warnings and alerts issued by the vote capture device SHALL be distinguishable from other information and should clearly state:

      - The nature of the problem;
      - Whether the voter has performed or attempted an invalid operation or whether the vote capture device itself has malfunctioned in some way; and
      - The set of responses available to the voter.

   ii. When an instruction is based on a condition, the condition should be stated first, and then the action to be performed.

   iii. The vote capture device should use familiar, common words and avoid technical or specialized words that voters are not likely to understand.

   iv. Each distinct instruction should be separated spatially from other instructions for visual or tactile interfaces, and temporally for auditory interfaces.

   v. The vote capture device should issue instructions on the correct way to perform actions, rather than telling voters what not to do.

   vi. The instructions should address the voter directly rather than use passive voice constructions.

   vii. The vote capture device should avoid the use of gender-based pronouns.

d. Consistent with election law, the voting application SHALL support a process that does not introduce bias for or against any of the contest choices to be presented to the voter. In both visual and aural formats, the choices SHALL be presented in an equivalent manner.

e. The voting system SHALL provide the capability to design a ballot with a high level of clarity and comprehensibility.

   i. The vote capture device should not visually present a single contest spread over two pages or two columns.

   ii. The ballot SHALL clearly indicate the maximum number of candidates for which one can vote within a single contest.

iii. The relationship between the name of a candidate and the mechanism used to vote for that candidate SHALL be consistent throughout the ballot.

iv. The vote capture device should present instructions near to where they are needed.

f. The use of color SHALL agree with common conventions: (a) green, blue or white is used for general information or as a normal status indicator; (b) amber or yellow is used to indicate warnings or a marginal status; (c) red is used to indicate error conditions or a problem requiring immediate attention.

g. When an icon is used to convey information, indicate an action, or prompt a response, it SHALL be accompanied by a corresponding linguistic label.

3.2.3 Perceptual issues

The requirements of this section are designed to minimize perceptual difficulties for the voter. Some of these requirements are designed to assist voters with poor reading vision. These are voters who might have some difficulty in reading normal text, but are not typically classified as having a visual disability.

a. The electronic display screen of the vote capture device SHALL have the following characteristics:

- Flicker frequency NOT between 2 Hz and 55 Hz.
- Minimum display brightness: 130 cd/m2
- Minimum display darkroom 7×7 checkerboard contrast: 150:1
- Minimum display pixel pitch: 85 pixels/inch (0.3 mm/pixel)
- Minimum display area 700 cm2
- Antiglare screen surface that shows no distinct virtual image of a light source
- Minimum uniform diffuse ambient contrast for 500 1× illuminance: 10:1

b. Any aspect of the vote capture device that is adjustable by either the voter or kiosk worker, including font size, color, contrast, audio volume, or rate of speech, SHALL automatically reset to a standard default value upon completion of that voter's session.

c. If any aspect of a vote capture device is adjustable by either the voter or kiosk worker, there SHALL be a mechanism to allow the voter to reset all such aspects to their default values while preserving the current votes.

d. For all text the vote capture device SHALL provide a font with the following characteristics

- Height of capital letters at least: 3.0 mm
- x-height of a least: 70% of cap height
- Stroke width at least: 0.35 mm.

e. The vote capture device electronic image display SHALL be capable of showing all information in at least two font sizes:

- 3.0-4.0 mm cap height, with a corresponding x-height at least 70% of the cap height and a minimum stroke width of 0.35 mm;
- 6.3-9.0 mm cap height, with a corresponding x-height at least 70% of the cap height and a minimum stroke width of 0.7 mm; under control of the voter. The device SHALL allow the voter to adjust font size throughout the voting session while preserving the current votes.

f. Text should be presented in a sans serif font.

g. Vote capture devices providing paper verification records SHALL provide features that assist in the reading of such records by voters with poor reading vision.

   i. The vote capture device may achieve legibility of paper records by supporting the printing of those records in at least two font sizes, 3.0-4.0mm and 6.3-9.0mm.

   ii. The vote capture device may achieve legibility of paper records by supporting magnification of those records. This magnification may be done by optical or electronic devices. The manufacturer may either: 1) provide the magnifier itself as part of the system, or 2) provide the make and model number of readily available magnifiers that are compatible with the system.

h. The minimum figure-to-ground ambient contrast ratio for all text and informational graphics (including icons) SHALL be 10:1. For paper records, contrast is measured based on ambient lighting of at least 300 l×.

i. The electronic display screen of the vote capture device SHALL be capable of showing all information in high contrast either by default or under the control of the voter. If the device allows the voter to adjust contrast during the voting session it SHALL preserve the current votes. High contrast is a figure-to-ground ambient contrast ratio for text and informational graphics of at least 50:1.

j. The default color coding SHALL support correct perception by voters with color blindness.

   i. Ordinary information presented to the voter should be in the form of black text on a white background. The use of color should be reserved for special cases, such as warnings or alerts.

   ii. No information presented to the voter SHALL be in the form of colored text on a colored background. Either the text or background SHALL be black or white.

   iii. If text is colored other than black or white:

      1. The background SHALL be black or white.
      2. The text SHALL be presented in a bold font (minimum 0.6 mm stroke width).
      3. If the background is black, the text color SHALL be yellow or light cyan.
      4. If the background is white, the text color SHALL be dark enough to maintain a 10:1 contrast ratio.

   iv. If the background is colored other than black or white, the presentation SHALL follow these guidelines:

      1. The text color SHALL be black.

2. The background color SHALL be yellow or light cyan.

k. Color coding SHALL not be used as the sole means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.

3.2.4 Interaction issues

The requirements of this section are designed to minimize interaction difficulties for the voter.

a. The vote capture device SHALL not require page scrolling by the voter.

b. The vote capture device SHALL provide unambiguous feedback regarding the voter's selection, such as displaying a checkmark beside the selected option or conspicuously changing its appearance.

c. Vote capture device input mechanisms SHALL be designed to prevent accidental activation.

i. On touch screens, the sensitive touch areas SHALL have a minimum height of 0.5 inches and minimum width of 0.7 inches. The vertical distance between the centers of adjacent areas SHALL be at least 0.6 inches, and the horizontal distance at least 0.8 inches. Touch areas SHALL not overlap.

3.2.4.1 Timing issues

These requirements address how long the system and voter wait for each other to interact.

a. The initial system response time of the vote capture device SHALL be no greater than 0.5 seconds.

b. When the voter performs an action to record a single vote, the completed system response time of the vote capture device SHALL be no greater than one second in the case of a visual response, and no greater than five seconds in the case of an audio response.

c. The completed system response time of the vote capture device SHALL be no greater than 10 seconds.

d. If the vote capture device has not completed its visual response within one second, it SHALL present to the voter, within 0.5 seconds of the voter's action, some indication that it is preparing its response.

e. If the vote capture device requires a response by a voter within a specific period of time, it SHALL issue an alert at least 20 seconds before this time period has expired and provide a means by which the voter may receive additional time

3.2.5 Alternative languages

HAVA Section 301 (a)(4) states that the voting system SHALL provide alternative language accessibility pursuant to the requirements of Section 203 of the Voting Rights Act of 1965 (42 U.S.C. 1973aa-1a). Ideally every voter would be able to vote independently and privately, regardless of language. As a practical matter, alternative language access is mandated under the Voting Rights Act of 1975, subject to certain thresholds (e.g., if the language group exceeds 5% of the voting

age population). Thus, election officials must ensure that the pilot voting system is capable of handling the languages meeting the legal threshold within their districts.

a. The voting system SHALL be capable of presenting the ballot, contest choices, review screens, paper verification records, and voting instructions in any language declared by the manufacturer to be supported by the system.

3.2.6 Usability for kiosk workers

Voting systems are used not only by voters to record their votes, but also by kiosk workers who are responsible for kiosk site set-up, light maintenance, and kiosk site closing. Because of the variety of possible implementations, it is impossible to specify detailed design requirements for these functions. The requirements below describe general capabilities that all pilot systems must support.

a. Messages generated by the vote capture device for kiosk workers in support of the set up, maintenance, or safety of the system SHALL adhere to the requirements for clarity in Section 3.2.4 “Cognitive issues”.

3.2.6.1 Operation

Kiosk workers are responsible for opening the kiosk locations each day of the voting period, keeping them running smoothly during voting hours, closing the kiosk locations at the end of each day of the voting period, and shutting down the kiosks at the end of the voting period.

Operations may be categorized in three phases: initial system set up, daily set up and operation, and shutting down the system at the end of the voting period.

Initial setup includes all the steps necessary to remove the system from its shipping crate, physically set up and configure the vote capture devices and peripherals, verify the integrity of the software, load and check out the software, initiate and check out the communications links. .

Daily operation of the kiosk location includes such functions as:

- voter identification and authorization;
- provision of smartcard to voter to initiate the voting session ;
- assistance to voters who need help;
- system recovery in the case of voters who abandon the voting session without having cast a ballot; and
- routine supplies replenishment, such as adding paper to the printer.

Daily shutdown includes all the steps necessary to take the vote capture device from the state in which it is ready to record votes to its overnight storage state.

a. The procedures for voting system setup, polling, and shutdown, as documented by the manufacturer, SHALL be reasonably easy for the typical poll worker to learn, understand, and perform.

b. The manufacturer SHALL provide clear, complete, and detailed instructions and messages for kiosk location setup, daily operation, and shutdown.

    i. The documentation SHALL be presented at a level appropriate for kiosk workers who are not experts in voting system and computer technology.

    ii. The documentation SHALL be in a format suitable for use in the kiosk location.

iii. The instructions and messages SHALL enable the kiosk worker to verify that the vote capture device, peripherals, and communications links

- Has been set up correctly;
- Is in correct working order to record votes; and
- Has been shut down correctly.

3.2.6.2 Safety

All voting systems and their components must be designed so as to eliminate hazards to personnel or to the equipment itself. Hazards include, but are not limited to:

- Fire hazards;
- Electrical hazards;
- Potential for equipment tip-over (stability);
- Potential for cuts and scrapes (e.g., sharp edges);
- Potential for pinching (e.g., tight, spring-loaded closures); and
- Potential for hair or clothing entanglement.

Devices associated with the voting system SHALL be certified in accordance with the requirements of UL 60950-1, Information Technology Equipment – Safety – Part 1 by a certification organization accredited by the Department of Labor, Occupational Safety and Health Administration's Nationally Recognized Testing Laboratory program. The certification organization's scope of accreditation SHALL include IEC/UL 60950-1.

IEC/UL 60950 is a comprehensive standard for IT equipment and addresses all the hazards discussed above under Safety.

3.3 Accessibility requirements

The voting process is to be accessible to voters with disabilities through the use of a specially equipped voting station. A machine so equipped is referred to herein as an accessible voting station (Acc-VS).

The requirements in this section are intended to address this HAVA mandate. Ideally, every voter would be able to vote independently and privately. As a practical matter, there may be some number of voters who, because of the nature of their disabilities, will need personal assistance with any system. Nonetheless, these requirements are meant to make the voting system independently accessible to as many voters as possible. This includes access across all voting processes: capabilities to generate, verify and cast an official ballot must be provided.

This section is organized according to the type of disability being addressed. For each type, certain appropriate design features are specified. Note, however, that a feature intended primarily to address one kind of disability may very well assist voters with other kinds. Moreover, this organization in no way implies that the various sets of requirements are optional or mutually exclusive. In order to conform, an Accessible Voting Station must fulfill all the requirements of all the sub-sections of Chapter 3.3.

There are many other requirements, such as the general usability requirements, that apply to the Acc-VS besides those in this section. Please see Section 3.1.3 “Interaction of usability and accessibility requirements” for a full explanation.

3.3.1 General

The requirements of this section are relevant to a wide variety of disabilities.

a. The Acc-VS SHALL be integrated into the manufacturer’s complete voting system so as to support accessibility for disabled voters throughout the voting session.
    i. The manufacturer SHALL supply documentation describing 1) recommended procedures that fully implement accessibility for voters with disabilities and 2) how the Acc-VS supports those procedures.

b. When the provision of accessibility for Acc-VS involves an alternative format for ballot presentation, then all information presented to non-disabled voters, including instructions, warnings, error and other messages, and contest choices, SHALL be presented in that alternative format.

c. The support provided to voters with disabilities SHALL be intrinsic to the accessible voting station. It SHALL not be necessary for the accessible voting station to be connected to any personal assistive device of the voter in order for the voter to operate it correctly.

d. If a voting system provides for voter identification or authentication by using biometric measures that require a voter to possess particular biological characteristics, then Acc-VS SHALL provide a secondary means that does not depend on those characteristics.

e. If the Acc-VS generates a paper record (or some other durable, human-readable record) for the purpose of allowing voters to verify their votes, then the system SHALL provide a means to ensure that the verification record is accessible to all voters with disabilities, as identified in 3.3 “Accessibility requirements”.
    i. If the Acc-VS generates a paper record (or some other durable, human-readable record) for the purpose of allowing voters to verify their votes, then the system SHALL provide a mechanism that can read that record and generate an audio representation of its contents.

3.3.2 Low vision

These requirements specify the features of the accessible voting station designed to assist voters with low vision.

In general, low vision is defined as having a visual acuity worse than 20/70. Low (or partial) vision also includes dimness of vision, haziness, film over the eye, foggy vision, extreme near-sightedness or far-sightedness, distortion of vision, color distortion or blindness, visual field defects, spots before the eyes, tunnel vision, lack of peripheral vision, abnormal sensitivity to light or glare and night blindness.

People with tunnel vision can see only a small part of the ballot at one time. For these users it is helpful to have letters at the lower end of the font size range in order

to allow them to see more letters at the same time. Thus, there is a need to provide font sizes at both ends of the range.

People with low vision or color blindness benefit from high contrast and from a selection of color combinations appropriate for their needs. Between 7% and 10% of all men have color vision deficiencies. Certain color combinations in particular cause problems. Therefore, use of color combinations with good contrast is required. Note also the general Requirement 3.2.5 j.

However, some users are very sensitive to very bright displays and cannot use them for long. An overly bright background causes a visual white-out that makes these users unable to distinguish individual letters. Thus, use of non-saturated color options is an advantage for some people.

It is important to note that some of the requirements in 3.2.5 “Perceptual issues” also provide support for voters with certain kinds of vision problems.

a. An accessible voting station with a color electronic image display SHALL allow the voter to adjust the color saturation throughout the voting session while preserving the current votes. Two options SHALL be available: 1) black text on white background and 2) white text on black background.

b. Buttons and controls on accessible voting stations SHALL be distinguishable by both shape and color. This applies to buttons and controls implemented either "on-screen" or in hardware. This requirement does not apply to sizeable groups of keys, such as a conventional 4x3 telephone keypad or a full alphabetic keyboard.

c. The Acc-VS SHALL provide synchronized audio output to convey the same information as that which is displayed on the screen. There SHALL be a means by which the voter can disable either the audio or the video output, resulting in a video-only or audio-only presentation, respectively. The system SHALL allow the voter to switch among the three modes (synchronized audio/video, video-only, or audio-only) throughout the voting session while preserving the current votes.

3.3.3 Blindness

These requirements specify the features of the accessible voting station designed to assist voters who are blind.

a. The accessible voting station SHALL provide an audio-tactile interface (ATI) that supports the full functionality of the visual ballot interface.

    i. The ATI of VEBD-A of the accessible voting station SHALL provide the same capabilities to vote and cast a ballot as are provided by its visual interface.

    ii. The ATI SHALL allow the voter to have any information provided by the voting system repeated.

    iii. The ATI SHALL allow the voter to pause and resume the audio presentation.

    iv. The ATI SHALL allow the voter to skip to the next contest or return to previous contests.

    v. The ATI SHALL allow the voter to skip over the reading of a referendum so as to be able to vote on it immediately.

b. Voting stations that provide audio presentation of the ballot SHALL do so in a usable way, as detailed in the following sub-requirements.

i. The ATI SHALL provide its audio signal through an industry standard connector for private listening using a 3.5mm stereo headphone jack to allow voters to use their own audio assistive devices.

ii. When VEBD-A utilizes a telephone style handset or headphone to provide audio information, it SHALL provide a wireless T-Coil coupling for assistive hearing devices so as to provide access to that information for voters with partial hearing. That coupling SHALL achieve at least a category T4 rating as defined by [ANSI01] American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19.

iii. A sanitized headphone or handset SHALL be made available to each voter.

iv. VEBD-A SHALL set the initial volume for each voting session between 40 and 50 dB SPL.

v. The audio system SHALL allow the voter to control the volume throughout the voting session while preserving the current votes. The volume SHALL be adjustable from a minimum of 20dB SPL up to a maximum of 100 dB SPL, in increments no greater than 10 dB.

vi. The audio system SHALL be able to reproduce frequencies over the audible speech range of 315 Hz to 10 KHz.

vii. The audio presentation for VEBD-A of verbal information should be readily comprehensible by voters who have normal hearing and are proficient in the language. This includes such characteristics as proper enunciation, normal intonation, appropriate rate of speech, and low background noise. Candidate names should be pronounced as the candidate intends.

viii. The audio system SHALL allow the voter to control the rate of speech throughout the voting session while preserving the current votes. The range of speeds supported SHALL include 75% to 200% of the nominal rate. Adjusting the rate of speech SHALL not affect the pitch of the voice.

c. If Acc-VS supports ballot activation for non-blind voters, then it SHALL also provide features that enable voters who are blind to perform this activation.

d. If Acc-VS supports ballot submission or vote verification for non-blind voters, then it SHALL also provide features that enable voters who are blind to perform these actions.

e. Mechanically operated controls or keys, or any other hardware interface on Acc-VS available to the voter SHALL be tactilely discernible without activating those controls or keys.

f. The status of all locking or toggle controls or keys (such as the "shift" key) for Acc-VS SHALL be visually discernible, and also discernible through either touch or sound.

3.3.4 Dexterity

These requirements specify the features of the accessible voting station designed to assist voters who lack fine motor control or use of their hands.

a. The accessible voting station SHALL provide a mechanism to enable non-manual input that is functionally equivalent to tactile input. All the functionality of the accessible voting station (e.g., straight party voting, write-in candidates) that is available through the conventional forms of input, such as tactile, SHALL also be available through the non-manual input mechanism.

b. If Acc-VS supports ballot submission or vote verification for non-disabled voters, then it SHALL also provide features that enable voters who lack fine motor control or the use of their hands to perform these actions.

c. Keys, controls, and other manual operations on the accessible voting station SHALL be operable with one hand and SHALL not require tight grasping, pinching, or twisting of the wrist. The force required to activate controls and keys SHALL be no greater 5 lbs. (22.2 N).

d. The accessible voting station controls SHALL not require direct bodily contact or for the body to be part of any electrical circuit.

3.3.5 Mobility

These requirements specify the features of the accessible voting station designed to assist voters who use mobility aids, including wheelchairs. Many of the requirements of this section are based on the ADA Accessibility Guidelines for Buildings and Facilities (ADAAG).

a. The accessible voting station SHALL provide a clear floor space of 30 inches minimum by 48 inches minimum for a stationary mobility aid. The clear floor space SHALL be designed for a forward approach or a parallel approach.

b. When deployed according to the installation instructions provided by the manufacturer, Acc-VS SHALL allow adequate room for an assistant to the voter. This includes clearance for entry to and exit from the area of the voting station.

c. Labels, displays, controls, keys, audio jacks, and any other part of the accessible voting station necessary for the voter to operate the voting system SHALL be legible and visible to a voter in a wheelchair with normal eyesight (no worse than 20/40, corrected) who is in an appropriate position and orientation with respect to the accessible voting station.

3.3.5.1 Controls within reach

The requirements of this section ensure that the controls, keys, audio jacks and any other part of the accessible voting station necessary for its operation are within easy reach. Note that these requirements have meaningful application mainly to controls in a fixed location. A hand-held tethered control panel is another acceptable way of providing reachable controls.

a. If the accessible voting station has a forward approach with no forward reach obstruction then the high reach SHALL be 48 inches maximum and the low reach SHALL be 15 inches minimum. See Part 1: Figure 3-1.

b. If the accessible voting station has a forward approach with a forward reach obstruction, the following sub-requirements SHALL apply. (See Part 1: Figure 3-2).

    i. The forward obstruction for Acc-VS SHALL be no greater than 25 inches in depth, its top no higher than 34 inches and its bottom surface no lower than 27 inches.

ii. If the obstruction for Acc-VS is no more than 20 inches in depth, then the maximum high reach SHALL be 48 inches, otherwise it SHALL be 44 inches.

iii. Space under the obstruction between the finish floor or ground and 9 inches above the finish floor or ground SHALL be considered toe clearance and SHALL comply with the following provisions for Acc-VS:

1. Toe clearance depth SHALL extend 25 inches maximum under the obstruction;
2. The minimum toe clearance depth under the obstruction SHALL be either 17 inches or the depth required to reach over the obstruction to operate the accessible voting station, whichever is greater; and
3. Toe clearance width SHALL be 30 inches minimum.

iv. Space under the obstruction between 9 inches and 27 inches above the finish floor or ground SHALL be considered knee clearance and SHALL comply with the following provisions:

1. Knee clearance depth SHALL extend 25 inches maximum under the obstruction at 9 inches above the finish floor or ground;
2. The minimum knee clearance depth at 9 inches above the finish floor or ground SHALL be either 11 inches or 6 inches less than the toe clearance, whichever is greater;
3. Between 9 inches and 27 inches above the finish floor or ground, the knee clearance depth SHALL be permitted to reduce at a rate of 1 inch in depth for each 6 inches in height. (It follows that the minimum knee clearance at 27 inches above the finish floor or ground SHALL be 3 inches less than the minimum knee clearance at 9 inches above the floor.); and
4. Knee clearance width SHALL be 30 inches minimum.

c. If the accessible voting station has a parallel approach with no side reach obstruction then the maximum high reach SHALL be 48 inches and the minimum low reach SHALL be 15 inches. See Part 1: Figure 3-3.

d. If the accessible voting station has a parallel approach with a side reach obstruction, the following sub-requirements SHALL apply. See Figure 3-1.

i. The side obstruction for Acc-VS SHALL be no greater than 24 inches in depth and its top no higher than 34 inches.

ii. If the obstruction is no more than 10 inches in depth, then the maximum high reach SHALL be 48 inches, otherwise it SHALL be 46 inches.

Figure 3-1 Unobstructed reach measurements

Dimensions shown in inches above the line, SI units (in millimeters) below the line

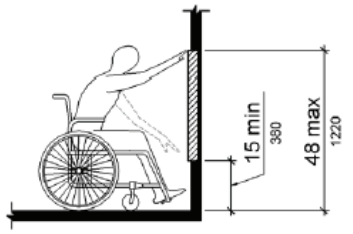


Figure 1: Unobstructed forward reach

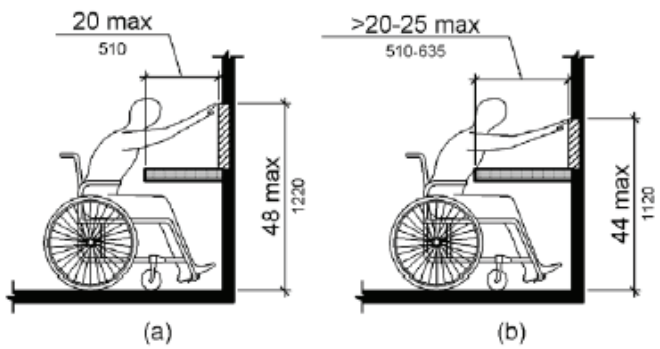


Figure 2: Obstructed forward reach

(a) for an obstruction depth of up to 20 inches
(b) for an obstruction depth of up to 25 inches

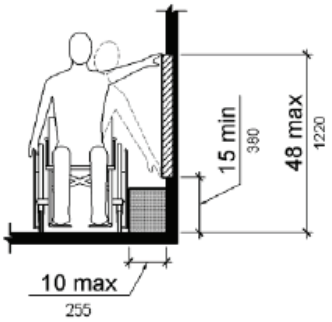


Figure 3: Unobstructed side reach with an allowable obstruction less than 10 inches deep

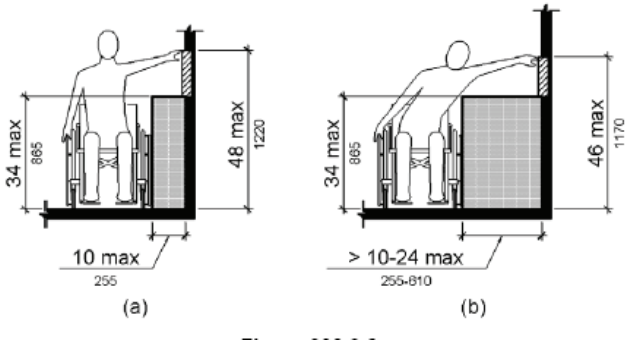


Figure 4: Obstructed side reach

(a) for an obstruction depth of up to 10 inches
(b) for an obstruction depth of up to 24 inches

3.3.6 Hearing

These requirements specify the features of the accessible voting station designed to assist voters with hearing disabilities.

a. The accessible voting station SHALL incorporate the features listed under Requirement 3.3.3-C for voting systems that provide audio presentation of the ballot.

b. If the accessible voting system provides sound cues as a method to alert the voter, the tone SHALL be accompanied by a visual cue, unless the station is in audio-only mode.

c. No voting device SHALL cause electromagnetic interference with assistive hearing devices that would substantially degrade the performance of those devices. The voting device, measured as if it were a wireless device, SHALL achieve at least a category T4 rating as defined by [ANSI01] American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19.

3.3.7 Cognition

These requirements specify the features of the accessible voting station designed to assist voters with cognitive disabilities.

a. The accessible voting station should provide support to voters with cognitive disabilities.

3.3.8 English proficiency

These requirements specify the features of the accessible voting station designed to assist voters who lack proficiency in reading English.

a. For voters who lack proficiency in reading English, Acc-VS SHALL provide an audio interface for instructions and ballots as described in 3.3.3 b.

Section 4: Software

4.1 Selection of Programming Languages

4.1.1 Acceptable Programming Language Constructs

Application logic SHALL be produced in a high-level programming language that has all of the following control constructs:

a. Sequence;

b. Loop with exit condition (e.g., for, while, and/or do-loops);

c. If/Then/Else conditional;

d. Case conditional; and

e. Block-structured exception handling (e.g., try/throw/catch).

Test Method: Inspection

Test Entity: Manufacturer

4.2 Selection of General Coding Conventions

4.2.1 Acceptable Coding Conventions

Application logic SHALL adhere to (or be based on) a published, credible set of coding rules, conventions or standards (herein simply called "coding conventions") that enhance the workmanship, security, integrity, testability, and maintainability of applications.

Test Method: Inspection

Test Entity: Manufacturer

4.2.1.1 Published

Coding conventions SHALL be considered published if they appear in publicly available media.

Test Method: Inspection

Test Entity: Manufacturer

4.2.1.2 Credible

Coding conventions SHALL be considered credible if at least two different organizations independently decided to adopt them and made active use of them at some time within the three years before conformity assessment was first sought.

Test Method: Inspection

Test Entity: ***Manufacturer***

4.3 Software Modularity and Programming

4.3.1.1 Modularity

Application logic SHALL be designed in a modular fashion.

4.3.1.2 Module testability

Each module SHALL have a specific function that can be tested and verified independently from the remainder of the code.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.3.1.3 Module size and identification

Modules SHALL be small and easily identifiable.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.4 Structured Programming

4.4.1 Exception Handling

4.4.1.1 Exception handling

Application logic SHALL handle exceptions using block-structured exception handling constructs.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.4.1.2 Legacy library units must be wrapped

If application logic makes use of any COTS or third-party logic callable units that do not throw exceptions when exceptional conditions occur, those callable units SHALL be wrapped in callable units that check for the relevant error conditions and translate them into exceptions, and the remainder of application logic SHALL use only the wrapped version.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.4.2 Unstructured Control Flow is Prohibited

Application logic SHALL contain no unstructured control constructs.

Test Method: Inspection

Test Entity: Manufacturer

4.4.2.1 Branching

Arbitrary branches (a.k.a. GoTos) SHALL NOT be allowed.

Test Method: Inspection

Test Entity: Manufacturer

4.4.2.2 Intentional exceptions

Exceptions SHALL only be used for abnormal conditions. Exceptions SHALL NOT be used to redirect the flow of control in normal ("non-exceptional") conditions.

Test Method: Inspection

Test Entity: Manufacturer

4.4.2.3 Unstructured exception handling

Unstructured exception handling (e.g., On Error GoTo, setjmp/longjmp) SHALL NOT be allowed.

Test Method: Inspection

Test Entity: Manufacturer

4.4.2.4 Separation of code and data

Application logic SHALL NOT compile or interpret configuration data or other input data as a programming language.

Test Method: Inspection

Test Entity: Manufacturer

4.5 Comments

4.5.1 Header Comments

Application logic modules SHALL include header comments that provide at least the following information for each callable unit (e.g., function, method, operation, subroutine, procedure.):

a. The purpose of the unit and how it works (if not obvious);

b. A description of input parameters, outputs and return values, exceptions thrown, and side-effects; and

c. Any protocols that must be observed (e.g., unit calling sequences).

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.6 Executable Code and Data Integrity

4.6.1 Code Coherency

Application logic SHALL conform to the following sub-requirements:

a. Self-modifying code SHALL NOT be allowed;

b. Application logic SHALL be free of race conditions, deadlocks, livelocks, and resource starvation;

c. If compiled code is used, it SHALL only be compiled using a COTS compiler; and

d. If interpreted code is used, it SHALL only be run under a specific, identified version of a COTS runtime interpreter.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.6.2 Prevent Tampering With Code

Programmed devices SHALL defend against replacement or modification of executable or interpreted code.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.6.3 Prevent Tampering With Data

The voting system SHALL prevent access to or manipulation of configuration data, vote data, or audit records.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.7 Error Checking

4.7.1 Detect Garbage Input

4.7.1.1 Validity check

Programmed devices SHALL check information inputs for completeness and validity.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.7.1.2 Defend against garbage input

Programmed devices SHALL ensure that incomplete or invalid inputs do not lead to irreversible error.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.7.2 Mandatory Internal Error Checking

4.7.2.1 Error checking

Application logic that is vulnerable to the following types of errors SHALL check for these errors at run time and respond defensively (as specified by Requirement 4.7.2.8) when they occur:

- Out-of-bounds accesses of arrays or strings (includes buffers used to move data);
- Stack overflow errors;
- CPU-level exceptions such as address and bus errors, dividing by zero, and the like;
- Variables that are not appropriately handled when out of expected boundaries;
- Numeric overflows; and
- Known programming language specific vulnerabilities.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.7.2.2 Range checking of indices

If the application logic uses arrays, vectors, character sequences, strings or any analogous data structures, and the programming language does not provide automatic run-time range checking of the indices, the indices SHALL be ranged-checked on every access.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.7.2.3 Stack overflows

If stack overflow does not automatically result in an exception, the application logic SHALL explicitly check for and prevent stack overflow.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.7.2.4 CPU traps

The application logic SHALL implement such handlers as are needed to detect and respond to CPU-level exceptions including address and bus errors and dividing by zero.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.7.2.5 Garbage input parameters

All scalar or enumerated type parameters whose valid ranges as used in a callable unit (e.g., function, method, operation, subroutine, procedure.) do not cover the entire ranges of their declared data types SHALL be range-checked on entry to the unit.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.7.2.6 Numeric overflows

If the programming language does not provide automatic run-time detection of numeric overflow, all arithmetic operations that could potentially overflow the relevant data type SHALL be checked for overflow.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.7.2.7 Nullify freed pointers

If pointers are used, any pointer variables that remain within scope after the memory they point to is deallocated SHALL be set to null or marked as invalid (pursuant to the idiom of the programming language used) after the memory they point to is deallocated.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.7.2.8 React to errors detected

The detection of any of the errors enumerated in Requirement 4.7.2.1 SHALL be treated as a complete failure of the callable unit in which the error was detected. An appropriate exception SHALL be thrown and control SHALL pass out of the unit forthwith.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.7.2.9 Do not disable error checks

Error checks detailed in Requirement 4.7.2.1 SHALL remain active in production code.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.7.2.10 Roles authorized to respond to errors

Exceptions resulting from failed error checks or CPU-level exceptions SHALL require intervention by an election official or administrator before voting can continue.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.7.2.11 Election integrity monitoring

The voting system SHALL proactively detect or prevent basic violations of election integrity (e.g., stuffing of the ballot box or the accumulation of negative votes) and alert an election official or administrator if such violations they occur.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.8 Recovery

4.8.1 Voting System Device Failure

4.8.1.1 Resuming normal operations

All voting systems SHALL be capable of resuming normal operations following the correction of a failure in any device.

Test Method: ***Functional***

Test Entity: ***Manufacturer***

4.8.1.2 Failures not compromise voting or audit data

Exceptions and system recovery SHALL be handled in a manner that protects the integrity of all recorded votes and audit log information.

Test Method: Functional

Test Entity: Manufacturer

4.8.1.3 Device survive component failure

All vote capture device SHALL be capable of resuming normal operation following the correction of a failure in any component (e.g., memory, CPU, printer) provided that catastrophic electrical or mechanical damage has not occurred.

Test Method: Functional

Test Entity: Manufacturer

4.8.2 Controlled Recovery

Error conditions SHALL be corrected in a controlled fashion so that voting system status may be restored to the initial state existing before the error occurred.

Test Method: Functional

Test Entity: Manufacturer

4.8.2.1 Nested error conditions

Nested error conditions that are corrected without reset, restart, reboot, or shutdown of the vote capture device SHALL be corrected in a controlled sequence so that voting system status may be restored to the initial state existing before the first error occurred.

Test Method: Functional

Test Entity: Manufacturer

4.8.2.2 Reset CPU error states

CPU-level exceptions that are corrected without reset, restart, reboot, or shutdown of the vote capture device SHALL be handled in a manner that restores the CPU to a normal state and allows the voting system to log the event and recover as with a software-level exception.

Test Method: Functional

Test Entity: Manufacturer

4.8.3 Restore Device to Checkpoints

When recovering from non-catastrophic failure or from any error or malfunction that is within the operator's ability to correct, the voting system SHALL restore the device to

the operating condition existing immediately prior to the error or failure, without loss or corruption of voting data previously stored in the device.

Test Method: ***Functional***

Test Entity: ***Manufacturer***

4.9 Source Code Review

In the source code review, the accredited test lab shall look at programming completeness, consistency, correctness, modifiability, structure, modularity and construction.

4.9.1 Workmanship

Although these requirements are scoped to application logic, in some cases the test lab may need to inspect border logic and third-party logic to assess conformity.

4.9.1.1 Review source versus manufacturer specifications

The test lab SHALL assess the extent to which the application logic adheres to the specifications made in its design documentation.

Test Method: ***Inspection***

Test Entity: ***VSTL***

4.9.1.2 Review source versus coding conventions

The test lab SHALL assess the extent to which the application logic adheres to the published, credible coding conventions chosen by the manufacturer.

Test Method: ***Inspection***

Test Entity: ***VSTL***

4.9.1.3 Review source versus workmanship requirements

The test lab SHALL assess the extent to which the application logic adheres to the requirements of Section 4 Software.

Test Method: ***Inspection***

Test Entity: ***VSTL***

4.9.1.4 Efficacy of built-in self-tests

The test lab SHALL verify the efficacy of built-in measurement, self-test, and diagnostic capabilities.

Test Method: ***Inspection***

Test Entity: ***VSTL***

4.9.2 Security

4.9.2.1 Security control source code review

The test lab SHALL analyze the source code of the security controls to assess whether they function correctly and cannot be bypassed.

Test Method: ***Inspection***

Test Entity: ***VSTL***

Section 5: Security

5.1 Access Control

This section states requirements for the identification of authorized system users, processes and devices and the authentication or verification of those identities as a prerequisite to granting access to system processes and data. It also includes requirements to limit and control access to critical system components to protect system and data integrity, availability, confidentiality, and accountability.

This section applies to all entities attempting to physically enter voting system facilities or to request services or data from the voting system.

5.1.1 Separation of Duties

5.1.1.1 Definition of roles

The voting system SHALL allow the definition of personnel roles with segregated duties and responsibilities on critical processes to prevent a single person from compromising the integrity of the system.

Test Method: Functional

Test Entity: VSTL

5.1.1.2 Access to election data

The voting system SHALL ensure that only authorized roles, groups, or individuals have access to election data.

Test Method: Functional

Test Entity: VSTL

5.1.1.3 Separation of duties

The voting system SHALL require at least two persons from a predefined group for validating the election configuration information, accessing the cast vote records, and starting the tabulation process.

Test Method: Functional

Test Entity: VSTL

5.1.2 Voting System Access

The voting system SHALL provide access control mechanisms designed to permit authorized access and to prevent unauthorized access to the system.

5.1.2.1 Identity verification

The voting system SHALL identify and authenticate each person to whom access is granted, and the specific functions and data to which each person holds authorized access.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.1.2.2 Access control configuration

The voting system SHALL allow the administrator group or role to configure permissions and functionality for each identity, group or role to include account and group/role creation, modification, and deletion.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.1.2.3 Default access control configuration

The voting system's default access control permissions SHALL implement the least privileged role or group needed.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.1.2.4 Escalation prevention

The voting system SHALL prevent a lower-privilege process from modifying a higher-privilege process.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.1.2.5 Operating system privileged account restriction

The voting system SHALL NOT require its execution as an operating system privileged account and SHALL NOT require the use of an operating system privileged account for its operation.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.1.2.6 Logging of account

The voting system SHALL log the identification of all personnel accessing or attempting to access the voting system to the system event log.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.1.2.7 Monitoring voting system access

The SHALL provide tools for monitoring access to the system. These tools SHALL provide specific users real time display of persons accessing the system as well as reports from logs.

Test Method: Functional

Test Entity: VSTL

5.1.2.8 Login failures

The vote capture devices at the kiosk locations and the central server SHALL have the capability to restrict access to the voting system after a preset number of login failures.

a. The lockout threshold SHALL be configurable by appropriate administrators/operators.

b. The voting system SHALL log the event.

c. The voting system SHALL immediately send a notification to appropriate administrators/operators of the event.

d. The voting system SHALL provide a mechanism for the appropriate administrators/operators to reactivate the account after appropriate confirmation.

Test Method: Functional

Test Entity: VSTL

5.1.2.9 Account lockout logging

The voting system SHALL log a notification when any account has been locked out.

Test Method: Functional

Test Entity: VSTL

5.1.2.10 Session time-out

Authenticated sessions on critical processes SHALL have an inactivity time-out control that will require personnel re-authentication when reached. This time-out SHALL be implemented for administration and monitor consoles on all voting system devices.

Test Method: Functional

Test Entity: VSTL

5.1.2.11 Screen lock

Authenticated sessions on critical processes SHALL have a screen-lock functionality that can be manually invoked.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.2 Identification and Authentication

Authentication mechanisms and their associated strength may vary from one voting system capability and architecture to another but all must meet the minimum requirement to maintain integrity and trust. It is important to consider a range of roles individuals may assume when operating different components in the voting system and each may require different authentication mechanisms.

The requirements described in this section vary from role to role. For instance, a kiosk worker will have different identification and authentication characteristics than a voter. Also, for selected critical functions there may be cases where split knowledge or dual authorization is necessary to ensure security. This is especially relevant for critical cryptographic key management functions.

5.2.1 Authentication

5.2.1.1 Strength of authentication

Authentication mechanisms supported by the voting system SHALL support authentication strength of at least 1/1,000,000.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.2.1.2 Minimum authentication methods

The voting system SHALL authenticate users per the minimum authentication methods outlined below.

Test Method: ***Functional***

Test Entity: ***VSTL***

Table 5-1 Roles

GROUP OR ROLE	MINIMUM AUTHENTICATION STRENGTH
Election Judge	Two factor
Kiosk Worker	One factor
Voter	Not required

Election Official	Two factor
Administrator	Two-factor
Application or Process	Digital signature 112 bits of security[1]

5.2.1.3 Multiple authentication mechanisms

The voting system SHALL provide multiple authentication methods to support multi-factor authentication.

Test Method: Functional

Test Entity: VSTL

5.2.1.4 Secure storage of authentication data

When private or secret authentication data is stored by the voting system, it SHALL be protected to ensure that the confidentiality and integrity of the data are not violated.

Test Method: Functional

Test Entity: VSTL

5.2.1.5 Password reset

The voting system SHALL provide a mechanism to reset a password if it is forgotten, in accordance with the system access/security policy.

Test Method: Functional

Test Entity: VSTL

5.2.1.6 Password strength configuration

The voting system SHALL allow the administrator group or role to specify password strength for all accounts including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters per NIST 800-63 Electronic Authentication Guideline Standards.

Test Method: Functional

Test Entity: VSTL

5.2.1.7 Password history configuration

The voting system SHALL enforce password histories and allow the administrator to configure the history length when passwords are stored by the system.

[1] NIST Special Publication 800-57

Test Method: ***Functional***

Test Entity: ***VSTL***

5.2.1.8 Account information password restriction

The voting system SHALL ensure that the user name is not used in the password.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.2.1.9 Automated password expiration

The voting system SHALL provide a means to automatically expire passwords.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.2.1.10 Device authentication

The voting system servers and vote capture devices SHALL identify and authenticate one another using NIST - approved cryptographic authentication methods at the 112 bits of security.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.2.1.11 Network authentication

Remote voting location site Virtual Private Network (VPN) connections (i.e., vote capture devices) to voting servers SHALL be authenticated using strong mutual cryptographic authentication at the 112 bits of security.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.2.1.12 Message authentication

Message authentication SHALL be used for applications to protect the integrity of the message content using a schema with 112 bits of security.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.2.1.13 Message authentication mechanisms

IPsec, SSL, or TLS and MAC mechanisms SHALL all be configured to be compliant with FIPS 140-2 using approved algorithm suites and protocols.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.3 Cryptography

Cryptography serves several purposes in voting systems. They include:

Confidentiality: where necessary the confidentiality of voting records can be provided by encryption;

Authentication: data and programs can be authenticated by a digital signature or message authentication codes (MAC), or by comparison of the cryptographic hashes of programs or data with the reliably known hash values of the program or data. If the program or data are altered, then that alteration is detected when the signature or MAC is verified, or the hash on the data or program is compared to the known hash value. Typically the programs loaded on voting systems and the ballot definitions used by voting systems are verified by the systems, while systems apply digital signatures to authenticate the critical audit data that they output. For remote connections cryptographic user authentication mechanism SHALL be based on strong authentication methods; and

Random number generation: random numbers are used for several purposes including the creation of cryptographic keys for cryptographic algorithms and methods to provide the services listed above, and as identifiers for voting records that can be used to identify or correlate the records without providing any information that could identify the voter.

5.3.1 General Cryptography Requirements

5.3.1.1 Cryptographic functionality

All cryptographic functionality SHALL be implemented using NIST-approved cryptographic algorithms/schemas, or use published and credible cryptographic algorithms/schemas/protocols.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.3.1.2 Required security strength

Cryptographic algorithms and schemas SHALL be implemented with a security strength equivalent to at least 112 bits of security to protect sensitive voting information and election records.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.3.1.3 Use NIST-approved cryptography for communications

Cryptography used to protect information in-transit over public telecommunication networks SHALL use NIST-approved algorithms and cipher suites. In addition the implementations of these algorithms SHALL be NIST-approved (Cryptographic Algorithm Validation Program).

Test Method: ***Function***

Test Entity: ***VSTL***

5.3.2 Key Management

The following requirements apply to voting systems that generate cryptographic keys internally.

5.3.2.1 Key generation methods

Cryptographic keys generated by the voting system SHALL use a NIST-approved key generation method, or a published and credible key generation method.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.3.2.2 Security of key generation methods

Compromising the security of the key generation method (e.g., guessing the seed value to initialize the deterministic random number generator (RNG)) SHALL require as least as many operations as determining the value of the generated key.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.3.2.3 Seed values

If a seed key is entered during the key generation process, entry of the key SHALL meet the key entry requirements in 5.3.3.1. If intermediate key generation values are output from the cryptographic module, the values SHALL be output either in encrypted form or under split knowledge procedures.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.3.2.4 Use NIST-approved key generation methods for communications

Cryptographic keys used to protect information in-transit over public telecommunication networks SHALL use NIST-approved key generation methods. If the approved key generation method requires input from a random number generator, then an approved (FIPS 140-2) random number generator SHALL be used.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.3.2.5 Random number generator health tests

Random number generators used to generate cryptographic keys SHALL implement one or more health tests that provide assurance that the random number generator continues to operate as intended (e.g., the entropy source is not stuck).

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.3.3 Key Establishment

Key establishment may be performed by automated methods (e.g., use of a public key algorithm), manual methods (use of a manually transported key loading device), or a combination of automated and manual methods.

5.3.3.1 Key entry and output

Secret and private keys established using automated methods SHALL be entered into and output from a voting system in encrypted form. Secret and private keys established using manual methods may be entered into or output from a system in plaintext form.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.3.4 Key Handling

5.3.4.1 Key storage

Cryptographic keys stored within the voting system SHALL NOT be stored in plaintext. Keys stored outside the voting system SHALL be protected from disclosure or modification.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.3.4.2 Key zeroization

The voting system SHALL provide methods to zeroize all plaintext secret and private cryptographic keys within the system.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.3.4.3 Support for rekeying

The voting system SHALL support the capability to reset cryptographic keys to new values.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.4 Voting System Integrity Management

This section addresses the secure deployment and operation of the voting system, including the protection of removable media and protection against malicious software.

5.4.1 Protecting the Integrity of the Voting System

5.4.1.1 Cast vote integrity; transmission

The integrity and authenticity of each individual cast vote SHALL be protected from any tampering or modification during transmission.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.4.1.2 Cast vote integrity; storage

The integrity and authenticity of each individual cast vote SHALL be preserved by means of a digital signature during storage.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.4.1.3 Cast vote storage

Cast vote data SHALL NOT be permanently stored on the vote capture device.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.4.1.4 Electronic ballot box integrity

The integrity and authenticity of the electronic ballot box SHALL be protected by means of a digital signature.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.4.1.5 Malware detection

The voting system SHALL use malware detection software to protect against known malware that targets the operating system, services, and applications.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.4.1.6 Updating malware detection

The voting system SHALL provide a mechanism for updating malware detection signatures.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.4.1.7 Validating software on kiosk voting devices

The voting system SHALL provide the capability for kiosk workers to validate the software used on the vote capture devices as part of the daily initiation of kiosk operations.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.5 Communications Security

This section provides requirements for communications security. These requirements address ensuring the integrity of transmitted information and protecting the voting system from external communications-based threats.

5.5.1 Data Transmission Integrity

5.5.1.1 Data integrity protection

Voting systems that transmit data over communications links SHALL provide integrity protection for data in transit through the generation of integrity data (digital signatures and/or message authentication codes) for outbound traffic and verification of the integrity data for inbound traffic.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.5.1.2 TLS/SSL

Voting systems SHALL use at a minimum TLS 1.0, SSL 3.1 or equivalent protocols, including all updates to both protocols and implementations as of the date of the submission (e.g., RFC 5746 for TLS 1.0).

Test Method: ***Functional***

Test Entity: ***VSTL***

5.5.1.3 Virtual private networks (VPN)

Voting systems deploying VPNs SHALL configure them to only allow FIPS-compliant cryptographic algorithms and cipher suites.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.5.1.4 Unique system identifier

Each communicating device SHALL have a unique system identifier.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.5.1.5 Mutual authentication required

Each device SHALL mutually strongly authenticate using the system identifier before additional network data packets are processed.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.5.1.6 Secrecy of ballot data

Data transmission SHALL preserve the secrecy of voters' ballot selections and SHALL prevent the violation of ballot secrecy and integrity.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.5.2 External Threats

Voting systems SHALL implement protections against external threats to which the system may be susceptible.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.5.2.1 Disabling network interfaces

Voting system components SHALL have the ability to enable or disable physical network interfaces.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.5.2.2 Minimizing interfaces

The number of active ports and associated network services and protocols SHALL be restricted to the minimum required for the voting system to function.

Test Method: ***Inspection/Vulnerability***

Test Entity: ***VSTL***

5.5.2.3 Prevention of attacks and security non-compliance

The voting system SHALL block all network connections that are not over a mutually authenticated channel.

Test Method: ***Functional/Vulnerability***

Test Entity: ***VSTL***

5.6 Logging

5.6.1 Log Management

5.6.1.1 Default settings

The voting system SHALL implement default settings for secure log management activities, including log generation, transmission, storage, analysis, and disposal.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.6.1.2 Log access

Logs SHALL only be accessible to authorized roles.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.6.1.3 Log access

The voting system SHALL restrict log access to append-only for privileged logging processes and read-only for authorized roles.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.6.1.4 Logging events

The voting system SHALL log logging failures, log clearing, and log rotation.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.6.1.5 Log format

The voting system SHALL store log data in a publicly documented format, such as XML, or include a utility to export log data into a publicly documented format.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.6.1.6 Log separation

The voting system SHALL ensure that each jurisdiction's event logs and each component's logs are separable from each other.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.6.1.7 Log review

The voting system SHALL include an application or program to view, analyze, and search event logs.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.6.1.8 Log preservation

All logs SHALL be preserved in a useable manner prior to voting system decommissioning.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.6.1.9 Voter privacy

Logs SHALL NOT contain any data that could violate the privacy of the voter's identity.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.6.1.10 Timekeeping format

Timekeeping mechanisms SHALL generate time and date values, including hours, minutes, and seconds.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.6.1.11 Timekeeping precision

The precision of the timekeeping mechanism SHALL be able to distinguish and properly order all log events.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.6.1.12 System clock security

Only the system administrator SHALL be permitted to set the system clock.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.6.2 Communications Logging

5.6.2.1 General

All communications actions SHALL be logged.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.6.2.2 Log content

The communications log SHALL contain at least the following entries:

- Times when the communications are activated and deactivated;
- Services accessed;
- Identification of the device which data was transmitted to or received from;
- Identification of authorized entity; and
- Successful and unsuccessful attempts to access communications or services.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.6.3 System Event Logging

This section describes requirements for the voting system to perform event logging for system maintenance troubleshooting, recording the history of system activity, and detecting unauthorized or malicious activity. The operating system, and/or applications software may perform the actual event logging. There may be multiple logs in use for any system component.

5.6.3.1 Event log format

The voting system SHALL log the following data for each event:

a. System ID;

b. Unique event ID and/or type;

c. Timestamp;

d. Success or failure of event, if applicable;

e. User ID triggering the event, if applicable; and

f. Jurisdiction, if applicable.

Test Method: Inspection

Test Entity: VSTL

5.6.3.2 Critical events

All critical events SHALL be recorded in the system event log.

Test Method: Functional

Test Entity: VSTL

5.6.3.3 System events

At a minimum the voting system SHALL log the events described in the table below.

Test Method: Inspection

Test Entity: VSTL

Table 5-2 System Events

SYSTEM EVENT	DESCRIPTION
GENERAL SYSTEM FUNCTIONS	
Error and exception messages	Includes but not limited to: • The source and disposition of system interrupts resulting in entry into exception handling routines. • Messages generated by exception handlers. • The identification code and number of occurrences for each hardware and software error or failure. • Notification of physical violations of security. • Other exception events such as power failures, failure of critical hardware components, data transmission errors or other types of operating anomalies. • All faults and the recovery actions taken. • Error and exception messages such as ordinary timer system interrupts and normal I/O system interrupts do not need to be logged.
Critical system status messages	Critical system status messages other than information messages displayed by the device during the course of normal operations. Includes but not limited to:

SYSTEM EVENT	DESCRIPTION
	• Diagnostic and status messages upon startup. • The “zero totals” check conducted before starting the voting period.
Non-critical status messages	Non-critical status messages that are generated by the data quality monitor or by software and hardware condition monitors.
Events that require election official intervention	Events that require election official intervention, so that each election official access can be monitored and access sequence can be constructed.
Shutdown and restarts	Both normal and abnormal shutdowns and restarts.
Changes to system configuration settings	Configuration settings include but are not limited to registry keys, kernel settings, logging settings, and other system configuration settings.
Integrity checks for executables, configuration files, data, and logs	Integrity checks that may indicate possible tampering with files and data.
The addition and deletion of files	Files added or deleted from the system.
System readiness results	Includes but not limited to: • System pass or fail of hardware and software test for system readiness. • Identification of the software release, identification of the election to be processed, kiosk locations, and the results of the software and hardware diagnostic tests. • Pass or fail of ballot style compatibility and integrity test. • Pass or fail of system test data removal.
Removable media events	Removable media that is inserted into or removed from the system.
Backup and restore	Successful and failed attempts to perform backups and restores.
Authentication related events	Includes but not limited to: • Login/logoff events (both successful and failed attempts). • Account lockout events. • Password changes.
Access control related events	Includes but not limited to: • Use of privileges. • Attempts to exceed privileges. • All access attempts to application and underlying system resources. • Changes to the access control configuration of the system.
User account and role (or groups) management activity	Includes but not limited to: • Addition and deletion of user accounts and roles. • User account and role suspension and reactivation.

SYSTEM EVENT	DESCRIPTION
	• Changes to account or role security attributes such as password length, access levels, login restrictions, permissions. • Administrator account and role password resets.
Installation, upgrading, patching, or modification of software or firmware	Logging for installation, upgrading, patching, or modification of software or firmware include logging what was installed, upgraded, or modified as well as a cryptographic hash or other secure identifier of the old and new versions of the data.
Changes to configuration settings	Includes but not limited to: • Changes to critical function settings. At a minimum critical function settings include location of ballot definition file, contents of the ballot definition file, vote reporting, location of logs, and system configuration settings. • Changes to settings including but not limited to enabling and disabling services. • Starting and stopping processes.
Abnormal process exits	All abnormal process exits.
Successful and failed database connection attempts (if a database is utilized).	All database connection attempts.
Changes to cryptographic keys	At a minimum critical cryptographic settings include key addition, key removal, and re-keying.
Voting events	Includes: • Opening and closing the voting period. • Casting a vote. • Success or failure of log and election results exportation.

5.7 Incident Response

5.7.1 Incident Response Support

5.7.1.1 Critical events

Manufacturers SHALL document what types of system operations or security events (e.g., failure of critical component, detection of malicious code, unauthorized access to restricted data) are classified as critical.

Test Method: Inspection

Test Entity: VSTL

5.7.1.2 Critical event alarm

An alarm that notifies appropriate personnel SHALL be generated on the vote capture device, system server, or tabulation device, depending upon which device has the error, if a critical event is detected.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.8 Physical and Environmental Security

5.8.1 Physical Access

5.8.1.1 Unauthorized physical access requirement

Any unauthorized physical access SHALL leave physical evidence that an unauthorized event has taken place.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.8.2 Physical Ports and Access Points

5.8.2.1 Non-essential ports

The voting system SHALL disable physical ports and access points that are not essential to voting operations, testing, and auditing.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.8.3 Physical Port Protection

5.8.3.1 Physical port shutdown requirement

If a physical connection between the vote capture device and a component is broken, the affected vote capture device port SHALL be automatically disabled.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.8.3.2 Physical component alarm requirement

The voting system SHALL produce a visual alarm if a connected component is physically disconnected.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.8.3.3 Physical component event log requirement

An event log entry that identifies the name of the affected device SHALL be generated if a vote capture device component is disconnected.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.8.3.4 Physical port enablement requirement

Disabled ports SHALL only be re-enabled by authorized administrators.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.8.3.5 Physical port restriction requirement

Vote capture devices SHALL be designed with the capability to restrict physical access to voting device ports that accommodate removable media with the exception of ports used to activate a voting session.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.8.3.6 Physical port tamper evidence requirement

Vote capture devices SHALL be designed to give a physical indication of tampering or unauthorized access to ports and all other access points, if used as described in the manufacturer's documentation.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.8.3.7 Physical port disabling capability requirement

Vote capture devices SHALL be designed such that physical ports can be manually disabled by an authorized administrator.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.8.4 Door Cover and Panel Security

5.8.4.1 Access points security requirement

Access points such as covers and panels SHALL be secured by locks or tamper evident or tamper resistant countermeasures and SHALL be implemented so that

kiosk workers can monitor access to vote capture device components through these points.

Test Method: Inspection

Test Entity: VSTL

5.8.5 Secure Paper Record Receptacle

5.8.5.1 Secure paper record container requirement

If the voting system provides paper record containers then they SHALL be designed such that any unauthorized physical access results in physical evidence that an unauthorized event has taken place.

Test Method: Inspection

Test Entity: VSTL

5.8.6 Secure Physical Lock and Key

5.8.6.1 Secure physical lock access requirement

Voting equipment SHALL be designed with countermeasures that provide physical indication that unauthorized attempts have been made to access locks installed for security purposes.

Test Method: Inspection

Test Entity: VSTL

5.8.6.2 Secure locking system key requirement

Manufacturers SHALL provide locking systems for securing vote capture devices that can make use of keys that are unique to each owner.

Test Method: Inspection

Test Entity: VSTL

5.8.7 Media Protection

These requirements apply to all media, both paper and digital, that contain personal privacy related data or other protected or sensitive types of information.

5.8.7.1 Kiosk site protection

The voting system SHALL meet the following requirements:

a. All paper records (including rejected ones) printed at the kiosk locations SHALL be deposited in a secure container;

b. Vote capture device hardware, software and sensitive information (e.g., electoral roll) SHALL be physically protected to prevent unauthorized modification or disclosure; and

c. Vote capture device hardware components, peripherals and removable media SHALL be identified and registered by means of a unique serial number or other identifier.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.9 Penetration Resistance

5.9.1 Resistance to Penetration Attempts

5.9.1.1 Resistant to attempts

The voting system SHALL be resistant to attempts to penetrate the system by any remote unauthorized entity.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.9.1.2 System information disclosure

The voting system SHALL be configured to minimize ports, responses and information disclosure about the system while still providing appropriate functionality.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.9.1.3 System access

The voting system SHALL provide no access, information or services to unauthorized entities.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.9.1.4 Interfaces

All interfaces SHALL be penetration resistant including TCP/IP, wireless, and modems from any point in the system.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.9.1.5 Documentation

The configuration and setup to attain penetration resistance SHALL be clearly and completely documented.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.9.2 Penetration Resistance Test and Evaluation

5.9.2.1 Scope

The scope of penetration testing SHALL include all the voting system components. The scope of penetration testing includes but is not limited to the following:

- System server;
- Vote capture devices;
- Tabulation device;
- All items setup and configured per Technical Data Package (TDP) recommendations;
- Local wired and wireless networks; and
- Internet connections.

Test Method: ***Penetration***

Test Entity: ***VSTL***

5.9.2.2 Test environment

Penetration testing SHALL be conducted on a voting system set up in a controlled lab environment. Setup and configuration SHALL be conducted in accordance with the TDP, and SHALL replicate the real world environment in which the voting system will be used.

Test Method: ***Penetration***

Test Entity: ***VSTL***

5.9.2.3 White box testing

The penetration testing team SHALL conduct white box testing using manufacturer supplied documentation and voting system architecture information. Documentation includes the TDP and user documentation. The testing team SHALL have access to any relevant information regarding the voting system configuration. This includes, but is not limited to, network layout and Internet Protocol addresses for system devices and components. The testing team SHALL be provided any source code included in the TDP.

Test Method: ***Penetration***

Test Entity: ***VSTL***

5.9.2.4 Focus and priorities

Penetration testing seeks out vulnerabilities in the voting system that might be used to change the outcome of an election, interfere with voter ability to cast ballots, ballot counting, or compromise ballot secrecy. The penetration testing team SHALL prioritize testing efforts based on the following:

a. Threat scenarios for the voting system under investigation;

b. Remote attacks SHALL be prioritized over in-person attacks;

c. Attacks with a large impact SHALL be prioritized over attacks with a more narrow impact; and

d. Attacks that can change the outcome of an election SHALL be prioritized over attacks that compromise ballot secrecy or cause non-selective denial of service.

Test Method: Penetration

Test Entity: VSTL

Section 6: Quality Assurance

6.1 General Requirements

At a minimum, this program SHALL:

a. Include procedures for specifying, procuring, inspecting, accepting, and controlling parts and raw materials of the requisite quality;

b. Require the documentation of the software development process;

c. Require the documentation of the hardware specification and selection process;

d. Identify and enforce all requirements for:

   i. In-process inspection and testing that the manufacturer deems necessary to ensure proper fabrication and assembly of hardware

   ii. Installation and operation of software and firmware

e. Include plans and procedures for post-production environmental screening and acceptance testing; and

f. Include a procedure for maintaining all data and records required to document and verify the quality inspections and tests.

Test Method: Inspection

Test Entity: Manufacturer

6.2 Components from Third Parties

A manufacturer who does not manufacture all the components of its voting system, but instead procures components as standard commercial items for assembly and integration into a voting system, SHALL verify that the supplier manufacturers follow documented quality assurance procedures that are at least as stringent as those used internally by the voting system manufacturer.

Test Method: Inspection

Test Entity: Manufacturer

6.3 Responsibility for Tests

Manufacturer SHALL be responsible for performing all quality assurance tests, acquiring and documenting test data, and providing test reports for examination by the VSTL as part of the national certification process. These reports SHALL also be provided to the purchaser upon request.

Test Method: Inspection

Test Entity: Manufacturer

6.4 Parts and Materials, Special Tests, and Examinations

In order to ensure that voting system parts and materials function properly, manufacturers SHALL:

a. Select parts and materials to be used in voting systems and components according to their suitability for the intended application. Suitability may be determined by similarity of this application to existing standard practice or by means of special tests;

b. Design special tests, if needed, to evaluate the part or material under conditions accurately simulating the actual voting system operating environment; and

c. Maintain the resulting test data as part of the quality assurance program documentation.

Test Method: Inspection

Test Entity: Manufacturer

6.5 Quality Conformance Inspections

The manufacturer performs conformance inspections to ensure the overall quality of the voting system and components delivered to the VSTL for national certification testing and to the jurisdiction for implementation. To meet the conformance inspection requirements the manufacturer SHALL:

a. Inspect and test each voting system or component to verify that it meets all inspection and test requirements for the voting system; and

b. Deliver a record of tests or a certificate of satisfactory completion with each voting system or component.

Test Method: Inspection

Test Entity: Manufacturer

Section 7: Configuration Management

7.1 Scope

7.1.1 Configuration Management Requirements

The configuration management documentation provided for manufacturer registration SHALL be sufficient for pilot projects.

Test Method: Inspection

Test Entity: EAC

7.1.2 Audit of Configuration Management Documentation

The manufacturer SHALL provide the following documentation to the EAC for review. This documentation will be audited during the registration review which will be conducted during the pilot testing period. The items which the EAC will audit are the following:

a. Application of configuration management requirements;
b. Configuration management policy;
c. Configuration identification;
d. Baseline, promotion, and demotion procedures;
e. Configuration control procedures;
f. Release process;
g. Configuration audits; and
h. Configuration management resources.

Test Method: Inspection

Test Entity: EAC

7.2 Configuration Identification

Configuration identification is the process of identifying, naming, and acquiring configuration items. Configuration identification encompasses all voting system components.

7.2.1 Classification and Naming Configuration Items

Manufacturers SHALL describe the procedures and conventions used to classify configuration items into categories and subcategories, uniquely number or otherwise identify configuration items and name configuration items.

Test Method: Inspection

Test Entity: Manufacturer

7.2.2 Versioning Conventions

When a voting system component is part of a higher level system element such as a subsystem, the manufacturer SHALL describe the conventions used to:

a. Identify the specific versions of individual configuration items and sets of items that are incorporated in higher level system elements such as subsystems;

b. Uniquely number or otherwise identify versions; and

c. Name versions.

Test Method: Inspection

Test Entity: Manufacturer

7.3 Baseline and Promotion Procedures

Manufacturers SHALL establish formal procedures and conventions for establishing and providing a complete description of the procedures and related conventions used to:

a. Establish a particular instance of a component as the starting baseline;

b. Promote subsequent instances of a component to baseline status as development progresses through to completion of the initial completed version released to the VSTL for testing; and

c. Promote subsequent instances of a component to baseline status as the component is maintained throughout its life cycle until system retirement (i.e., the system is no longer sold or maintained by the manufacturer).

Test Method: Inspection

Test Entity: Manufacturer

7.4 Configuration Control Procedures

Configuration control is the process of approving and implementing changes to a configuration item to prevent unauthorized additions, changes or deletions. The manufacturer SHALL establish such procedures and related conventions, providing a complete description of those procedures used to:

a. Develop and maintain internally developed items;

b. Acquire and maintain third-party items;

c. Resolve internally identified defects for items regardless of their origin; and

d. Resolve externally identified and reported defects (i.e., by customers and VSTLs).

Test Method: Inspection

Test Entity: Manufacturer

7.5 Configuration Audits

7.5.1 Physical Configuration Audit (PCA)

For the PCA, a manufacturer SHALL provide:

a. Identification of all items that are to be a part of the pilot release;

b. Specification of compiler (or choice of compilers) to be used to generate voting system executable programs;

c. Identification of all hardware that interfaces with the software;

d. Configuration baseline data for all hardware that is unique to the voting system;

e. Copies of all software documentation intended for distribution to users, including program listings, specifications, operations manual, voter manual, and maintenance manual;

f. Identification of any changes between the physical configuration of the voting system submitted for the PCA and that submitted for the Functional Configuration Audit (FCA), with a certification that any differences do not degrade the functional characteristics; and

g. Complete descriptions of its procedures and related conventions used to support this audit by

   i. Establishing a configuration baseline of the software and hardware to be tested; and

   ii. Confirming whether the voting system documentation matches the corresponding system components.

Test Method: Inspection

Test Entity: VSTL

7.5.2 Functional Configuration Audit (FCA)

The Functional Configuration Audit is conducted by the VSTL to verify that the voting system performs all the functions described in the system documentation. Manufacturers SHALL:

a. Completely describe its procedures and related conventions used to support this audit for all voting system components; and

b. Provide the following information to support this audit:

c. Copies of all procedures used for module or unit testing, integration testing, and system testing;

d. Copies of all test cases generated for each module and integration test, and sample ballot formats or other test cases used for system tests; and

e. Records of all tests performed by the procedures listed above, including error corrections and retests.

Test Method: Functional / Inspection

Test Entity: VSTL

Section 8: Technical Data Package

8.1 Scope

This section contains a description of manufacturer documentation relating to the voting system that must be submitted with the system as a precondition of conformity assessment. These items are necessary to define the product and its method of operation; to provide technical and test data supporting the manufacturer's claims of the system's functional capabilities and performance levels; and to document instructions and procedures governing system operation and field maintenance. Any other items relevant to the system evaluation, such as media, materials, source code, object code, and sample output report formats, must be submitted along with this documentation.

This documentation is used by the VSTL in constructing the test plan. Testing of systems submitted by manufacturers that consistently adhere to particularly strong and well-documented quality assurance and configuration management practices will generally be more efficient than for systems developed and maintained using less rigorous or less well-documented practices.

Both formal documentation and notes of the manufacturer's system development process must be submitted for conformity assessment. Documentation describing the system development process permits assessment of the manufacturer's systematic efforts to develop and test the system and correct defects. Inspection of this process also enables the design of a more precise test plan. The VSTL must design and conduct the appropriate tests to cover all elements of the system and to ensure conformance with all system requirements.

8.1.1 Content and Format

The content of the Technical Data Package (TDP) is intended to provide clear, complete descriptions of the following information about the voting system:

- Overall system design, including subsystems, modules and the interfaces among them;
- Specific functional capabilities provided by the system;
- Performance and design specifications;
- Design constraints, applicable standards, and compatibility requirements;
- Personnel, equipment, and facility requirements for system operation, maintenance, and logistical support;
- Manufacturer practices for assuring system quality during the system's development and subsequent maintenance; and
- Manufacturer practices for managing the configuration of the system during development and for modifications to the system throughout its life cycle.

8.1.1.1 Required content for initial conformity assessment

8.1.1.1.1 Identify full system configuration

Manufacturers SHALL submit to the VSTL documentation necessary for the identification of the full system configuration submitted for evaluation and for the development of an appropriate test plan by the VSTL.

Test Method: Inspection

Test Entity: Manufacturer

8.1.1.1.2 Required content for pilot certification

Manufacturers SHALL provide a list of all documents submitted controlling the design, construction, operation, and maintenance of the voting system. At minimum, the TDP SHALL contain the following documentation:

- Implementation statement;
- Voting system user documentation (See Section 9 Voting Equipment User Documentation);
- System hardware specification;
- Application logic design and specification;
- System security specification;
- System test specification;
- Configuration for testing; and
- Training documentation.

Test Method: Inspection

Test Entity: Manufacturer

8.1.1.2 Format

The requirements for formatting the TDP are general in nature; specific format details are of the manufacturer's choosing.

8.1.1.2.1 Table of contents and abstracts

The TDP SHALL include a detailed table of contents for the required documents, an abstract of each document, and a listing of each of the informational sections and appendices presented.

Test Method: Inspection

Test Entity: Manufacturer

8.1.1.2.2 Cross-index

A cross-index SHALL be provided indicating the portions of the documents that are responsive to the documentation requirements enumerated in section 8.1.1.1.2.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.1.2 Protection of Proprietary Information

8.1.2.1 Identify proprietary data

Manufacturers SHALL identify all documents, or portions of documents, containing proprietary information that is not releasable to the public.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.2 Implementation Statement

8.2.1 TDP Implementation Statement

The TDP SHALL include an implementation statement.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.3 System Hardware Specification

8.3.1 System Hardware Specification Scope

Manufacturers SHALL expand on the system overview included in the user documentation by providing detailed specifications of the hardware components of the voting system, including specifications of hardware used to support the telecommunications capabilities of the voting system, if applicable.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.3.2 System Hardware Characteristics

8.3.2.1 Description of hardware characteristics

Manufacturers SHALL provide a detailed discussion of the characteristics of the system, indicating how the hardware meets individual requirements defined in this document, including:

a. Performance characteristics: Basic system performance attributes and operational scenarios that describe the manner in which system functions are invoked, describe environmental capabilities, describe life expectancy, and describe any other essential aspects of system performance;

b. Physical characteristics: Suitability for intended use, requirements for security criteria, and vulnerability to adverse environmental factors;

c. Reliability: System and component reliability stated in terms of the system's operating functions, and identification of items that require special handling or operation to sustain system reliability; and

d. Environmental conditions: Ability of the system to withstand natural environments, and operational constraints in normal and test environments, including all requirements and restrictions regarding electrical service, telecommunications services, environmental protection, and any additional facilities or resources required to install and operate the system.

Test Method: Inspection

Test Entity: Manufacturer

8.3.3 Design and Construction

8.3.3.1 System configuration

Manufacturers SHALL provide sufficient data, or references to data, to identify unequivocally the details of the system configuration submitted for testing.

Test Method: Inspection

Test Entity: Manufacturer

8.3.3.2 Photographs for hardware validation

Manufacturers SHALL provide photographs of the exterior and interior of devices included in the system to identify the hardware of the system configuration submitted for testing.

Test Method: Inspection

Test Entity: Manufacturer

8.3.3.3 List of materials

Manufacturers SHALL provide a list of materials and components used in the system and a description of their assembly into major system components and the system as a whole.

Test Method: Inspection

Test Entity: Manufacturer

8.3.3.4 Design and construction miscellany

Text and diagrams SHALL be provided that describe:

a. Materials, processes, and parts used in the system, their assembly, and the configuration control measures to ensure compliance with the system specification;

b. Electromagnetic environment generated by the system; and

c. Operator and voter safety considerations and any constraints on system operations or the use environment.

Test Method: Inspection

Test Entity: Manufacturer

8.3.4 Hardwired Logic

8.3.4.1 Hardwired and mechanical implementations of logic

For each non-COTS hardware component (e.g., an application-specific integrated circuit or a manufacturer-specific integration of smaller components), manufacturers SHALL provide complete design and logic specifications, such as Computer Aided Design and Hardware Description Language files.

Test Method: Inspection

Test Entity: Manufacturer

8.3.4.2 Logic specifications for PLDs, FPGAs and PICs

For each Programmable Logic Device (PLD), Field-Programmable Gate Array (FPGA), or Peripheral Interface Controller (PIC) that is programmed with non-COTS logic, manufacturers SHALL provide complete logic specifications, such as Hardware Description Language files or source code.

Test Method: Inspection

Test Entity: Manufacturer

8.4 Application Logic Design and Specification

8.4.1 Application Logic Design and Specification

Manufacturers SHALL expand on the system overview included in the user documentation by providing detailed specifications of the application logic components of the system, including those used to support the telecommunications capabilities of the system, if applicable.

Test Method: Inspection

Test Entity: Manufacturer

8.4.2 Purpose and Scope

8.4.2.1 Application logic functions

Manufacturers SHALL describe the function or functions that are performed by the application logic comprising the system, including that used to support the telecommunications capabilities of the system, if applicable.

Test Method: Inspection

Test Entity: Manufacturer

8.4.3 Applicable Documents

8.4.3.1 Documents controlling application logic development

Manufacturers SHALL list all documents controlling the development of application logic and its specifications.

Test Method: Inspection

Test Entity: Manufacturer

8.4.4 Application Logic Overview

8.4.4.1 Application logic overview

Manufacturers SHALL provide an overview of the application logic.

Test Method: Inspection

Test Entity: Manufacturer

8.4.4.2 Application logic architecture

The overview SHALL include a description of the architecture, the design objectives, and the logic structure and algorithms used to accomplish those objectives.

Test Method: Inspection

Test Entity: Manufacturer

8.4.4.3 Application logic design

The overview SHALL include the general design, operational considerations, and constraints influencing the design.

Test Method: Inspection

Test Entity: Manufacturer

8.4.4.4 Application logic overview miscellany

The overview SHALL include the following additional information for each separate software package:

a. Package identification;

b. General description;

c. Requirements satisfied by the package;

d. Identification of interfaces with other packages that provide data to, or receive data from, the package; and

e. Concept of execution for the package.

Test Method: Inspection

Test Entity: Manufacturer

8.4.5 Application Logic Standards and Conventions

8.4.5.1 Application logic standards and conventions

Manufacturers SHALL provide information on application logic standards and conventions developed internally by the manufacturer as well as published industry standards that have been applied by the manufacturer.

Test Method: Inspection

Test Entity: Manufacturer

8.4.5.2 Application logic standards and conventions, checklist

Manufacturers SHALL provide information that addresses the following standards and conventions related to application logic:

a. Development methodology;

b. Design standards, including internal manufacturer procedures;

c. Specification standards, including internal manufacturer procedures;

d. Coding conventions, including internal manufacturer procedures;

e. Testing and verification standards, including internal manufacturer procedures, that can assist in determining the correctness of the logic; and

f. Quality assurance standards or other documents that can be used to examine and test the application logic. These documents include standards for logic diagrams, program documentation, test planning, and test data acquisition and reporting.

Test Method: Inspection

Test Entity: Manufacturer

8.4.5.3 Justify coding conventions

Manufacturers SHALL furnish evidence that the selected coding conventions are "published" and "credible" as specified in section 4.3.1.

Test Method: Inspection

Test Entity: Manufacturer

8.4.6 Application Logic Operating Environment

8.4.6.1 Application logic operating environment

Manufacturers SHALL describe or make reference to all operating environment factors that influence the design of application logic.

Test Method: Inspection

Test Entity: Manufacturer

8.4.7 Hardware Environment and Constraints

8.4.7.1 Hardware environment and constraints

Manufacturers SHALL identify and describe the hardware characteristics that influence the design of the application logic, such as:

a. Logic and arithmetic capability of the processor;

b. Memory read-write characteristics;

c. External memory device characteristics;

d. Peripheral device interface hardware;

e. Data input/output device protocols; and

f. Operator controls, indicators, and displays.

Test Method: Inspection

Test Entity: Manufacturer

8.4.8 Application Logic Environment

8.4.8.1 Operating system

Manufacturers SHALL identify the operating system and the specific version thereof, or else clarify how the application logic operates without an operating system.

Test Method: Inspection

Test Entity: Manufacturer

8.4.8.2 Compilers and assemblers

For systems containing compiled or assembled application logic, manufacturers SHALL identify the COTS compilers or assemblers used in the generation of executable code, and the specific versions thereof.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.8.3 Interpreters

For systems containing interpreted application logic, manufacturers SHALL specify the COTS runtime interpreter that SHALL be used to run this code, and the specific version thereof.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.9 Application Logic Functional Specification

8.4.9.1 Application logic functional specification

Manufacturers SHALL provide a description of the operating modes of the system and of application logic capabilities to perform specific functions.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.10 Functions and Operating Modes

8.4.10.1 Functions and operating modes

Manufacturers SHALL describe all application logic functions and operating modes of the system, such as ballot preparation, election programming, preparation for opening the voting period, recording votes and/or counting ballots, closing the voting period, and generating reports.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.10.2 Functions and operating modes detail

For each application logic function or operating mode, manufacturers SHALL provide:

a. A definition of the inputs to the function or mode (with characteristics, limits, tolerances or acceptable ranges, as applicable);

b. An explanation of how the inputs are processed; and

c. A definition of the outputs produced (again, with characteristics, limits, tolerances, or acceptable ranges, as applicable).

Test Method: Inspection

Test Entity: Manufacturer

8.4.11 Application Logic Integrity Features

8.4.11.1 Application logic integrity features

Manufacturers SHALL describe the application logic's capabilities or methods for detecting or handling:

a. Exception conditions;

b. System failures;

c. Data input/output errors;

d. Error logging for audit record generation;

e. Production of statistical ballot data;

f. Data quality assessment; and

g. Security monitoring and control.

Test Method: Inspection

Test Entity: Manufacturer

8.4.12 Programming Specifications

8.4.12.1 Programming specifications

Manufacturers SHALL provide in this section an overview of the application logic's design, its structure, and implementation algorithms and detailed specifications for individual modules.

Test Method: Inspection

Test Entity: Manufacturer

8.4.13 Programming Specifications Overview

The programming specifications overview SHALL document the architecture of the application logic.

8.4.13.1 Programming specifications overview, diagrams

This overview SHALL include such items as Unified Modeling Language diagrams, data flow diagrams, and/or other graphical techniques that facilitate understanding of the programming specifications.

Test Method: Inspection

Test Entity: ***Manufacturer***

8.4.13.2 Internal functioning of individual modules

This section SHALL be prepared to facilitate understanding of the internal functioning of the individual modules.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.13.3 Programming specifications overview, content

Implementation of the functions SHALL be described in terms of the architecture, algorithms, and data structures.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.14 Programming Specifications Details

8.4.14.1 Programming specifications details

The programming specifications SHALL describe individual application logic modules and their component units, if applicable.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.14.2 Module and callable unit documentation

For each application logic module and callable unit, manufacturers SHALL document:

a. Significant module and unit design decisions, if any, such as algorithms used;

b. Any constraints, limitations, or unusual features in the design of the module or callable unit; and

c. A description of its inputs, outputs, and other data elements as applicable with respect to communication over system interfaces. (See section 8.4.16 Interfaces.)

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.14.3 Mixed-language software

If an application logic module is written in a programming language other than that generally used within the system, the specification for the module SHALL indicate the programming language used and the reason for the difference.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.14.4 References for foreign programming languages

If a module contains embedded border logic commands for an external library or package (e.g., menu selections in a database management system for defining forms and reports, on-line queries for database access and manipulation, input to a graphical user interface builder for automated code generation, commands to the operating system, or shell scripts), the specification for the module SHALL contain a reference to user manuals or other documents that explain them.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.14.5 Source code

For each callable unit (e.g., function, method, operation, subroutine, procedure) in application logic, border logic, and third-party logic, manufacturers SHALL supply the source code.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.14.6 Inductive assertions

For each callable unit (e.g., function, method, operation, subroutine, procedure) in core logic, manufacturers SHALL specify:

a. Preconditions and postconditions of the callable unit, including any assumptions about capacities and limits within which the system is expected to operate; and

b. A sound argument (preferably, but not necessarily, a formal proof) that the preconditions and postconditions of the callable unit accurately represent its behavior, assuming that the preconditions and postconditions of any invoked units are similarly accurate.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.14.7 High-level constraints

Manufacturers SHALL specify a sound argument (preferably, but not necessarily, a formal proof) that the core logic as a whole satisfies each of the constraints for all cases within the aforementioned capacities and limits, assuming that the preconditions and postconditions of callable units accurately characterize their behaviors.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.14.8 Safety of concurrency

Manufacturers SHALL specify a sound argument (preferably, but not necessarily, a formal proof) that application logic is free of race conditions, deadlocks, livelocks, and resource starvation.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.15 System Database

8.4.15.1 System database

Manufacturers SHALL identify and provide a diagram and narrative description of the system's databases and any external files used for data input or output.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.15.2 Database design levels

For each database or external file, manufacturers SHALL specify the number of levels of design and the names of those levels (e.g., conceptual, internal, logical, and physical).

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.15.3 Database design conventions

For each database or external file, the manufacturer SHALL specify any design conventions and standards (which may be incorporated by reference) needed to understand the design.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.15.4 Data models

For each database or external file, manufacturers SHALL identify and describe all logical entities and relationships and how these are implemented physically (e.g., tables, files).

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.15.5 Schemata

Manufacturers SHALL document the details of table, record or file contents (as applicable), individual data elements and their specifications, including:

a. Names/identifiers;

b. Data type (e.g., alphanumeric, integer);

c. Size and format (such as length and punctuation of a character string);

d. Units of measurement (e.g., meters, seconds

e. Range or enumeration of possible values (e.g., 0–99

f. Accuracy (how correct) and precision (number of significant digits);

g. Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether business rules apply;

h. Security and privacy constraints; and

i. Sources (setting/sending entities) and recipients (using/receiving entities).

Test Method: Inspection

Test Entity: Manufacturer

8.4.15.6 External file maintenance and security

For external files, manufacturers SHALL document the procedures for file maintenance, management of access privileges, and security.

Test Method: Inspection

Test Entity: Manufacturer

8.4.16 Interfaces

8.4.16.1 Description of interfaces

Using a combination of text and diagrams, manufacturers SHALL identify and provide a complete description of all major internal and external interfaces.

Test Method: Inspection

Test Entity: Manufacturer

8.4.17 Interface Identification

8.4.17.1 Interface identification details

For each interface identified in the system overview, manufacturers SHALL:

a. Provide a unique identifier assigned to the interface;

b. Identify the interfacing entities (e.g., systems, configuration items, users) by name, number, version, and documentation references, as applicable; and

c. Identify which entities have fixed interface characteristics (and therefore impose interface requirements on interfacing entities) and which are being

developed or modified (thus having interface requirements imposed upon them).

Test Method: Inspection

Test Entity: Manufacturer

8.4.18 Interface Description

8.4.18.1 Interface types

For each interface identified in the system overview, manufacturers SHALL describe the type of interface (e.g., real-time data transfer, data storage-and-retrieval) to be implemented.

Test Method: Inspection

Test Entity: Manufacturer

8.4.18.2 Interface signatures

For each interface identified in the system overview, manufacturers SHALL describe characteristics of individual data elements that the interfacing entity (ies) will provide, store, send, access, receive, etc., such as:

a. Names/identifiers;

b. Data type (e.g., alphanumeric, integer);

c. Size and format (such as length and punctuation of a character string);

d. Units of measurement (e.g., meters, seconds);

e. Range or enumeration of possible values (e.g., 0–99);

f. Accuracy (how correct) and precision (number of significant digits);

g. Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether business rules apply;

h. Security and privacy constraints; and

i. Sources (setting/sending entities) and recipients (using/receiving entities).

Test Method: Inspection

Test Entity: Manufacturer

8.4.18.3 Interface protocols

For each interface identified in the system overview, manufacturers SHALL describe characteristics of communication methods that the interfacing entity (ies) will use for the interface, such as:

a. Communication links/bands/frequencies/media and their characteristics;

b. Message formatting;

c. Flow control (e.g., sequence numbering and buffer allocation);

d. Data transfer rate, whether periodic/aperiodic, and interval between transfers;

e. Routing, addressing, and naming conventions;

f. Transmission services, including priority and grade; and

g. Safety/security/privacy considerations, such as encryption, user authentication, compartmentalization, and auditing.

Test Method: Inspection

Test Entity: Manufacturer

8.4.18.4 Protocol details

For each interface identified in the system overview, manufacturers SHALL describe characteristics of protocols the interfacing entity (ies) will use for the interface, such as:

a. Priority/layer of the protocol;

b. Packeting, including fragmentation and reassembly, routing, and addressing;

c. Legality checks, error control, and recovery procedures;

d. Synchronization, including connection establishment, maintenance, termination; and

e. Status, identification, and any other reporting features.

Test Method: Inspection

Test Entity: Manufacturer

8.4.18.5 Characteristics of interfaces

For each interface identified in the system overview, manufacturers SHALL describe any other pertinent characteristics, such as physical compatibility of the interfacing entity (ies) (e.g., dimensions, tolerances, loads, voltages, plug compatibility).

Test Method: Inspection

Test Entity: Manufacturer

8.4.19 Appendices

Manufacturers SHALL provide descriptive material and data supplementing the various sections of the body of the logic specifications. The content and arrangement of appendices are at the discretion of the manufacturer. Topics recommended for amplification or treatments in appendix form include:

- Glossary: A listing and brief definition of all module names and variable names, with reference to their locations in the logic structure. Abbreviations, acronyms, and terms should be included, if they are either uncommon in data processing and software development or are used with an unorthodox meaning;

- References: A list of references to all related manufacturer documents, data, standards, and technical sources used in logic development and testing; and
- Program Analysis: The results of logic configuration analysis, algorithm analysis and selection, timing studies, and hardware interface studies that are reflected in the final logic design and coding.

Test Method: Inspection

Test Entity: Manufacturer

8.5 System Security Specification

This section defines the security documentation requirements for systems. These recommendations apply to the full scope of system functionality, including functionality for defining the ballot and other pre-voting functions, as well as functions for casting and storing votes, vote reporting, system logging, and maintenance of the system. User documentation includes all public information that is provided to end users. The Technical Data Package (TDP) includes the user documentation along with proprietary information that is viewed only by the VSTL.

8.5.1 General

8.5.1.1 Overall security

Manufacturers SHALL document in the TDP all aspects of system design, development, and proper usage that are relevant to system security. This includes, but is not limited to the following:

- System security objectives;
- All hardware and software security mechanisms;
- All cryptographic algorithms, protocols and schemes that are used;
- Development procedures employed to ensure absence of malicious code;
- Initialization, usage, and maintenance procedures necessary to secure operation;
- All attacks the system is designed to resist or detect; and
- Any security vulnerabilities known to the manufacturer.

Test Method: Inspection

Test Entity: Manufacturer

8.5.1.2 High level security

Manufacturers SHALL provide at a minimum the high-level documents listed in Table 8-1 as part of the TDP.

Test Method: Inspection

Test Entity: Manufacturer

Table 8-1 High level system documentation

DOCUMENT	DESCRIPTION
Security Threats Controls	This document identifies the threats the system protects against and the implemented security controls on the system and system components.
Security Architecture	This document provides an architecture level description of how the security requirements are met, and SHALL include the various authentication, access control, audit, confidentiality, integrity, and availability requirements.
Interface Specification	This document describes external interfaces (programmatic, human, and network) provided by each of the components of the system.
Design Specification	This document provides a high-level design of each system component.
Development Environment Specification	This document provides descriptions of the physical, personnel, procedural, and technical security of the development environment including configuration management, tools used, coding standards used, software engineering model used, and description of developer and independent testing.
Security Testing and Vulnerability Analysis Documentation	This document describes security tests performed to identify vulnerabilities and the results of the testing. This also includes testing performed as part of software development, such as unit, module, and subsystem testing.

8.5.2 Access Control

8.5.2.1 General user

Manufacturers SHALL provide user documentation of access control capabilities of the system.

Test Method: Inspection

Test Entity: Manufacturer

8.5.2.2 General access control technical specification

Manufacturers SHALL provide descriptions and specifications of all access control mechanisms of the system including management capabilities of authentication, authorization, and passwords.

Test Method: Inspection

Test Entity: Manufacturer

8.5.2.3 Unauthorized access technical specification

Manufacturers SHALL provide descriptions and specifications of methods to prevent unauthorized access to the access control mechanisms of the system.

Test Method: Inspection

Test Entity: Manufacturer

8.5.2.4 Access control dependent system mechanisms

Manufacturers SHALL provide descriptions and specifications of all system mechanisms that are dependent upon, support, and interface with access controls.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.2.5 Voting operations and roles

Manufacturers SHALL provide a list of all of the operations possible on the voting system and list the default roles that have permission to perform each such operation.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.2.6 Critical event escalation

Manufacturers SHALL document a prioritized critical event escalation list of appropriate personnel to be notified.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.3 System Event Logging

8.5.3.1 General

Manufacturers SHALL provide documentation of event logging capabilities of the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.4 Software Installation

8.5.4.1 Software list

Manufacturers SHALL provide a list of all software related to the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.4.2 Software information

Manufacturers SHALL provide, at a minimum, the following information for each piece of software related to the system:

- Software product name;
- Software version number;
- Software manufacturer name;
- Software manufacturer contact information;
- Type of software (application logic, border logic, third party logic, COTS software, or installation software);
- List of software documentation;
- Component identifier(s) (such as filename(s)) of the software; and
- Type of software component (executable code, source code, or data).

Test Method: Inspection

Test Entity: Manufacturer

8.5.4.3 Software location information

Manufacturers SHALL provide the location (such as full path name or memory address) and storage device (such as type and part number of storage device) where each piece of software is installed on programmed devices of the system.

Test Method: Inspection

Test Entity: Manufacturer

8.5.4.4 Software functionality for programmed devices

Manufacturers SHALL document the functionality provided to the system by the software installed on programmed devices.

Test Method: Inspection

Test Entity: Manufacturer

8.5.4.5 Software dependencies and interaction

Manufacturers SHALL map the dependencies and interactions between software installed on programmed devices.

Test Method: Inspection

Test Entity: Manufacturer

8.5.4.6 Build environment software and hardware

Manufacturers SHALL provide a list of all software and hardware required to assemble the build environment used to create system software executable code including application logic, border logic, and third party logic.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.4.7 Build environment assembly procedures

Manufacturers SHALL document the procedures to assemble the build environment(s) used to create system software executable code including application logic, border logic, and third party logic.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.4.8 System software build procedures

Manufacturers SHALL document the procedures used to build the system software executable code including application logic, border logic, and third party logic.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.5 Physical Security

8.5.5.1 Unauthorized physical access

Manufacturers SHALL provide a list of all system components to which access must be restricted and a description of the function of each such component.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.5.2 Physical port and access point

Manufacturers SHALL provide a listing of all ports and access points.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.5.3 Physical lock use

For each lock, manufacturers SHALL document whether the lock was installed to secure an access point.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.5.4 Power usage

Manufacturer SHALL provide a list of all physical security countermeasures that require power supplies.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.5.5 Physical security

Manufacturer SHALL document the design and implementation of all physical security controls for the system and its components.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.6 System Integrity Management

8.5.6.1 Binaries per system

Manufacturers SHALL provide a list of the binaries that are required to be executed on the system devices.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.7 Setup Inspection

8.5.7.1 Software integrity verification

Manufacturers SHALL provide a technical specification of how the integrity of software installed on programmed devices of the system is verified.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.7.2 Software integrity verification technique software non-modification

Manufacturers SHALL provide documentation of software integrity verification techniques that prevent the modification of software installed on programmed devices of the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.7.3 Register and variable value inspection

Manufacturers SHALL provide a technical specification of how the inspection of all the system registers and variables is implemented by the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.7.4 Backup power inspection

Manufacturers SHALL provide a technical specification of how the inspection of the remaining charge of the backup power sources is implemented by the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.7.5 Cabling connectivity inspection

Manufacturers SHALL provide a technical specification of how the inspection of the connectivity of cabling attached is implemented by the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.7.6 Communications operational status inspection

Manufacturers SHALL provide a technical specification of how the inspection of the operational status of the communications capability is implemented by the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.7.7 Communications on/off inspection

Manufacturers SHALL provide a technical specification of how the inspection of the on/off status of the communications capability is implemented by the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.7.8 Consumable inspection

Manufacturers SHALL provide a technical specification of how the inspection of the remaining amount of each consumable is implemented by the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.7.9 Calibration of voting device components inspection

Manufacturers SHALL provide a technical specification of how the inspection of the calibration for each component is implemented by the system.

Test Method: Inspection

Test Entity: Manufacturer

8.5.7.10 Calibration of voting device components adjustment

Manufacturers SHALL provide a technical specification of how the adjustment to the calibration of each component is implemented by the system.

Test Method: Inspection

Test Entity: Manufacturer

8.6 Test Specifications

Manufacturers SHALL provide test specifications for:

a. Development test specifications; and

b. System test specifications.

Test Method: Inspection

Test Entity: Manufacturer

8.6.1 Development Test Specifications

8.6.1.1 Development test specifications

Manufacturers SHALL describe the plans, procedures, and data used during development and system integration to verify system logic correctness, data quality, and security. This description SHALL include:

a. Test identification and design, including test structure, test sequence or progression, and test conditions;

b. Standard test procedures, including any assumptions or constraints;

c. Special purpose test procedures including any assumptions or constraints;

d. Test data, including the data source, whether it is real or simulated, and how test data are controlled;

e. Expected test results; and

f. Criteria for evaluating test results.

Test Method: Inspection

Test Entity: Manufacturer

8.6.2 System Test Specifications

8.6.2.1 Specifications for verification and validation of system performance

Manufacturers SHALL provide specifications for verification and validation of overall system performance. These specifications SHALL cover:

a. Control and data input/output;

b. Processing accuracy;

c. Data quality assessment and maintenance;

d. Ballot interpretation logic;

e. Exception handling;

f. Security;

g. Production of audit trails and statistical data;

h. Expected test results; and

i. Criteria for evaluating test results.

Test Method: Inspection

Test Entity: Manufacturer

8.6.2.2 Demonstrate fitness for purpose

The specifications SHALL identify procedures for assessing and demonstrating the suitability of the system for election use.

Test Method: Inspection

Test Entity: Manufacturer

8.7 Configuration for Testing

8.7.1 Configuration Description

Configuration of hardware and software, both operating systems and applications, is critical to proper system functioning. Correct test design and sufficient test execution must account for the intended and proper configuration of all system components. If the system can be set up in both conforming and nonconforming configurations, the configuration actions necessary to obtain conforming behavior must be specified.

8.7.1.1 Hardware set-up

Manufacturers SHALL provide instructions and photographs illustrating the proper set up of the system hardware.

Test Method: Inspection

Test Entity: Manufacturer

8.7.1.2 Provide answers to installation prompts

Manufacturers SHALL provide a record of all user selections that must be made during software/firmware installation for the system to meet the requirements of the UOCAVA Pilot Testing Requirements.

Test Method: Inspection

Test Entity: Manufacturer

8.7.1.3 Configuration data

Manufacturers SHALL submit all configuration data needed to set up and operate the system.

Test Method: Inspection

Test Entity: Manufacturer

Section 9: System Users Manual

9.1 Scope

This section contains requirements on the content of the documentation that manufacturers supply to jurisdictions that use their systems. In this context, "user" refers to election officials, others in the jurisdictions who implement systems, and VSTLs. The user documentation is also included in the TDP provided to the VSTL.

It is not the intent of these requirements to prescribe an outline for user documentation. Manufacturers are encouraged to innovate in the quality and clarity of their user documentation. The intent of these requirements is to ensure that certain information that is of interest to end users and VSTLs will be included within the user documentation. To expedite the VSTL review, manufacturers SHALL provide the VSTL with a short index that relates the corresponding sections of the user documentation to the specific requirements in this document.

9.2 System Overview

9.2.1 User Documentation System Overview

In the system overview, manufacturers SHALL provide information that enables the user to identify the functional and physical components of the system, how the components are structured, and the interfaces between them.

Test Method: Inspection

Test Entity: Manufacturer

9.2.2 System Overview Functional Diagram

The system overview SHALL include a high-level functional diagram of the system that includes all of its components. The diagram SHALL portray how the various components relate and interact.

Test Method: Inspection

Test Entity: Manufacturer

9.2.3 System Description

9.2.3.1 User documentation system description

The system description SHALL include written descriptions, drawings and diagrams that present:

a. A description of the functional components or subsystems, (e.g., environment, election management and control, vote recording, vote conversion, reporting, and their logical relationships);

b. A description of the operational environment of the system that provides an overview of the hardware, firmware, software, and communications structure;

c. A description that explains each system function and how the function is achieved in the design;

d. Descriptions of the functional and physical interfaces between subsystems and components;

e. Identification of all COTS products (both hardware and software) included in the system and/or used as part of the system's operation, identifying the name, manufacturer, and version used for each such component;

f. Communications (network) software;

g. Interfaces among internal components and interfaces with external systems. For components that interface with other components for which multiple products may be used, the manufacturers SHALL identify file specifications, data objects, or other means used for information exchange, and the public standard used for such file specifications, data objects, or other means; and

h. Listings of all software and firmware and associated documentation included in the manufacturer's release in the order in which each piece of software or firmware would normally be installed upon system setup and installation.

Test Method: Inspection

Test Entity: Manufacturer

9.2.3.2 Identify software and firmware by origin

The system description SHALL include the identification of all software and firmware items, indicating items that were:

a. Written in-house;

b. Written by a subcontractor;

c. Procured as COTS; and

d. Procured and modified, including descriptions of the modifications to the software or firmware and to the default configuration options.

Test Method: Inspection

Test Entity: Manufacturer

9.2.3.3 Traceability of procured software

The system description SHALL include a declaration that procured software items were obtained directly from the manufacturer or from a licensed dealer or distributor.

Test Method: Inspection

Test Entity: Manufacturer

9.2.4 System Performance

9.2.4.1 User documentation system performance

Manufacturers SHALL provide system performance information including:

a. Device capacities and limits that were stated in the implementation statement;

b. Performance characteristics of each operating mode and function in terms of expected and maximum speed, throughput capacity, maximum volume (maximum number of voting positions and maximum number of ballot styles supported), and processing frequency;

c. Quality attributes such as reliability, maintainability, availability, usability, and portability;

d. Provisions for safety, security, voter privacy, ballot secrecy, and continuity of operations; and

e. Design constraints, applicable standards, and compatibility requirements.

Test Method: Inspection

Test Entity: Manufacturer

9.3 System Functionality Description

9.3.1 User Documentation, System Functionality Description

Manufacturers SHALL provide a listing of the system's functional processing capabilities, encompassing capabilities required by the UOCAVA Pilot Program Testing Requirements, and any additional capabilities provided by the system, with a description of each capability.

a. Manufacturers SHALL explain, in a manner that is understandable to users, the capabilities of the system declared in the implementation statement;

b. Additional capabilities (extensions) SHALL be clearly indicated;

c. Required capabilities that may be bypassed or deactivated during installation or operation by the user SHALL be clearly indicated;

d. Additional capabilities that function only when activated during installation or operation by the user SHALL be clearly indicated; and

e. Additional capabilities that normally are active but may be bypassed or deactivated during installation or operation by the user SHALL be clearly indicated.

Test Method: Inspection

Test Entity: Manufacturer

9.4 System Security Specification

9.4.1 Access Control

9.4.1.1 Access control implementation, configuration, and management

Manufacturers SHALL provide user documentation containing guidelines and usage instructions on implementing, configuring, and managing access control capabilities.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.4.1.2 Access control policy

Manufacturers SHALL provide, within the user documentation, the access control policy under which the system was designed to operate.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.4.1.3 Privileged account

Manufacturers SHALL disclose and document information on all privileged accounts included on the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.4.2 System Event Logging

9.4.2.1 System event logging

Manufacturers SHALL provide user documentation that describes system event logging capabilities and usage.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.4.2.2 Log format

Manufacturers SHALL provide fully documented log format information.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.4.3 Ballot Decryption

9.4.3.1 Ballot decryption process

Manufacturers SHALL provide documentation on the proper procedures for the authorized entity to implement ballot decryption while maintaining the security and privacy of the data.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.4.3.2 Ballot decryption key reconstruction

Manufacturers SHALL provide documentation describing the proper procedure for the authorized entity to reconstruct the election private key to decrypt the ballots.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.4.3.3 Ballot decryption key destruction

Manufacturers SHALL document when any cryptographic keys created or used by the system may be destroyed. The documentation SHALL describe how to delete keys securely and irreversibly at the appropriate time.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.4.4 Physical Security

9.4.4.1 Physical security

Manufacturers SHALL provide user documentation explaining the implementation of all physical security controls for the system, including procedures necessary for effective use of countermeasures.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.4.5 Audit

9.4.5.1 Ballot count and vote total auditing

The system's user documentation SHALL fully specify a secure, transparent, workable and accurate process for producing all records necessary to verify the accuracy of the electronic tabulation result.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.5 Software

9.5.1 Software installation

9.5.1.1 Software list

Manufacturers SHALL provide a list of all software to be installed on the programmed devices of the system and installation software used to install the software.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.5.1.2 Software information

Manufacturers SHALL provide at a minimum, the following information for each piece of software to be installed or used to install software on programmed devices of the system: software product name, software version number, software manufacturer name, software manufacturer contact information, type of software (application logic, border logic, third party logic, COTS software, or installation software), list of software documentation, component identifier(s) (such filename(s)) of the software, type of software component (executable code, source code, or data).

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.5.1.3 Software location information

Manufacturers SHALL provide the location (such as full path name or memory address) and storage device (such as type and part number of storage device) where each piece of software is installed on programmed devices of the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.5.1.4 Election specific software identification

Manufacturers SHALL identify election specific software in the user documentation.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.5.1.5 Installation software and hardware

Manufacturers SHALL provide a list of software and hardware required to install software on programmed devices of the system in the user documentation.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.5.1.6 Software installation procedure

Manufacturers SHALL document the software installation procedures used to install software on programmed devices of the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.5.1.7 Compiler installation prohibited

The software installation procedures used to install software on programmed devices of the system SHALL specify that no compilers SHALL be installed on the programmed device.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.5.1.8 Procurement of system software

The software installation procedures SHALL specify that system software SHALL be obtained from the VSTL or approved distribution repositories.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.5.1.9 Erasable storage media preparation

The software installation procedures SHALL specify how previously stored information on erasable storage media is removed before installing software on the media.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.5.1.10 Installation media unalterable storage media

The software installation procedures SHALL specify that unalterable storage media SHALL be used to install software on programmed devices of the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.5.1.11 Software hardening

Manufacturers SHALL provide documentation that describes the hardening procedures for the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6 Setup Inspection

9.6.1 Setup inspection process

Manufacturers SHALL provide a setup inspection process that the system was designed to support.

Test Method: Inspection

Test Entity: Manufacturer

9.6.1.1 Minimum properties included in a setup inspection process

A setup inspection process SHALL, at a minimum, include the inspection of system software, storage locations that hold election information that changes during an election, and execution of logic and accuracy testing related to readiness for use in an election.

Test Method: Inspection

Test Entity: Manufacturer

9.6.1.2 Setup inspection record generation

The setup inspection process SHALL describe the records that result from performing the setup inspection process.

Test Method: Inspection

Test Entity: Manufacturer

9.6.1.3 Installed software identification procedure

Manufacturers SHALL provide the procedures to identify all software installed on programmed devices.

Test Method: Inspection

Test Entity: Manufacturer

9.6.1.4 Software integrity verification procedure

Manufacturers SHALL describe the procedures to verify the integrity of software installed on programmed devices of system.

Test Method: Inspection

Test Entity: Manufacturer

9.6.1.5 Election information value

Manufacturers SHALL provide the values of system storage locations that hold election information that changes during the election, except for the values set to conduct a specific election.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.6 Maximum values of election information storage locations

Manufacturers SHALL provide the maximum values for the storage locations where election information is stored.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.7 Backup power operational range

Manufacturers SHALL provide the nominal operational range for the backup power sources of the voting system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.8 Backup power inspection procedure

Manufacturers SHALL provide the procedures to inspect the remaining charge of the backup power sources of the voting system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.9 Cabling connectivity inspection procedure

Manufacturers SHALL provide the procedures to inspect the connectivity of the cabling attached to the vote capture device.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.10 Communications operational status inspection procedure

Manufacturers SHALL provide the procedures to inspect the operational status of the communications capabilities of the vote capture device.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.11 Communications on/off status inspection procedure

Manufacturers SHALL provide the procedures to inspect the on/off status of the communications capabilities of the vote capture device.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.12 Consumables quantity of vote capture device

Manufacturers SHALL provide a list of consumables associated with the vote capture device, including estimated number of usages per quantity of consumable.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.13 Consumable inspection procedure

Manufacturers SHALL provide the procedures to inspect the remaining amount of each consumable of the vote capture device.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.14 Calibration of vote capture device components nominal range

Manufacturers SHALL provide a list of components associated with the vote capture devices that require calibration and the nominal operating ranges for each component.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.15 Calibration of vote capture device components inspection procedure

Manufacturers SHALL provide the procedures to inspect the calibration of each component.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.16 Calibration of vote capture device components adjustment procedure

Manufacturers SHALL provide the procedures to adjust the calibration of each component.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.17 Checklist of properties to be inspected

Manufacturers SHALL provide a checklist of other properties of the system to be inspected.

Test Method: ***Inspection***

9.7 System Operations Manual

9.7.1 General

9.7.1.1 System operations manual

The system operations manual SHALL provide all information necessary for system set up and use by all personnel who administer and operate the system at the state and/or local election offices and at the kiosk locations, with regard to all system functions and operations identified in Section 9.3 System Functionality Description.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.1.2 Support training

The system operations manual SHALL contain all information that is required for the preparation of detailed system operating procedures and for the training of administrators, state and/or local election officials, election judges, and kiosk workers.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.2 Introduction

9.7.2.1 Functions

Manufacturers SHALL provide a summary of system operating functions to permit understanding of the system's capabilities and constraints.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.2.2 Roles

The roles of operating personnel SHALL be identified and related to the functions of the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.2.3 Conditional actions

Decision criteria and conditional operator functions (such as error and failure recovery actions) SHALL be described.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.2.4 References

Manufacturers SHALL list all reference and supporting documents pertaining to the use of the system during election operations.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.3 Operational Environment

9.7.3.1 Operational environment

Manufacturers SHALL describe the system environment and the interfaces between the system and state and/or local election officials, kiosk workers, system administrators, and voters.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.3.2 Operational environment; equipment and facility

Manufacturers SHALL identify all facilities, furnishings, fixtures, and utilities that will be required for equipment operations, including equipment that operates at the:

a. Kiosk locations;

b. State and/or local election offices; and

c. Other locations.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.3.3 Operational environment; installation

The operations manual SHALL include a statement of all requirements and restrictions regarding environmental protection, electrical service, recommended auxiliary power, telecommunications service, and any other facility or resource required for the proper installation and operation of the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.4 System Installation and Test Specification

9.7.4.1 Readiness testing

Manufacturers SHALL provide specifications for testing of system installation and readiness.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.4.1.1 Readiness test entire system

These specifications SHALL cover testing of all components of the system and all locations of installation (e.g., kiosk locations, state and/or local election offices), and SHALL address all elements of system functionality and operations identified in Section 9.3 System Functionality Description above, including general capabilities and functions specific to particular voting activities.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.5 Operational Features

9.7.5.1 Features

Manufacturers SHALL provide documentation of system operating features that includes:

a. Detailed descriptions of all input, output, control, and display features accessible to the operator or voter;

b. Examples of simulated interactions to facilitate understanding of the system and its capabilities;

c. Sample data formats and output reports; and

d. Illustration and description of all status indicators and information messages.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.5.2 Document straight party override algorithms

For systems that support straight party voting, manufacturers SHALL document the available algorithms for counting straight party overrides.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.5.3 Document double vote reconciliation algorithms

For systems that support write-in voting, manufacturers SHALL document the available algorithms for reconciling write-in double votes.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.6 Operating Procedures

9.7.6.1 Operating procedures

Manufacturers SHALL provide documentation of system operating procedures that:

a. Provides a detailed description of procedures required to initiate, control, and verify proper system operation;

b. Enables the operator to assess the correct flow of system functions (as evidenced by system-generated status and information messages);

c. Enables the administrator to intervene in system operations to recover from an abnormal system state;

d. Defines and illustrates the procedures and system prompts for situations where operator intervention is required to load, initialize, and start the system;

e. Defines and illustrates procedures to enable and control the external interface to the system operating environment if supporting hardware and software are involved. Such information also SHALL be provided for the interaction of the system with other data processing systems or data interchange protocols;

f. Provides administrative procedures and off-line operator duties (if any) if they relate to the initiation or termination of system operations, to the assessment of system status, or to the development of an audit trail;

g. Supports successful ballot and program installation and control by state and/or local election officials;

h. Provides a schedule and steps for the software and ballot installation, including a table outlining the key dates, events and deliverables; and

i. Specifies diagnostic tests that may be employed to identify problems in the system, verify the correction of problems, and isolate and diagnose faults from various system states.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.6.2 Printer error recovery guidelines

Manufacturers SHALL provide documentation for procedures to recover from printer errors and faults including procedures for how to cancel a vote suspended during an error.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.7 Transportation and Storage

9.7.7.1 Transportation

Manufacturers SHALL include any special instructions for preparing vote capture devices for shipment.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.7.2 Storage

Manufacturers SHALL include any special storage instructions for vote capture devices.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.7.3 Precautions for removable media

Manufacturers SHALL detail the care and handling precautions necessary for removable media and records.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.8 Appendices

Manufacturers SHALL provide descriptive material and data supplementing the various sections in the body of the system operations manual. The content and arrangement of appendices are at the discretion of the manufacturer. Topics required for discussion include:

- Glossary: A listing and brief definition of all terms that may be unfamiliar to persons not trained in either systems or computer operations;
- References: A list of references to all manufacturer documents and to other sources related to operation of the system;
- Detailed Examples: Detailed scenarios that outline correct system responses to faulty operator input; and
- Manufacturer's Recommended Security Procedures: Security procedures that are to be executed by the system operator.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.8 System Maintenance Manual

9.8.1.1 User documentation system maintenance manual

The system maintenance manual SHALL provide information to support election officials, kiosk workers, information systems personnel, or maintenance personnel in the adjustment or removal and replacement of components or modules in the field.

Test Method: Inspection

Test Entity: Manufacturer

9.8.1.2 General contents

Manufacturers SHALL describe service actions recommended to correct malfunctions or problems; personnel and expertise required to repair and maintain the system, equipment, and materials; and facilities needed for proper maintenance.

Test Method: Inspection

Test Entity: Manufacturer

9.8.2 Introduction

9.8.2.1 Equipment overview, maintenance viewpoint

Manufacturers SHALL describe the structure and function of the hardware, firmware and software for election preparation, programming, vote recording, tabulation, and reporting in sufficient detail to provide an overview of the system for maintenance and for identification of faulty hardware or software.

Test Method: Inspection

Test Entity: Manufacturer

9.8.3 Maintenance Procedures

9.8.3.1 Maintenance manual maintenance procedures

Manufacturers SHALL describe preventive and corrective maintenance procedures for hardware, firmware and software.

Test Method: Inspection

Test Entity: Manufacturer

9.8.3.2 Maintenance manual preventive maintenance procedures

Manufacturers SHALL identify and describe:

a. All required and recommended preventive maintenance tasks, including software and data backup, database performance analysis, and database tuning;

b. Number and skill levels of personnel required for each task;

c. Parts, supplies, special maintenance equipment, software tools, or other resources needed for maintenance; and

d. Any maintenance tasks that must be referred to the manufacturer.

Test Method: Inspection

Test Entity: Manufacturer

9.8.3.3 Corrective maintenance procedures

9.8.3.3.1 Troubleshooting procedures

Manufacturers SHALL provide fault detection, fault isolation, correction procedures, and logic diagrams for all operational abnormalities identified by design analysis and operating experience.

Test Method: Inspection

Test Entity: Manufacturer

9.8.3.3.2 Troubleshooting procedures details

Manufacturers SHALL identify specific procedures to be used in diagnosing and correcting problems in the system hardware, firmware and software. Descriptions SHALL include:

a. Steps to replace failed or deficient equipment;

b. Steps to correct deficiencies or faulty operations in software or firmware;

c. Number and skill levels of personnel needed to accomplish each procedure;

d. Special maintenance equipment, parts, supplies, or other resources needed to accomplish each procedure; and

e. Any coordination required with the manufacturer.

Test Method: Inspection

Test Entity: Manufacturer

9.8.4 Maintenance Equipment

9.8.4.1 Special equipment

Manufacturers SHALL identify and describe any special purpose test or maintenance equipment recommended for fault isolation and diagnostic purposes.

Test Method: Inspection

Test Entity: Manufacturer

9.8.5 Parts and Materials

Manufacturers SHALL provide detailed documentation of parts and materials needed to operate and maintain the system.

Test Method: Inspection

Test Entity: Manufacturer

9.8.6 Maintenance Facilities and Support

9.8.6.1 Maintenance environment

Manufacturers SHALL identify all facilities, furnishings, fixtures, and utilities that will be required for equipment maintenance.

Test Method: Inspection

Test Entity: Manufacturer

9.8.6.2 Maintenance support and spares

Manufacturers SHALL specify:

a. Recommended number and locations of spare devices or components to be kept on hand for repair purposes during periods of system operation;

b. Recommended number and locations of qualified maintenance personnel who need to be available to support repair calls during system operation; and

c. Organizational affiliation (e.g., jurisdiction, manufacturer) of qualified maintenance personnel.

Test Method: Inspection

Test Entity: Manufacturer

9.8.7 Appendices

Manufacturers SHALL provide descriptive material and data supplementing the various sections in the body of the system maintenance manual. The content and arrangement of appendices are at the discretion of the manufacturer. Topics required for amplification or treatment in an appendix includes:

- Glossary: A listing and brief definition of all terms that may be unfamiliar to persons not trained in either systems or computer maintenance;
- References: A list of references to all manufacturer documents and other sources related to maintenance of the system;
- Detailed Examples: Detailed scenarios that outline correct system responses to faulty operator input; and

- Maintenance and Security Procedures: Technical illustrations and schematic representations of electronic circuits unique to the system.

Test Method: Inspection

Test Entity: Manufacturer

9.9 Personnel Deployment and Training Requirements

Manufacturers SHALL describe the personnel resources and training required for a jurisdiction to operate and maintain the system for the duration of the pilot project.

Test Method: Inspection

Test Entity: Manufacturer

9.9.1 Personnel

9.9.1.1 Training manual personnel

Manufacturers SHALL specify the number of personnel and skill levels required to perform each of the following functions:

a. Pre-voting or election preparation functions;

b. System operations for system functions performed at the kiosk locations;

c. System operations for system functions performed at the state and/or local election offices;

d. Preventive maintenance tasks;

e. Diagnosis of faulty hardware, firmware, or software;

f. Corrective maintenance tasks; and

g. Testing to verify the correction of problems.

Test Method: Inspection

Test Entity: Manufacturer

9.9.1.2 User functions versus manufacturer functions

Manufacturers SHALL distinguish which functions may be carried out by user personnel and which must be performed by manufacturer personnel.

Test Method: Inspection

Test Entity: Manufacturer

9.9.2 Training

9.9.2.1 Training requirements

Manufacturers SHALL provide training materials to instruct system administrators, kiosk workers, and state and/or local election officials on how to set up, configure and operate the system.

Test Method: Inspection

Test Entity: Manufacturer

Appendix A: Glossary

This section defines selected terms and acronyms used in this document. Readers may be familiar with many of these terms, but the definitions as used herein may differ from those in other contexts.

Terminology for standardization purposes must be sufficiently precise and formal to avoid ambiguity in the interpretation and testing of the requirements. Any term that is not defined here retains its common English usage meaning.

absentee ballot:	A ballot cast from any location not defined as a polling place.
absentee model:	The ballot remains associated with the voter ID until the close of the voting period and is subject to an adjudication process to be accepted for tabulation.
absentee voting:	The process of casting a ballot from any location not defined as a polling place.
accessible voting station:	Voting station specially equipped for individuals with disabilities referred to in HAVA 301 (a)(3)(B).
administrator:	The role responsible for installing, configuring, and managing the technical operations of the system.
alert time:	The amount of time the system will wait for detectible voter activity after issuing an alert before going into an inactive state requiring poll worker intervention.
application logic:	Software, firmware, or hardwired logic from any source that is specific to the system, with the exception of border logic.
audio-tactile interface	Voter interface designed to not require visual reading of a ballot. Audio is used to convey information to the voter and sensitive tactile controls allow the voter to convey information to the voting system.
authenticated session:	Process that requires all users to provide proof of identity.
ballot image:	Human-readable electronic representation of the ballot, including the voter's selections.
ballot measure:	Contest in which the choices are Yes and No.
ballot secrecy:	Not being able to associate the selections of the ballot with the voter who cast it.
ballot style:	Particular set of contests to appear on the ballot for a particular election district, their order, the list of ballot positions for each contest, and the binding of candidate names to ballot positions
ballot:	The official presentation of all of the contests to be decided in a particular election. See also ballot image, cast vote record, and paper record.
baseline configuration:	The exact system configuration tested by the VSTL. It includes all the system components that were tested, including the specific hardware, operating system, application software, and third-party COTS applications.
border logic:	Software, firmware, or hardwired logic that is developed to connect application logic to COTS or third-party logic.

callable unit:	Function, method, operation, subroutine, procedure, or analogous structural unit that appears within a module (of a software program or analogous logical design).
candidate:	Person contending in a contest for office.
cast ballot:	Ballot in which the voter has taken final action in the selection of contest choices and submitted it for tabulation.
cast vote record:	The record of all votes selected by a voter.
common industry format:	Format described in ISO/IEC 25062:2006 "Common Industry Format (CIF) for Usability Test Reports".
completed system response time	The time taken from when the voter performs some detectible action to when the voting system completes its response and settles into a stable state (e.g., finishes "painting" the screen with a new page).
component:	A discrete and identifiable element of hardware or software within a system.
concept of operations:	Description of roles and responsibilities for system administration, operation and use.
configuration data:	Non-executable input to software, firmware, or hardwired logic, not including vote data.
conformity assessment:	Demonstration that specified requirements relating to a product, process, system, person or body are fulfilled.
contest:	A single decision being put before the voters (e.g., the selection of a candidate for office or the response to ballot questions).
core logic:	Subset of application logic that is responsible for vote recording and tabulation.
COTS:	Commercial Off the Shelf
credible methodologies:	Methodologies (e.g., coding conventions, cryptographic algorithms) are considered credible if at least two organizations other than the voting system manufacturer have independently adopted them and made active use of them at some time within the three years before conformity assessment was first sought.
cryptography:	The protection of information by converting the information into an unreadable format.
CVR:	Cast vote record
device:	Functional unit that performs its assigned tasks as an integrated whole.
election definition:	Definition of the contests and questions that will appear on the ballot for a specific election.
election judge:	A member of the canvassing board that adjudicates the acceptance of absentee ballots
election management system:	Set of processing functions and databases within a system that defines, develops and maintains election databases, performs election definitions and setup functions, formats ballots, counts votes, consolidates and reports results, and maintains audit trails
election officials:	The persons responsible for administering and conducting elections.
election title:	The heading on a ballot specifying the name of the election (e.g., General Election, Primary Election).

equivalent configuration:	A system configuration that has been attested to by the manufacturer to perform identically to the baseline configuration.
error rate:	Ratio of the number of errors detected in relation to the volume of data processed:
failure:	Events that result in (a) loss of one or more functions, (b) degradation of performance such that the device is unable to perform its intended function for longer than 10 seconds, (c) automatic reset, restart or reboot of the voting device, operating system or application software, (d) a requirement for an unanticipated intervention by a person in the role of kiosk worker or technician before normal operation can continue, or (e) error messages and/or audit log entries indicating that a failure has occurred.
fault:	Flaw in design or implementation that may result in the qualities or behavior of the system deviating from the qualities or behavior that are specified in the UOCAVA Pilot Program Testing Requirements and/or in manufacturer-provided documentation.
functional:	Functional testing is the determination through operational testing of whether the behavior of a system or device in specific scenarios conforms to requirements. Functional tests are derived by analyzing the requirements and the behaviors that should result from implementing those requirements.
hardwired logic:	Logic implemented through the design of an integrated circuit; the programming of a Programmable Logic Device (PLD), Field-Programmable Gate Array (FPGA), Peripheral Interface Controller (PIC), or similar; the integration of smaller hardware components; or mechanical design (e.g., as in lever machines).
initial system response time	The time taken from when the voter performs some detectible action (such as pressing a button) to when the voting system begins responding in some obvious way (such as an audible response or any change on the screen).
implementation statement:	Statement by a manufacturer indicating the capabilities, features, and optional functions and extensions that have been implemented in a system.
inspection:	Examination of a product design, product, process or installation and determination of its conformity with specific requirements or, on the basis of professional judgment, with general requirements.
kiosk:	A terminal tasked to display information, accepts user input, and transmit information
kiosk workers:	Election workers who staff the remote voting kiosk locations.
manufacturer:	Entity with ownership and control over a system submitted for testing.
module:	Structural unit of software or analogous logical design, typically containing several callable units that are tightly coupled.
paper record identifier:	Unique randomly generated code that links the paper record to the corresponding cast vote record.
paper record receptacle:	A secure unit for storing paper records at kiosk locations.
paper record:	Printed record of ballot selections made by the voter.
programmed device:	Electronic device that includes application logic.
published:	Methodologies (e.g., coding conventions, cryptographic algorithms) are considered published if they appear in publicly available media.
straight party override:	Ability to make an exception to straight party voting in selected races.

straight party voting:	Mechanism that allows voters to cast a single vote to select all candidates on the ballot from a single political party.
tabulation device:	A device used to calculate election results.
third-party logic:	Software, firmware, or hardwired logic that is neither application logic nor COTS; e.g., general-purpose software developed by a third party that is either customized (e.g., ported to a new platform, as is Windows CE) or not widely used, or source code generated by a COTS package.
UOCAVA:	Uniformed and Overseas Citizens Absentee Voting Act
vote capture device:	Device that is used directly by a voter to vote a ballot.
voted ballot:	Ballot that contains all of a voter's selections and has been cast.
voter inactivity time:	The amount of time from when the system completes its response until there is detectible voter activity. In particular, note that audio prompts from the system may take several minutes and that this time does not count as voter inactivity.
voter privacy:	The inability of anyone to observe, or otherwise determine, what selections a voter has made.
voting process:	Entire array of procedures, people, resources, equipment and locations associated with the conduct of elections.
voting session:	Span of time beginning when a ballot is enabled or activated and ending when the ballot is cast.
voting system:	Equipment (including hardware, firmware, and software), materials, and documentation used to define elections and ballot styles, configure voting equipment, identify and validate voting equipment configurations, perform readiness tests, activate ballots, capture votes, count votes, generate reports, transmit election data, archive election data, and audit elections.
VPN:	Virtual Private Network
VSTL:	Voting System Test Laboratory
white-box testing:	Uses an internal perspective of the system to design test cases based on internal structure. White box testing strategy deals with the internal logic and structure of the code.
write-in:	To make a selection of an individual not listed on the ballot.

Appendix B: List of References

The following is a list of documents or publications used in the creation of the UOCAVA Pilot Program Testing Requirements.

ANSI 02:	ANSI/TIA-968-A: 2002, Technical Requirements for Connection of Terminal Equipment to the Telephone Network.
BS 7799:	Data center certification standard
CERT 06:	CERT® Coordination Center, Secure Coding homepage, July 2006, Available from http://www.cert.org/secure-coding/.
DHS 06:	Department of Homeland Security, Build Security In, July 2006, Available from https://buildsecurityin.us-cert.gov/.
EAC06:	U.S. Election Assistance Commission, Testing and Certification Program Manual, Version 1.0, December 5, 2006. Available from http://www.eac.gov/program-areas/voting-systems/docs/testingandcertmanual.pdf/attachment_download/file.
FIPS 81:	(1980): DES Modes of Operation
FIPS 46-3:	(1999): Data Encryption Standard (DES)
FIPS 140-2:	Security Requirements for Cryptographic Modules
FIPS 180-2:	(2002): Secure Hash Standard (SHA1)
FIPS 186-2:	(2000): Digital Signature Standard (DSS)
FIPS 197:	(2001): Advanced Encryption Standard (AES)
FIPS 198:	(2002): The Keyed-Hash Message Authentication Code (HMAC)
FIPS 200:	Minimum security requirements for federal information and information systems.
FCC 07a:	Title 47, Part 68, Rules and Regulations of the Federal Communications Commission, Connection of Terminal Equipment to the Telephone Network: 2000.
GPO 90:	Performance and Test Standards for Punchcard, Marksense, and Direct Recording Electronic Voting Systems, January 1990 edition with April 1990 revisions, in Voting System Standards, U.S. Government Printing Office, 1990.14 Available from http://josephhall.org/fec_vss_1990_pdf/1990_VSS.pdf.
GPO 99:	Government Paper Specification Standards No. 11, February 1999.
HAVA 02:	The Help America Vote Act of 2002, Public Law 107-252. Available from http://www.fec.gov/hava/hava.htm.
HFP 07:	Human Factors and Privacy Subcommittee of the TGDC, “Usability Performance Benchmarks for the VVSG,” August 2007. Available from http://vote.nist.gov/meeting-08172007/Usability-Benchmarks-081707.pdf.
IEEE 00:	IEEE 100:2000 The Authoritative Dictionary of IEEE Standard Terms, Seventh Edition.

IEEE 97:	IEEE/EIA 12207.1-1997, Industry implementation of International Standard ISO/IEC 12207:1995—(ISO/IEC 12207) standard for information technology—software life cycle processes—life cycle data.
IEEE 98:	IEEE Std 829-1998, IEEE standard for software test documentation.
IETF RFC 2246:	(1999): The TLS Protocol Version 1.0
IETF RFC 2510:	(1999): Internet X.509 PKI Certificate Management Protocols
IETF RFC 2817:	(2000): Upgrading to TLS within HTTP/1.1
IETF RFC 2818:	(2000): HTTP Over TLS
IETF RFC 3280:	(1999): Internet X.509 PKI Certificate and CRL Profile
IETF RFC 3369:	(2002): Cryptographic Message Syntax
IETF RFC 3370:	(2002): Cryptographic Message Syntax (CMS) Algorithms
IETF RFC 3546:	(2003): TLS Extensions
IETF RFC 3739:	(2004): Internet X.509 PKI Qualified Certificates Profile
IETF RFC 4279:	(2005): Pre-Shared Key Cipher suites for TLS
ISO 00:	ISO 9001:2000, Quality management systems – Requirements.
ISO 00a:	ISO/IEC TR 15942:2000, Information technology—Programming languages—Guide for the use of the Ada programming language in high integrity systems.
ISO 03:	ISO 10007:2003, Quality management systems – Guidelines for configuration management.
ISO 03a:	ISO/IEC 14882:2003, Programming languages—C.
ISO 04a:	ISO 17000:2004, Conformity assessment—Vocabulary and general principles.
ISO 05:	ISO 9000:2005, Quality management systems – Fundamentals and vocabulary.
ISO 06:	ISO/IEC 23270:2006, Information technology—Programming languages—C#.
ISO 06e:	ISO/IEC 25062:2006 Common Industry Format (CIF) for Usability Test Reports.
ISO 94:	ISO 9706:1994, Information and documentation—Paper for documents—Requirements for permanence.
ISO 95:	ISO/IEC 8652:1995, Information technology—Programming languages—ADA.
ISO 98a:	ISO 9241-11:1998, Ergonomic requirements for office work with visual display terminals (VDTs) -- Part 11: Guidance on usability.
ISO 99:	ISO/IEC 9899:1999, Programming languages—C.
ITU-T X.509:	(2000)/ISO/IEC 9594-8 (2001): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework
Java 05:	The Java Language Specification, Third Edition, 2005. Available from http://java.sun.com/docs/books/jls/index.html.

LOTSE-V:	Legal, Operational and Technical Standards for E-Voting
MIL 83:	MIL-STD-810-D, Environmental Test Methods and Engineering Guidelines, 1983-7-19.
MIL 85:	MIL-STD-1521B (USAF) Technical Reviews and Audits for Systems, Equipments [sic], and Computer Software, rev. December 19, 1985.
MIL 96:	MIL-HDBK-781A, Handbook for Reliability Test Methods, Plans, and Environments for Engineering, Development, Qualification, and Production, April 1, 1996.
MIRA 04:	MISRA-C: 2004: Guidelines for the use of the C language in critical systems, MIRA Limited, U.K., November 2004.
Morris 84:	F. L. Morris and C. B. Jones, "An Early Program Proof by Alan Turing," IEEE Annals of the History of Computing, v. 6, n. 2, April 1984, pp. 139-143.
Moulding 89:	M. R. Moulding, "Designing for high integrity: the software fault tolerance approach," Section 3.4. In C. T. Sennett, ed., High-Integrity Software, Plenum Press, New York and London, 1989.
MS 05:	Request For Proposal #3443, Mississippi, April 28, 2005.
MS 05:	Paul Vick, The Microsoft® Visual Basic® Language Specification, Version 8.0, 2005. Available from Microsoft Download Center, http://go.microsoft.com/fwlink/?linkid=62990.
NGC 06:	Nevada Gaming Commission and State Gaming Control Board, Technical Standards for Gaming Devices and On-Line Slot Systems, March 2006. Available from http://gaming.nv.gov/stats_regs/reg14_tech_stnds.pdf.
NIST 02:	John P. Wack, Ken Cutler, Jamie Pole, National Institute of Standards and Technology Special Publication 800-41: Guidelines on Firewalls and Firewall Policy, January 2002. Available from http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf.
NIST 03:	Fred R. Byers, Care and Handling of CDs and DVDs—A Guide for Librarians and Archivists, National Institute of Standards and Technology Special Publication 500-252, 2003-10. Available from http://www.itl.nist.gov/div895/carefordisc/index.html.
NIST 05:	Recommended Security Controls for Federal Information Systems, National Institute of Standards and Technology Special Publication 800-53, 2005-02. Available from http://csrc.nist.gov/publications/nistpubs/.
NIST 05a:	Peter Mell, Karen Kent, Joseph Nusbaum, National Institute of Standards and Technology Special Publication 800-83: Guide to Malware Incident Prevention and Handling, November 2005. Available from http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf.
NIST 07:	Karen Scarfone, Peter Mell, National Institute of Standards and Technology Special Publication 800-94: Guide to Intrusion Detection and Prevention Systems, February 2007. Available from http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf.
NIST 75:	Saltman, Roy, National Institute of Standards Special Publication 500-30, Effective Use of Computing Technology in Vote-Tallying, 1975. Available from http://csrc.nist.gov/publications/nistpubs/NBS_SP_500-30.pdf.
ODBP CR:	ODBP Code Review
ODBP CRM:	ODBP Certification Matrix

ODBP DSF:	ODBP Description of System Features
ODBP P:	ODBP Plan
ODBP SPV:	ODBP System Performance Validation
ODBP SR:	ODBP System Requirements
ODBP SM:	ODBP Security Requirements Mapped to VVSG 2005
ODBP TR:	ODBP Test Report
OMG 07:	OMG Unified Modeling Language Superstructure Specification, version 2.1.1. Document formal/2007-02-05, Object Management Group, February 2007. Available from http://www.omg.org/cgi-bin/doc?formal/2007-02-05.
Oxford 93:	New Shorter Oxford English Dictionary, Clarendon Press, Oxford, 1993.
Pietrek 97:	Matt Pietrek, "A Crash Course on the Depths of Win32™ Structured Exception Handling," Microsoft Systems Journal, January 1997. Available from http://www.microsoft.com/msj/0197/exception/exception.aspx.
PKCS #1:	RSA Cryptography Standard
PKCS #5:	Password-based Encryption Standard
PKCS #7:	Cryptographic Message Syntax Standard
PKCS #8:	Private Key Information Syntax Standard
PKCS #10:	Certification Request Standard
PKCS #11:	Cryptographic Token Interface
PKCS #12:	Personal Information Exchange Syntax Standard
SCAM 01:	Joel Scambray, Stuart McClure, George Kurtz, Hacking Exposed: Network Security Secrets and Solutions, Second Edition, 2001.
SERVE DSF:	SERVE Description of System Features
SERVE EV:	SERVE Election Validation
SERVE R:	SERVE Requirements
SERVE SA:	SERVE Security Architecture
SERVE SACP:	SERVE System Accreditation and Certification Process
SERVE STC:	SERVE Security Test Conditions
SERVE TDP C:	SERVE TDP Checklist
SERVE TRA:	SERVE Threat Risk Assessment
SERVE VVP:	SERVE Vote Verification Process
SERVE WH:	SERVE White Hat
Sourceforge	CEXCEPT (exception handling in C), software package, 2000. Available from

00:	http://cexcept.sourceforge.net/.
SP 800-53:	Rev 2 Recommended Security Controls for Federal Information Systems
SP 800-63:	Electronic Authentication Guideline, April 2006. Available from: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf.
SP 800-113:	(2007): DRAFT Guide to SSL VPNs
TRIVS RN:	Testing Requirements for Internet Voting Systems Robert Naegele
UL 05:	UL 60950-1:2005, Information Technology Equipment – Safety – Part 1: General Requirements.
UL 437:	UL 437:2003, Standard for Key Locks. (2003).
UOCAVA PT:	UOCAVA Penetration Testing
UT 04:	Solicitation #DG5502, Utah, 2004-07-09. January 27, 2006.
VOI CAR:	VOI Certification and Accreditation Report
VOI COD:	VOI Concepts of Operations
VOI DSF:	VOI Description of System Features
VOI LEO M:	VOI LEO Manual
VOI LEO SSRS:	VOI LEO Server Software Requirement Spec
VOI PPR:	VOI Pilot Peer Review
VOI PSR:	VOI Pilot System Requirements
VOI Report:	VOI Test Report 2001
VOI SA:	VOI System Arch
VOI SD:	VOI System Design
VOI SP:	VOI Security Policy
VOI SRS:	VOI Software Requirement Spec
VOI STEP:	VOI System Test and Evaluation Plan
VOI STP:	VOI Software Test Plan
VOI TP:	VOI Test Procedures
VOI TR:	VOI Test Report 1999
VSS 2002:	2002 Voting Systems Standards. Available from http://www.eac.gov/program-areas/voting-systems/docs/voting-systems-standards-volume-i-performance.pdf/attachment_download/file
VVSG 2005:	2005 Voluntary Voting System Guidelines, Version 1.0, March 6, 2006. Available from http://www.eac.gov/program-areas/voting-

	systems/docs/vvsgvolumei.pdf/attachment_download/file
VVSG 2.0:	VVSG Recommendations to the EAC, TGDC, August 31, 2007.
RFI 2007-03:	EAC Decision on Request for Interpretation 2007-03, 2005 VVSG Vol. 1 Section 3.1.1, September 5, 2007. Available from http://www.eac.gov/program-areas/voting-systems/docs/certification-docs-eac-decision-on-request-for-interpretation-2007-03.pdf-1/attachment_download/file.
Wald 47:	Abraham Wald, Sequential Analysis, John Wiley & Sons, 1947.

Appendix C: Accuracy Test Case

Some voting system performance attributes are tested by inducing an event or series of events and the relative or absolute time intervals between repetitions of the event has no significance. Although equivalence between a number of events and a time period can be established when the operating scenarios of a system can be determined with precision, another type of test is required when such equivalence cannot be established. It uses event based failure frequencies to arrive at ACCEPT/REJECT criteria. This test may be performed simultaneously with time-based tests.

For example, the failure of a device is usually dependent on the processing volume that it is required to perform. The elapsed time over which a certain number of actuation cycles occur is, under most circumstances, not important. Another example of such an attribute is the frequency of errors in reading, recording, and processing vote data.

The error frequency, called “ballot position error rate,” applies to such functions as the process of detecting the presence or absence of a voting punch or mark, or to the closure of a switch corresponding to the selection of a candidate.

Certification and acceptance test procedures that accommodate event-based failures are, therefore, based on a discrete, rather than a continuous probability distribution. A Probability Ratio Sequential Test using the binomial distribution is recommended. In the case of ballot position error rate, the calculation for a specific device (and the processing function that relies on that device) is based on:

- HO: Desired error rate = 1 in 10,000,000
- H1: Maximum acceptable error rate = 1 in 500,000
- a = 0.05
- b = 0.05

The minimum error-free sample size to accept for qualification tests is 1,549,703 votes.

The nature of the problem may be illustrated by the following example, using the criteria contained in the VVSG 2005 for system error rate. A target for the desired accuracy is established at a very low error rate. A threshold for the worst error rate that can be accepted is then fixed at a somewhat higher error rate. Next, the decision risk is chosen, that is, the risk that the test results may not be a true indicator of either the system's acceptability or unacceptability. The process is as follows:

- The desired accuracy of the voting system, whatever its true error rate (which may be far better), is established as no more than one error in every ten million characters (including the null character).
- If it can be shown that the system's true error rate does not exceed one in every five hundred thousand votes counted, it will be considered acceptable. This is more than accurate enough to declare the winner correctly in almost every election.
- A decision risk of 5 percent is chosen, to be 95 percent certain that the test data will not indicate that the system is bad when it is good or good when it is bad.

This results in the following decision criteria:

a. If the system makes one error before counting 26,997 consecutive ballot positions correctly, it will be rejected. The vendor is then required to improve the system.

b. If the system reads at least 1,549,703 consecutive ballot positions correctly, it will be accepted.

c. If the system correctly reads more than 26,997 ballot positions but less than 1,549,703 when the first error occurs, the testing will have to be continued until another 1,576,701 consecutive ballot positions are counted without error (a total of 3,126,404 with one error).

Appendix C – VSTLs' Comments to the UPPTR

VSTL Comments to UPPTR Section 2 (Functional Requirements)

SLI's Comments to the UPPTR Section 2 (Functional Requirements)

Section	Requirements	SLI Comments
2.1 Accuracy		
2.1 Accuracy	The voting system SHALL achieve a target error rate of no more than one in 10,000,000 ballot positions, a maximum acceptable error rate in the test process of one in 500,000 ballot positions.	"Shall" should be removed from header
2.1.1 Components and Hardware		
2.1.1.1 Component accuracy	Memory hardware, such as semiconductor devices and magnetic storage media, SHALL be accurate.	1) Standards are recommended to specify appropriate component accuracy 2) This is better suited to Inspection, viewing the results overall of the testing, as well as review of hardware manufacturer specifications
2.1.1.2 Equipment design	The design of equipment in all voting systems SHALL provide for protection against mechanical, thermal, and electromagnetic stresses that impact voting system accuracy.	This should be Inspection / Review of hardware test reports and/or hardware specifications.
2.1.1.3 Voting system accuracy	To ensure vote accuracy, all voting systems SHALL:	
2.1.1.3 Voting system accuracy	a. Record the election contests, candidates, and issues exactly as defined by election officials;	
2.1.1.3 Voting system accuracy	b. Record the appropriate options for casting and recording votes;	
2.1.1.3 Voting system accuracy	c. Record each vote precisely as indicated by the voter and be able to produce an accurate report of all votes cast;	
2.1.1.3 Voting system accuracy	d. Include control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) to demonstrate that the voting system has been designed for accuracy;	1) Recommend this as Inspection. 2) Best suited for a source code review and environment specification, in particular for data at rest.
2.1.1.3 Voting system accuracy	e. Provide software that monitors the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected.	1) Recommend this as Inspection. As written, this requirement is only looking to verfiy that the monitoring software is provided. 2) Would recommend that the "...and how they were corrected." portion be broken out to another requirement, as this looks to be more of an event log.
2.1.2 Environmental Range	All voting systems SHALL meet the accuracy requirements over manufacturer specified operating conditions and after storage under non-operating conditions.	This should be Inspection / Review of hardware test reports and/or hardware specifications. As written this requirement seems to be written more for a traditional voting system than a UOCAVA internet based system.
2.1.3 Content of Data Verified for Accuracy		

VSTL Comments to UPPTR Section 5 (Security)

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.1 Access Control	This section states requirements for the identification of authorized system users, processes and devices and the authentication or verification of those identities as a prerequisite to granting access to system processes and data. It also includes requirements to limit and control access to critical system components to protect system and data integrity, availability, confidentiality, and accountability. This section applies to all entities attempting to physically enter voting system facilities or to request services or data from the voting system.	Manufacturer shall clearly define what level users, roles and groups are defined on, whether that be at the operating system or the voting system level	
5.1.1 Separation of Duties			
5.1.1.1 Definition of roles	The voting system SHALL allow the definition of personnel roles with segregated duties and responsibilities on critical processes to prevent a single person from compromising the integrity of the system.	Agree with Requirement	Specific roles should be defined to facilitate true segregation of duties.
5.1.1.2 Access to election data	The voting system SHALL ensure that only authorized roles, groups, or individuals have access to election data.	Agree with Requirement	No recommended change
5.1.1.3 Separation of duties	The voting system SHALL require at least two persons from a predefined group for validating the election configuration information, accessing the cast vote records, and starting the tabulation process.	Enumerate the activities	Current web based system do not do tabulation so this requirement was not applicable to our testing. The majority of election configuration is done independent of the Web application and is therefore not a critical function of our testing.
5.1.2 Voting System Access	The voting system SHALL provide access control mechanisms designed to permit authorized access and to prevent unauthorized access to the system.	SHALL should be removed, as it designates an actionable item. The header of a section is validated when all of its sub requirements are validated	This requirement does not define at what minimum level this security should be implemented.
5.1.2.1 Identity verification	The voting system SHALL identify and authenticate each person to whom access is granted, and the specific functions and data to which each person holds authorized access.	This requirement should be split out. It covers both authentication and authorization.	This requirement does not define at what minimum level this security should be implemented.
5.1.2.2 Access control configuration	The voting system SHALL allow the administrator group or role to configure permissions and functionality for each identity, group or role to include account and group/role creation, modification, and deletion.	Enumerate the activities	This requirement does not state whether this should be a system OS level or at a web based administration application level.

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.1 Access Control	This section states requirements for the identification of authorized system users, processes and devices and the authentication or verification of those identities as a prerequisite to granting access to system processes and data. It also includes requirements to limit and control access to critical system components to protect system and data integrity, availability, confidentiality, and accountability. This section applies to all entities attempting to physically enter voting system facilities or to request services or data from the voting system.	Manufacturer shall clearly define what level users, roles and groups are defined on, whether that be at the operating system or the voting system level	
5.1.1 Separation of Duties			
5.1.1.1 Definition of roles	The voting system SHALL allow the definition of personnel roles with segregated duties and responsibilities on critical processes to prevent a single person from compromising the integrity of the system.	Agree with Requirement	Specific roles should be defined to facilitate true segregation of duties.
5.1.1.2 Access to election data	The voting system SHALL ensure that only authorized roles, groups, or individuals have access to election data.	Agree with Requirement	No recommended change
5.1.1.3 Separation of duties	The voting system SHALL require at least two persons from a predefined group for validating the election configuration information, accessing the cast vote records, and starting the tabulation process.	Enumerate the activities	Current web based system do not do tabulation so this requirement was not applicable to our testing. The majority of election configuration is done independent of the Web application and is therefore not a critical function of our testing.
5.1.2 Voting System Access	The voting system SHALL provide access control mechanisms designed to permit authorized access and to prevent unauthorized access to the system.	SHALL should be removed, as it designates an actionable item. The header of a section is validated when all of its sub requirements are validated	This requirement does not define at what minimum level this security should be implemented.
5.1.2.1 Identity verification	The voting system SHALL identify and authenticate each person to whom access is granted, and the specific functions and data to which each person holds authorized access.	This requirement should be split out. It covers both authentication and authorization.	This requirement does not define at what minimum level this security should be implemented.
5.1.2.2 Access control configuration	The voting system SHALL allow the administrator group or role to configure permissions and functionality for each identity, group or role to include account and group/role creation, modification, and deletion.	Enumerate the activities	This requirement does not state whether this should be a system OS level or at a web based administration application level.

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.1.2.3 Default access control configuration	The voting system's default access control permissions SHALL implement the least privileged role or group needed.	Agree with Requirement	No recommended change
5.1.2.4 Escalation prevention	The voting system SHALL prevent a lower-privilege process from modifying a higher-privilege process.	Agree with Requirement	No recommended change
5.1.2.5 Operating system privileged account restriction	The voting system SHALL NOT require its execution as an operating system privileged account and SHALL NOT require the use of an operating system privileged account for its operation.	Should enumerate the activities	Wyle's testing was based on utilization of a web based application. Therefore this did not apply directly. But, it was noted that in some systems tested the OS administration privileges were required to configure election information.
5.1.2.6 Logging of account	The voting system SHALL log the identification of all personnel accessing or attempting to access the voting system to the system event log.	This is tested in 5.6.3.3	This requirement does not define what information should be logged. Some systems only log Administration functions while others only log Voter information.
5.1.2.7 Monitoring voting system access	The((voting system))SHALL provide tools ((or shall be provided)) for monitoring access to the system. These tools SHALL provide specific users real time display of persons accessing the system as well as reports from logs.	Should enumerate the activities. Concern for this requirement is if it is realistically feasible to monitor a globally distributed system, with potentially a very large set of users	This requirement does not define what information should be logged. This requirement also does not state if the tool is to be accessible via the Web based administration application or at an OS Level.
5.1.2.8 Login failures	The vote capture devices at the kiosk locations and the central server SHALL have the capability to restrict access to the voting system after a preset number of login failures.	1) SHALL should be removed, as it designates an actionable item. The header of a section is validated when all of its sub requirements are validated. 2) Enumerate activities 3) This requirement is too specific, should use the term "voting system" so that all areas are covered	This requirement does not define if this needs to be at a Web application level or at OS level. Reactivation of an account should not require utilization of anything but the Web based application.
5.1.2.8 Login failures	a. The lockout threshold SHALL be configurable by appropriate administrators/operators.	Agree with Requirement	not broken out
5.1.2.8 Login failures	b. The voting system SHALL log the event.	Covered in 5.6.3.3	not broken out
5.1.2.8 Login failures	c. The voting system SHALL immediately send a notification to appropriate administrators/operators of the event.	Agree with Requirement	not broken out

Section	Requirement	SLI Comments	Wyle Comments
5.1.2.8 Login failures	d. The voting system SHALL provide a mechanism for the appropriate administrators/operators to reactivate the account after appropriate confirmation.	Agree with Requirement	not broken out
5.1.2.9 Account lockout logging	The voting system SHALL log a notification when any account has been locked out.	Covered in 5.6.3.3	This requirement does not define what information should be logged.
5.1.2.10 Session time-out	Authenticated sessions on critical processes SHALL have an inactivity time-out control that will require personnel re-authentication when reached. This time-out SHALL be implemented for administration and monitor consoles on all voting system devices.	Enumerate activities	This requirement does not define how this function should be configured.
5.1.2.11 Screen lock	Authenticated sessions on critical processes SHALL have a screen-lock functionality that can be manually invoked	Should mention need for re-authentication in order to re-access	This requirement was deemed N/A due to the web based application being accessible from a privately controlled PC and not a public Voting site.
5.2 Identification and Authentication			
5.2.1 Authentication			
5.2.1.1 Strength of authentication	Authentication mechanisms supported by the voting system SHALL support authentication strength of at least 1/1,000,000.	This should be referring to appropriate NIST SP, NIST 800-63 Electronic Authentication Guideline Standards.	
5.2.1.2 Minimum authentication methods	The voting system SHALL authenticate users per the minimum authentication methods outlined below.		Since these systems do not tabulate and are not located in a polling location, the groups for Election Judge and Kiosk Worker do not really apply. (See Table 5-1 Roles : Section 5 | Page 59.)
5.2.1.2 Minimum authentication methods	Election Judge Two factor	Agree with Requirement	
5.2.1.2 Minimum authentication methods	Kiosk Worker One factor	Agree with Requirement	
5.2.1.2 Minimum authentication methods	Voter Not required	Assuming voter authentication is performed "outside" the scope of the voting system, by kiosk worker/Election Official	
5.2.1.2 Minimum authentication methods	Election Official Two factor	Agree with Requirement	
5.2.1.2 Minimum authentication methods	Administrator Two factor	Agree with Requirement	
5.2.1.2 Minimum authentication methods	Application or Process Digital signature 112 bits of security1	Agree with Requirement	
5.2.1.3 Multiple authentication mechanisms	The voting system SHALL provide multiple authentication methods to support multi-factor authentication.	Agree with Requirement	This requirement does not define what minimum level is required.

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.2.1.4 Secure storage of authentication data	When private or secret authentication data is stored by the voting system, it SHALL be protected to ensure that the confidentiality and integrity of the data are not violated.	Agree with Requirement	
5.2.1.5 Password reset	The voting system SHALL provide a mechanism to reset a password if it is forgotten, in accordance with the system access/security policy.	Covers passwords only. What if there are alternative methods of authentication?	This requirement does not define if this function is to be Web Based.
5.2.1.6 Password strength configuration	The voting system SHALL allow the administrator group or role to specify password strength for all accounts including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters per NIST 800-63 Electronic Authentication Guideline Standards.	Should specify the authentication level as defined in reference NIST SP	This requirement does not define if this configuration is to be Web Based or OS configurable.
5.2.1.7 Password history configuration	The voting system SHALL enforce password histories and allow the administrator to configure the history length when passwords are stored by the system. NIST Special Publication 800-57	Agree with Requirement	This requirement does not define if this configuration is to be Web Based or OS configurable.
5.2.1.8 Account information password restriction	The voting system SHALL ensure that the user name is not used in the password. Cannot be fully verified in lab; Testing at remote voting location(s) at operational level.	Agree with Requirement	
5.2.1.9 Automated password expiration	The voting system SHALL provide a means to automatically expire passwords.	Agree with Requirement	
5.2.1.10 Device authentication	The voting system servers and vote capture devices SHALL identify and authenticate one another using NIST - approved cryptographic authentication methods at the 112 bits of security.	Tested in 5.3.1.2	This requirement does not define which NIST standard or level to use.
5.2.1.11 Network authentication	Remote voting location site Virtual Private Network (VPN) connections (i.e., vote capture devices) to voting servers SHALL be authenticated using strong mutual cryptographic authentication at the 112 bits of security. Cannot be fully verified in lab; Testing at remote voting location(s) at operational level	Tested in 5.3.1.2	Wyle deems this requirement N/A due to the Web Based architecture. VPN systems will only be utilized at a system server level.
5.2.1.12 Message authentication	Message authentication SHALL be used for applications to protect the integrity of the message content using a schema with 112 bits of security.	1) need to define what is a "message" 2) Tested in 5.3.1.2	

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.2.1.13 Message authentication mechanisms	IPsec, SSL, or TLS and MAC mechanisms SHALL all be configured to be compliant with FIPS 140-2 using approved algorithm suites and protocols.	1) Is the intent here to use current certified communication methodologies? If so, would be better suited as an Inspection test method 2) Tested in 5.3.1.1 and 5.3.1.3 and 5.3.2.4	
5.3 Cryptography		1) SHALL should be removed, as it designates an actionable item. The header of a section is validated when all of its sub requirements are validated. 2) Note quantify "Strong Authentication", this term is too vague, should reference a standard	
5.3.1 General Cryptography Requirements		This section needs additional requirements that handle the situation of keys purchase from a Certificate Authority	
5.3.1.1 Cryptographic functionality	All cryptographic functionality SHALL be implemented using NIST-approved cryptographic algorithms/schemas, or use published and credible cryptographic algorithms/schemas/protocols	"… or use published and credible cryptographic algorithms/schemas/protocols " is something that should be qualified by FVAP/NIST. Preference is to not leave it to a VSTL to determine, or leave as a loophole for a manufacturer to argue.	This requirement does not define what minimum NIST level is required.
5.3.1.2 Required security strength	Cryptographic algorithms and schemas SHALL be implemented with a security strength equivalent to at least 112 bits of security to protect sensitive voting information and election records.	Agree with Requirement	
5.3.1.3 Use NIST-approved cryptography for communications	Cryptography used to protect information in-transit over public telecommunication networks SHALL use NIST-approved algorithms and cipher suites. In addition the implementations of these algorithms SHALL be NIST-approved (Cryptographic Algorithm Validation Program).	These requirements should be split out to discrete items	This requirement does not define which NIST standard or level to use.
5.3.2 Key Management	The following requirements apply to voting systems that generate cryptographic keys internally.		
5.3.2.1 Key generation methods	Cryptographic keys generated by the voting system SHALL use a NIST-approved key generation method, or a published and credible key generation method.	See comment on 5.3.1.1, as it is applicable here as well	This requirement does not define which NIST standard or level to use.

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.3.2.2 Security of key generation methods	Compromising the security of the key generation method (e.g., guessing the seed value to initialize the deterministic random number generator (RNG)) SHALL require as least as many operations as determining the value of the generated key.	Agree with Requirement	
5.3.2.3 Seed values	If a seed key is entered during the key generation process, entry of the key SHALL meet the key entry requirements in 5.3.3.1. If intermediate key generation values are output from the cryptographic module, the values SHALL be output either in encrypted form or under split knowledge procedures.	These requirements should be split out to discrete items	
5.3.2.4 Use NIST-approved key generation methods for communications	Cryptographic keys used to protect information in-transit over public telecommunication networks SHALL use NIST-approved key generation methods. If the approved key generation method requires input from a random number generator, then an approved (FIPS 140-2) random number generator SHALL be used.	1) These requirements should be split out to discrete items 2) Unless key is purchased from a Certificate Authority	This requirement does not define which NIST standard or level to use.
5.3.2.5 Random number generator health tests	Random number generators used to generate cryptographic keys SHALL implement one or more health tests that provide assurance that the random number generator continues to operate as intended (e.g., the entropy source is not stuck).	Agree with Requirement	
5.3.3 Key Establishment	Key establishment may be performed by automated methods (e.g., use of a public key algorithm), manual methods (use of a manually transported key loading device), or a combination of automated and manual methods.	Agree with Requirement	
5.3.3.1 Key entry and output	Secret and private keys established using automated methods SHALL be entered into and output from a voting system in encrypted form. Secret and private keys established using manual methods may be entered into or output from a system in plaintext form.	Agree with Requirement	
5.3.4 Key handling			
5.3.4.1 Key storage	Cryptographic keys stored within the voting system SHALL NOT be stored in plaintext. Keys stored outside the voting system SHALL be protected from disclosure or modification.	These requirements should be split out to discrete items	
5.3.4.2 Key zeroization	The voting system SHALL provide methods to zeroize all plaintext secret and private cryptographic keys within the system.	Agree with Requirement	

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.3.4.3 Support for rekeying	`	What is the acceptable level of effort to reset the cryptographic keys to new values? Is it acceptable to have to redefine the election? Or should the jurisdiction be able to just replace the keys?	
5.4 Voting System Integrity Management		This section has difficulty when applied to "ballot delivery" systems. Would work better to have 5.4.1 be specific to vote capture devices, then have a section 5.4.2 that pertains to vote capture devices and ballot delivery systems	
5.4.1 Protecting the Integrity of the Voting System		May need an additional requirement for nonrepudiation issues	
5.4.1.1 Cast vote integrity; transmission	The integrity and authenticity of each individual cast vote SHALL be protected from any tampering or modification during transmission.	Agree with Requirement	
5.4.1.2 Cast vote integrity; storage	The integrity and authenticity of each individual cast vote SHALL be preserved by means of a digital signature during storage.	Agree with Requirement	
5.4.1.3 Cast vote storage	Cast vote data SHALL NOT be permanently stored on the vote capture device	For the kiosk environment this works fine. If this is ever applied beyond section 1.1.3, to personal computers being used as the vote capture device, then there will be issues with regards to how the configuration is regulated.	
5.4.1.4 Electronic ballot box integrity	The integrity and authenticity of the electronic ballot box SHALL be protected by means of a digital signature.	Additional detailed definition of "electronic ballot box" is needed.	
5.4.1.5 Malware detection	The voting system SHALL use malware detection software to protect against known malware that targets the operating system, services, and applications	More definition is needed to quantify the level of protection needed. Potentially a hardware/software malware detection solution, instead of just software.	

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.4.1.6 Updating malware detection	The voting system SHALL provide a mechanism for updating malware detection signatures.	A follow on requirement to this one would be to have the manufacturer specify in their documentation (i.e. an Inspection test method) the recommend interval for requiring updated signatures	
5.4.1.7 Validating software on kiosk voting devices	The voting system SHALL provide the capability for kiosk workers to validate the software used on the vote capture devices as part of the daily initiation of kiosk operations.	This requirement needs to be expanded to cover all associated devices at the kiosk location. Some systems contain additional devices.	Wyle deems this requirement N/A due to the Web Based architecture.
5.5 Communications Security	This section provides requirements for communications security. These requirements address ensuring the integrity of transmitted information and protecting the voting system from external communications-based threats.	Some of the requirements in this section appear to explicitly call out specific communication protocols, which could be interpreted to exclude all other like communication protocols.	
5.5.1 Data Transmission Integrity			
5.5.1.1 Data integrity protection	Voting systems that transmit data over communications links SHALL provide integrity protection for data in transit through the generation of integrity data (digital signatures and/or message authentication codes) for outbound traffic and verification of the integrity data for inbound traffic.	Recommend that this requirement be broken out to handle outbound versus inbound separately	
5.5.1.2 TLS/SSL	Voting systems SHALL use at a minimum TLS 1.0, SSL 3.1 or equivalent protocols, including all updates to both protocols and implementations as of the date of the submission (e.g., RFC 5746 for TLS 1.0). verify all updates to both protocols and implementations as of the date of the submission (e.g., RFC 5746 for TLS 1.0).	Agree with Requirement	
5.5.1.3 Virtual private networks (VPN)	Voting systems deploying VPNs SHALL configure them to only allow FIPS-compliant cryptographic algorithms and cipher suites.	Tested in 5.3.1.1 and 5.3.1.3. As this appears to be a specific instance of the above mentioned requirements, would recommend removal in order to reduce redundancy.	Wyle deems this requirement N/A due to the Web Based architecture. VPN systems will only be utilized at a system server level.
5.5.1.4 Unique system identifier	Each communicating device SHALL have a unique system identifier	Agree with Requirement	
5.5.1.5 Mutual authentication required	Each device SHALL mutually strongly authenticate using the system identifier before additional network data packets are processed.	Recommend referencing appropriate NIST publication (SP 800-63) to more clearly define "mutually strongly authenticate"	

Section	Requirement	SLI Comments	Wyle Comments
5.5.1.6 Secrecy of ballot data	Data transmission SHALL preserve the secrecy of voters' ballot selections and SHALL prevent the violation of ballot secrecy and integrity.	1) This requirement should be split out 2) Recommend more clearly state that voter data is to be encrypted. "Preserve the secrecy …" creates ambiguity.	
5.5.2 External Threats	Voting systems SHALL implement protections against external threats to which the system may be susceptible.	"SHALL" should be removed from header	
5.5.2.1 Disabling network interfaces	Voting system components SHALL have the ability to enable or disable physical network interfaces.	Agree with Requirement	
5.5.2.2 Minimizing interfaces	The number of active ports and associated network services and protocols SHALL be restricted to the minimum required for the voting system to function.	Need to define test method "Inspection/Vulnerability"	
5.5.2.3 Prevention of attacks and security non-compliance	The voting system SHALL block all network connections that are not over a mutually authenticated channel.	Make this 5.5.2.4 need to define test method "Functional/Vulnerability"	
5.6 Logging			
5.6.1 Log Management			
5.6.1.1 Default settings	The voting system SHALL implement default settings for secure log management activities, including log generation, transmission, storage, analysis, and disposal.	1) This should be split to more discrete sub requirements 2) term "default settings" is ambiguous, should require "minimal settings" as per NIST SP 800-92	
5.6.1.2 Log access	Logs SHALL only be accessible to authorized roles	Term "authorized roles" is undefined within the requirements. This should be more clearly defined	
5.6.1.3 Log access	The voting system SHALL restrict log access to append-only for privileged logging processes and read-only for authorized roles.	Term "privileged logging processes" is undefined within the requirements. This should be more clearly defined	
5.6.1.4 Logging events	The voting system SHALL log logging failures, log clearing, and log rotation.	This should be split out to discrete 3 sub-requirements	This requirement does not specify if these logs should contain both voter and administration information.
5.6.1.5 Log format	The voting system SHALL store log data in a publicly documented format, such as XML, or include a utility to export log data into a publicly documented format.	Agree with Requirement	This requirement does not determine if these functions should be part of an administration web based application or at an OS level administration function.
5.6.1.6 Log separation	The voting system SHALL ensure that each jurisdiction's event logs and each component's logs are separable from each other.	This should be split out to discrete 2 sub-requirements	

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.6.1.7 Log review	The voting system SHALL include an application or program to view, analyze, and search event logs.	This should be split out to 3 discrete sub-requirements	This requirement does not determine if these functions should be part of an administration web based application or at an OS level administration function.
5.6.1.8 Log preservation	All logs SHALL be preserved in a useable manner prior to voting system decommissioning.	Term "prior to voting system decommissioning" is ambiguous. We believe the intent is that the log data remains intact for the life cycle of the given election data for a particular election. This may be defined at the jurisdictional level.	
5.6.1.9 Voter privacy	Logs SHALL NOT contain any data that could violate the privacy of the voter's identity.	Agree with Requirement	This requirement does not outline what information is deemed to violate a voter's identity. These systems utilize several voter specific credentials that are required for proper identification of voters.
5.6.1.10 Timekeeping format	Timekeeping mechanisms SHALL generate time and date values, including hours, minutes, and seconds	Agree with Requirement	
5.6.1.11 Timekeeping precision	The precision of the timekeeping mechanism SHALL be able to distinguish and properly order all log events.	Agree with Requirement	This requirement must meet 5.6.1.10
5.6.1.12 System clock security	Only the system administrator SHALL be permitted to set the system clock	Would recommend that the "system administrator" role be changed to indicate an appropriately authorized election official	Wyle determined that this requirement is N/A due to this function being a system administration function.
5.6.2 Communications Logging			
5.6.2.1 General	All communications actions SHALL be logged.	Agree with Requirement	This requirement does not define what all communications encompasses.
5.6.2.2 Log content	The communications log SHALL contain at least the following entries:	1) Enumerate, not using bullets, must be able to explicitly reference 2) Similar to 5.6.3.1, test method should be Inspection	
5.6.2.2 Log content	Times when the communications are activated and deactivated;	Agree with Requirement	
5.6.2.2 Log content	Services accessed;	Agree with Requirement	

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.6.2.2 Log content	Identification of the device which data was transmitted to or received from;	Agree with Requirement	
5.6.2.2 Log content	Identification of authorized entity; and	Agree with Requirement	
5.6.2.2 Log content	Successful and unsuccessful attempts to access communications or services.	Agree with Requirement	
5.6.3 System Event Logging	This section describes requirements for the voting system to perform event logging for system maintenance troubleshooting, recording the history of system activity, and detecting unauthorized or malicious activity. The operating system, and/or applications software may perform the actual event logging. There may be multiple logs in use for any system component.		
5.6.3.1 Event log format	The voting system SHALL log the following data for each event:	Agree with Requirement	
5.6.3.1 Event log format	a. System ID;	Agree with Requirement	
5.6.3.1 Event log format	b. Unique event ID and/or type;	Agree with Requirement	
5.6.3.1 Event log format	c. Timestamp;	Agree with Requirement	
5.6.3.1 Event log format	d. Success or failure of event, if applicable;	Agree with Requirement	
5.6.3.1 Event log format	e. User ID triggering the event, if applicable; and	Agree with Requirement	
5.6.3.1 Event log format	f. Jurisdiction, if applicable.	Agree with Requirement	
5.6.3.2 Critical events	All critical events SHALL be recorded in the system event log.	Define a critical event. The requirement as it is now leaves room for interpretation in regards to the scope of the requirement	This requirement does not define what a critical event might be.
5.6.3.3 System events	At a minimum the voting system SHALL log the events described in Table 5-2. (The contents of the table appear in this list under the 5.6.3.3 heading)	This section would be better served to be broken out into subparagraphs. Referencing back to a row, or a bullet in a cell is many times problematic Additionally the requirement only states "voting system" this is a broad scope of equipment and software. Does this apply to the O/S, The voting system application, or both? General Comment for this table would be to recommend that the term "include but not limited to" be avoided, as this term creates ambiguity and potential for inconsistent interpretation of the requirement	Wyle was unable to completely validate this requirement due to limited access to physical hardware. The majority of the events defined are from a server OS level and not a web based application level.

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.6.3.3.a1 Error and exception messages	The source and disposition of system interrupts resulting in entry into exception handling routines.	System interrupts at an operating system / hardware level could be potentially destructive. Source code can be analyzed for an understanding of exception handling routines then a script can be written to invoke a system interrupts that would result in an entry into exception handling routines.	
5.6.3.3.a2	Messages generated by exception handlers.	Agree with Requirement	
5.6.3.3.a3	The identification code and number of occurrences for each hardware and software error or failure.	Agree with Requirement	
5.6.3.3.a4	Notification of physical violations of security.	the term "physical violations of security" needs to be better defined as to what is included. I.e. computer room security, motion sensors, chassis alarms, etc.	
5.6.3.3.a5	Other exception events such as power failures, failure of critical hardware components, data transmission errors or other types of operating anomalies.	Agree with Requirement	
5.6.3.3.a6	All faults and the recovery actions taken.	the term "fault" is ambiguous, needs to be more clearly defined.	
5.6.3.3.a7	Error and exception messages such as ordinary timer system interrupts and normal I/O system interrupts do not need to be logged.	define "ordinary", and seems to be in conflict with bullet 2	
5.6.3.3.b	Critical system status messages	1) More detail/criteria is needed to define what is considered critical. "includes but not limited to" creates a large potential for gaps to occur, as well as disagreements by a manufacturer as to what is deemed critical.	
5.6.3.3.b1	Critical system status messages other than information messages displayed by the device during the course of normal operations. Includes but not limited to: Diagnostic and status messages upon startup.	Agree with Requirement Though Diagnostics and status messages upon startup do not seem to be critical type message	
5.6.3.3.b2	The “zero totals” check conducted before starting the voting period.	Agree with Requirement	

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.6.3.3.c Non-critical status messages	Non-critical status messages Non-critical status messages that are generated by the data quality monitor or by software and hardware condition monitors.	1) need better criteria for determining what is non-critical versus what is critical status messages. 2) need clarification as to what is meant by "data quality monitor". This term seems to be very subjective and open to interpretation. Likely to cause significant disagreement as to what is	
5.6.3.3.d Events that require election official intervention	Events that require election official intervention Events that require election official intervention, so that each election official access can be monitored and access sequence can be constructed.	Agree with Requirement	
5.6.3.3.e shutdown and restarts	Shutdown and restarts Both normal and abnormal shutdowns and restarts.	Recommend adding "Power up" to this line item	
5.6.3.3.f Changes to system configuration settings	Changes to system configuration settings Configuration settings include but are not limited to registry keys, kernel settings, logging settings, and other system configuration settings.	Recommend additional specificity , rather than alluding to "other system configuration settings"	
5.6.3.3.g Integrity checks for executables, configuration files, data and logs	Integrity checks for executables, configuration files, data, and logs Integrity checks that may indicate possible tampering with files and data.	Should explicitly call out "logs" in description	
5.6.3.3.h The addition and deletion of files	The addition and deletion of files Files added or deleted from the system.	Recommend additional detail as to file types. Would not recommend having to track temporary files that are automatically handled within the system	
5.6.3.3.i1 System readiness results	System readiness results Includes but not limited to: System pass or fail of hardware and software test for system readiness.	Agree with Requirement	
5.6.3.3.i2	Identification of the software release, identification of the election to be processed, kiosk locations, and the results of the software and hardware diagnostic tests.	Agree with Requirement	
5.6.3.3.13	Pass or fail of ballot style compatibility and integrity test.	Agree with Requirement	
5.6.3.3.i4	Pass or fail of system test data removal.	Agree with Requirement	
5.6.3.3.j Removable media events	Removable media events Removable media that is inserted into or removed from the system.	Agree with Requirement	

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.6.3.3.k Backup and restore	Backup and restore Successful and failed attempts to perform backups and restores.	Agree with Requirement	
5.6.3.3.l1 Authentication related events	Authentication related events Includes but not limited to: Login/logoff events (both successful and failed attempts).	Agree with Requirement	
5.6.3.3.l2	Account lockout events.	Agree with Requirement	
5.6.3.3.l3	Password changes.	Agree with Requirement	
5.6.3.3.m1 Access control related events	Access control related events Includes but not limited to: Use of privileges.	Agree with Requirement	
5.6.3.3.m2	Attempts to exceed privileges.	Agree with Requirement	
5.6.3.3.m3	All access attempts to application and underlying system resources.	Recommend removal of "…and underlying system resources", as this is beyond the scope of the voting system applications logging scope.	
5.6.3.3.m4	Changes to the access control configuration of the system.	Agree with Requirement	
5.6.3.3.n1 User account and role (or groups) management activity	User account and role (or groups) management activity Includes but not limited to: Addition and deletion of user accounts and roles.	Agree with Requirement	
5.6.3.3.n2	User account and role suspension and reactivation.	Agree with Requirement	
5.6.3.3.n3	Changes to account or role security attributes such as password length, access levels, login restrictions, permissions.	Agree with Requirement	
5.6.3.3.n4	Administrator account and role password resets.	Agree with Requirement	
5.6.3.3.o Installation, upgrading, patching, or modification of software or firmware	Installation, upgrading, patching, or modification of software or firmware Logging for installation, upgrading, patching, or modification of software or firmware include logging what was installed, upgraded, or modified as well as a cryptographic hash or other secure identifier of the old and new versions of the data.	1) This line item needs to be explicitly broken out to individual requirements. The potential scope is very large. In an initial certification, upgrading/patching/modification may well not be available. 2) "Cryptographic hash" needs to be defined. Would recommend using "hash code" instead.	

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.6.3.3.p1 Changes to configuration settings	Changes to configuration settings Includes but not limited to: Changes to critical function settings. At a minimum critical function settings include location of ballot definition file, contents of the ballot definition file, vote reporting, location of logs, and system configuration settings.	This requirement should be split out to more explicitly address either voting system applications or the underlying operating system	
5.6.3.3.p2	Changes to settings including but not limited to enabling and disabling services.	This requirement should be split out to more explicitly address either voting system applications or the underlying operating system.	
5.6.3.3.p3	Starting and stopping processes.	This requirement should be split out to more explicitly address either voting system applications or the underlying operating system	
5.6.3.3.q Abnormal process exits	Abnormal process exits All abnormal process exits.	Agree with Requirement	
5.6.3.3.r Successful and failed database connection attempts (if a database is utilized)	Successful and failed database connection attempts (if a database is utilized). All database connection attempts.	Agree with Requirement	
5.6.3.3.s Changes to cryptographic keys	Changes to cryptographic keys At a minimum critical cryptographic settings include key addition, key removal, and re-keying.	Recommend adding "key zeroization"	
5.6.3.3.t1 Voting events	Voting events Includes: Opening and closing the voting period.	Recommend including successful delivery of appropriate ballot style to voter Agree with Requirement	
5.6.3.3.t2	Casting a vote.	Agree with Requirement	
5.6.3.3.t3	Success or failure of log and election results exportation.	Agree with Requirement	
5.7 Incident Response			
5.7.1 Incident Response Support			

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.7.1.1 Critical events	Manufacturers SHALL document what types of system operations or security events (e.g., failure of critical component, detection of malicious code, unauthorized access to restricted data) are classified as critical.	1) Recommend that NIST/FVAP list minimum criteria of what should be classified as critical, in order to create a consistency for this requirement 2) Recommend removal of "e.g." and giving specific criteria that must be met, as in 1) above	Wyle determined that this requirement is not applicable to a web based application. But it is a requirement for a web server and therefore could not be tested at this time.
5.7.1.2 Critical event alarm	An alarm that notifies appropriate personnel SHALL be generated on the vote capture device, system server, or tabulation device, depending upon which device has the error, if a critical event is detected.	Agree with Requirement	Wyle determined that this requirement is not applicable to a web based application. A system server notification should be sent to administrators when issues arise with the web server.
5.8 Physical and Environmental Security		Recommend that additional specificity is added to explicitly call out whether each requirement is for the voting system (election creation machines and accumulation/tallying central servers included), or just the vote capture device	
5.8.1 Physical Access			
5.8.1.1 Unauthorized physical access requirement	Any unauthorized physical access SHALL leave physical evidence that an unauthorized event has taken place.	Agree with Requirement	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.
5.8.2 Physical Ports and Access Points			
5.8.2.1 Non-essential ports	The voting system SHALL disable physical ports and access points that are not essential to voting operations, testing, and auditing.	Recommend that "testing" be removed. In a production environment, would not want "test" ports/access points enabled.	
5.8.3 Physical Port Protection			
5.8.3.1 Physical port shutdown requirement	If a physical connection between the vote capture device and a component is broken, the affected vote capture device port SHALL be automatically disabled	Recommend changing Test Method to Functional	Wyle determined that this requirement is not applicable to a web based application. A physical connection will only be made during a single instance of vote casting.

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.8.3.2 Physical component alarm requirement	The voting system SHALL produce a visual alarm if a connected component is physically disconnected.	Recommend changing Test Method to Functional	Wyle determined that this requirement is not applicable to a web based application.
5.8.3.3 Physical component event log requirement	An event log entry that identifies the name of the affected device SHALL be generated if a vote capture device component is disconnected.	Agree with Requirement	Wyle determined that this requirement is not applicable to a web based application.
5.8.3.4 Physical port enablement requirement	Disabled ports SHALL only be re-enabled by authorized administrators.	Recommend changing Test Method to Functional	
5.8.3.5 Physical port restriction requirement	Vote capture devices SHALL be designed with the capability to restrict physical access to voting device ports that accommodate removable media with the exception of ports used to activate a voting session.	If implementing with custom designed vote capture device this requirement is applicable. If implementing with COTS products, this would not be applicable.	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.
5.8.3.6 Physical port tamper evidence requirement	Vote capture devices SHALL be designed to give a physical indication of tampering or unauthorized access to ports and all other access points, if used as described in the manufacturer's documentation.	If implementing with custom designed vote capture device this requirement is applicable. If implementing with COTS products, this would not be applicable.	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.
5.8.3.7 Physical port disability capability requirement	Vote capture devices SHALL be designed such that physical ports can be manually disabled by an authorized administrator.	If implementing with custom designed vote capture device this requirement is applicable. If implementing with COTS products, this would not be applicable.	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.
5.8.4 Door Cover and Panel Security			
5.8.4.1 Access point security requirement	Access points such as covers and panels SHALL be secured by locks or tamper evident or tamper resistant countermeasures and SHALL be implemented so that kiosk workers can monitor access to vote capture device components through these points.	Enumerate the activities	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.
5.8.5 Secure Paper Record Receptacle			
5.8.5.1 Secure paper record container requirement		Agree with Requirement	Wyle determined that this requirement is not applicable to a web based application
5.8.6 Secure Physical Lock and Key			
5.8.6.1	Voting equipment SHALL be designed with countermeasures that provide physical indication that unauthorized attempts have been made to access locks installed for security purposes.	If implementing with custom designed vote capture device this requirement is applicable. If implementing with COTS products, this would not be applicable.	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.8.6.2	Manufacturers SHALL provide locking systems for securing vote capture devices that can make use of keys that are unique to each owner.	Agree with Requirement	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.
5.8.7 Media Protection	These requirements apply to all media, both paper and digital, that contain personal privacy related data or other protected or sensitive types of information.	Recommend changing "person privacy related data" to "personally identifiable information (PII)", which is a common industry term	
5.8.7.1 Kiosk site protection	The voting system SHALL meet the following requirements: a. All paper records (including rejected ones) printed at the kiosk locations SHALL be deposited in a secure container; b. Vote capture device hardware, software and sensitive information (e.g., electoral roll) SHALL be physically protected to prevent unauthorized modification or disclosure; and c. Vote capture device hardware components, peripherals and removable media SHALL be identified and registered by means of a unique serial number or other identifier.	Agree with Requirement	Wyle determined that this requirement is not applicable to a web based application.
5.9 Penetration Resistance		Recommend referencing NIST SP dealing with hardening.	
5.9.1 Resistance to Penetration Attempts			
5.9.1.1 Resistant to attempts	The voting system SHALL be resistant to attempts to penetrate the system by any remote unauthorized entity.	Recommend defining resistant levels more definitively, and enumerating by device types within a voting system	
5.9.1.2 System information disclosure	The voting system SHALL be configured to minimize ports, responses and information disclosure about the system while still providing appropriate functionality	1) Recommend defining "appropriate functionality" by device types within a voting system. 2) Recommend referencing NIST SP dealing with hardening.	
5.9.1.3 System access	The voting system SHALL provide no access, information or services to unauthorized entities.	Enumerate the activities	
5.9.1.4 Interfaces	All interfaces SHALL be penetration resistant including TCP/IP, wireless, and modems from any point in the system.	Recommend closing all ports and shutting down all services not needed to perform voting activities	

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	Requirement	SLI Comments	Wyle Comments
5.9.1.5 Documentation	The configuration and setup to attain penetration resistance SHALL be clearly and completely documented.	Agree with Requirement	Based on the system documentation provided by the participants in this test campaign, Wyle was unable to validate this requirement. However, Wyle deems it necessary for future testing.
5.9.2 Penetration Resistance Test and Evaluation		This section is oriented to the VSTL. As such it should not be in the requirements document that manufacturer's are held to, but in a "Program Manual" that outlines the scope of a certification campaign	
5.9.2.1 Scope	The scope of penetration testing SHALL include all the voting system components. The scope of penetration testing includes but is not limited to the following:	Define Test Method "Penetration" versus "Functional"	
5.9.2.1 Scope	System server;	Agree with Requirement	
5.9.2.1 Scope	Vote capture devices;	Agree with Requirement	
5.9.2.1 Scope	Tabulation device;	Agree with Requirement	
5.9.2.1 Scope	All items setup and configured per Technical Data Package (TDP) recommendations;	Agree with Requirement	
5.9.2.1 Scope	Local wired and wireless networks; and	Agree with Requirement	
5.9.2.1 Scope	Internet connections.	Agree with Requirement	
5.9.2.2 Test environment	Penetration testing SHALL be conducted on a voting system set up in a controlled lab environment. Setup and configuration SHALL be conducted in accordance with the TDP, and SHALL replicate the real world environment in which the voting system will be used.	1) This requirement appears to be oriented to the VSTL, not the manufacturer. 2) This may not be feasible for all systems. Have encountered systems that are cloud base, for example.	Wyle was unable to validate this requirement, but deems it necessary for future testing.
5.9.2.3 White box testing	The penetration testing team SHALL conduct white box testing using manufacturer supplied documentation and voting system architecture information. Documentation includes the TDP and user documentation. The testing team SHALL have access to any relevant information regarding the voting system configuration. This includes, but is not limited to, network layout and Internet Protocol addresses for system devices and components. The testing team SHALL be provided any source code included in the TDP.	1) This requirement appears to be oriented to the VSTL, not the manufacturer. 2) The original text is not a definition of white box testing. 3) With added text, the source code review that would be required would be prohibitive from a cost/benefit viewpoint.	Wyle was unable to validate this requirement, but deems it necessary for future testing.
5.9.2.4 Focus and priorities	Penetration testing seeks out vulnerabilities in the voting system that might be used to change the outcome of an election, interfere with voter ability to cast ballots, ballot counting, or compromise ballot secrecy. The penetration testing team SHALL prioritize testing efforts based on the following:	1) This requirement appears to be oriented to the VSTL, not the manufacturer.	

VSTLs' Comments to the UPPTR Section 5 (Security)

Section	*Requirement*	*SLI Comments*	*Wyle Comments*
5.9.2.4 Focus and priorities	a. Threat scenarios for the voting system under investigation;		
5.9.2.4 Focus and priorities	b. Remote attacks SHALL be prioritized over in-person attacks;		
5.9.2.4 Focus and priorities	c. Attacks with a large impact SHALL be prioritized over attacks with a more narrow impact; and		
5.9.2.4 Focus and priorities	d. Attacks that can change the outcome of an election SHALL be prioritized over attacks that compromise ballot secrecy or cause non-selective denial of service.		

SLI's Comments to the UPPTR Section 2 (Functional Requirements)

Section	*Requirements*	*SLI Comments*
2.1 Accuracy		
2.1 Accuracy	The voting system SHALL achieve a target error rate of no more than one in 10,000,000 ballot positions, a maximum acceptable error rate in the test process of one in 500,000 ballot positions.	"Shall" should be removed from header
2.1.1 Components and Hardware		
2.1.1.1 Component accuracy	Memory hardware, such as semiconductor devices and magnetic storage media, SHALL be accurate.	1) Standards are recommended to specify appropriate component accuracy 2) This is better suited to Inspection, viewing the results overall of the testing, as well as review of hardware manufacturer specifications
2.1.1.2 Equipment design	The design of equipment in all voting systems SHALL provide for protection against mechanical, thermal, and electromagnetic stresses that impact voting system accuracy.	This should be Inspection / Review of hardware test reports and/or hardware specifications.
2.1.1.3 Voting system accuracy	To ensure vote accuracy, all voting systems SHALL:	
2.1.1.3 Voting system accuracy	a. Record the election contests, candidates, and issues exactly as defined by election officials;	
2.1.1.3 Voting system accuracy	b. Record the appropriate options for casting and recording votes;	
2.1.1.3 Voting system accuracy	c. Record each vote precisely as indicated by the voter and be able to produce an accurate report of all votes cast;	
2.1.1.3 Voting system accuracy	d. Include control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) to demonstrate that the voting system has been designed for accuracy;	1) Recommend this as Inspection. 2) Best suited for a source code review and environment specification, in particular for data at rest.
2.1.1.3 Voting system accuracy	e. Provide software that monitors the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected.	1) Recommend this as Inspection. As written, this requirement is only looking to verfiy that the monitoring software is provided. 2) Would recommend that the "…and how they were corrected." portion be broken out to another requirement, as this looks to be more of an event log.
2.1.2 Environmental Range	All voting systems SHALL meet the accuracy requirements over manufacturer specified operating conditions and after storage under non-operating conditions.	This should be Inspection / Review of hardware test reports and/or hardware specifications. As written this requirement seems to be written more for a traditional voting system than a UOCAVA internet based system.
2.1.3 Content of Data Verified for Accuracy		

SLI's Comments to the UPPTR Section 2 (Functional Requirements)

Section	*Requirements*	*SLI Comments*
2.1.3.1 Election management system accuracy	Voting systems SHALL accurately record all election management data entered by the user, including election officials or their designees.	As written, this requirement contains a high degree of vagueness. Each type of Election Management data should be enumerated.
2.1.3.2 Recording accuracy	For recording accuracy, all voting systems SHALL:	
2.1.3.2 Recording accuracy	a. Record every entry made by the user except where it violates voter privacy;	
2.1.3.2 Recording accuracy	b. Accurately interpret voter selection(s) and record them correctly to memory;	Recommend that the "… to memory" portion be removed. Is potentially too specific of a data recording method.
2.1.3.2 Recording accuracy	c. Verify the correctness of detection of the user selections and the addition of the selections correctly to memory;	It is not clear how this requirement is examining anything different from part b.
2.1.3.2 Recording accuracy	d. Verify the correctness of detection of data entered directly by the user and the addition of the selections correctly to memory; and	Our assumption here is that this requirement is testing write-ins as opposed to selecting choices, as in b and c. This requirement (b,c, and d) need to be clarified as to their specific intents, with any redundancies removed.
2.1.3.2 Recording accuracy	e. Preserve the integrity of election management data stored in memory against corruption by stray electromagnetic emissions, and internally generated spurious electrical signals.	2.1.3.2.e would be coverd under EMC testing. This should be Inspection / Review of hardware test reports and/or hardware specifications.
2.1.4 Telecommunications Accuracy	The telecommunications components of all voting systems SHALL achieve a target error rate of no more than one in 10,000,000 ballot positions, with a maximum acceptable error rate in the test process of one in 500,000 ballot positions.	For telecommunications, if TCP/IP protocols are used all transmissions are guaranteed to be accurate. The discussion of one in ten million and one in half a milion is somewhat obfuscated, the requirement should be more clearly defined stated.

Section	*Requirements*	*SLI Comments*
2.1.5 Accuracy Test Content	Voting system accuracy SHALL be verified by a specific test conducted for this objective. The overall test approach is described in Appendix C.	For a true internet voting system, that uses a web browser implementation for capturing votes, the accuracy test is whether or not the election is coded correctly. The technologies involved are mature, proven and robust. For a true internet voting system that employs physical devices such as a touch screen, the accuracy test would be similar to that of a ballot delivery system, in that the touch screen is dependent on the prescribed maintenance cycle of the device. For a ballot delivery system, where the cast ballot is potentially returned in any of a number or ways (fax, email, printed/scanned), the accuracy is dependent on the device used, within the confines of the prescribed maintenance cycles of the device.
2.1.5.1 Simulators	If a simulator is used, it SHALL be verified independently of the voting system in order to produce ballots as specified for the accuracy testing.	Not a voting system requirement
2.1.5.2 Ballots	Ballots used for accuracy testing SHALL include all the supported types (i.e., rotation, alternative languages) of contests and election types (primary, general).	Question as to the applicability of the ballot type to accuracy testing. Accuracy testing concerns itself with accuracy with regard to the scanning/reading of each possible ballot position on a given size ballot. The ability of the system to correctly handle the various supported voting variations is addressed in other specific tests.
2.1.6 Reporting Accuracy	Processing accuracy is defined as the ability of the voting system to process stored voting data. Processing includes all operations to consolidate voting data after the voting period has ended. The voting systems SHALL produce reports that are consistent, with no discrepancy among reports of voting data.	In general this is a bit high level, would like to see some specific metrics called out to ensure reporting accuracy. Similar v1.0 VVSG volume 1, sections 2.4.2. and 2.4.3
2.2 Operating capacities		

Section	Requirements	SLI Comments
2.2.1 Maximum Capacities	The manufacturer SHALL specify at least the following maximum operating capacities for the voting system (i.e. server, vote capture device, tabulation device, and communications links): - Throughput, - Memory, - Transaction processing speed, and - Election constraints: o Number of jurisdictions o Number of ballot styles per jurisdiction o Number of contests per ballot style o Number of candidates per contest o Number of voted ballots	Recommend that this section look at capacities more in terms of minimums that need to be met (as specified by NIST/FVAP), rather than as stated maximum capacities that a manufacturer claims they can accommodate. Many times a manufacturer will list an unrealistically high number for many of these categories. A minimum standard will create a consistent baseline for all manufacturers.
2.2.1.1 Capacity testing	The voting system SHALL achieve the maximum operating capacities stated by the manufacturer in section 2.2.1.	Recommend making the Test Method for this item Inspection/Functional. Some instances can be impractical to functionally validate within a reasonable cost/benefit ratio.
2.2.2 Operating Capacity notification	The voting system SHALL provide notice when any operating capacity is approaching its limit.	Recommend making the Test Method for this item Inspection/Functional. Some instances can be impractical to functionally validate within a reasonable cost/benefit ratio.
2.2.3 Simultaneous Transmissions	The voting system SHALL protect against the loss of votes due to simultaneous transmissions.	Recommend making the Test Method for this item Inspection/Functional. Some instances can be impractical to functionally validate within a reasonable cost/benefit ratio.
2.3 Pre-Voting Capabilities		
2.3.1 Import and Verify Election Definition		
2.3.1.1 Import the election definition	The voting system SHALL:	
2.3.1.1 Import the election definition	a. Keep all data logically separated by, and accessible only to, the appropriate state and local jurisdictions;	Agree with Requirement
2.3.1.1 Import the election definition	b. Provide the capability to import or manually enter ballot content, ballot instructions and election rules, including all required alternative language translations from each jurisdiction;	Enumerate the activities
2.3.1.1 Import the election definition	c. Provide the capability for the each jurisdiction to verify that their election definition was imported accurately and completely;	Agree with Requirement
2.3.1.1 Import the election definition	d. Support image files (e.g., jpg or gif) andor a handwritten signature image on the ballot so that state seals, official signatures and other graphical ballot elements may be properly displayed; and	Agree with Requirement

Section	Requirements	SLI Comments
2.3.1.1 Import the election definition	e. Support multiple ballot styles per each local jurisdiction.	Agree with Requirement
2.3.1.2 Protect the election definition	The voting system SHALL provide a method to protect the election definition from unauthorized modification.	Agree with Requirement
2.3.2 Readiness Testing		
2.3.2.1 Voting system test mode	The voting system SHALL provide a test mode to verify that the voting system is correctly installed, properly configured, and all functions are operating to support pre-election readiness testing for each jurisdiction.	Agree with Requirement
2.3.2.2 Test data segregation	The voting system SHALL provide the capability to zero-out or otherwise segregate test data from actual voting data.	Agree with Requirement
2.4 Voting Capabilities		
2.4.1 Opening the Voting Period		
2.4.1.1 Accessing the ballot	The voting system SHALL:	
2.4.1.1 Accessing the ballot	a. Present the correct ballot style to each voter;	Agree with Requirement
2.4.1.1 Accessing the ballot	b. Allow the voting session to be canceled; and	Agree with Requirement
2.4.1.1 Accessing the ballot	c. Prevent a voter from casting more than one ballot in the same election.	Agree with Requirement
2.4.2 Casting a Ballot	The voting system SHALL:	There should be a sub-requirement that deals with the system allowing the voter to change their selection within a contest prior to casting their ballot (similar to (g) for undervotes)
2.4.2.1 Record voter selections	a. Record the selection and non-selection of individual vote choices;	Agree with Requirement
2.4.2.1 Record voter selections	b. Record the voter's selection of candidates whose names do not appear on the ballot, if permitted under state law, and record as many write-ins as the number of candidates the voter is allowed to select;	Recommend splitting sub-requirement so that one validates the ability to enter a write in, and the other verifies that the correct number of write-ins is allowed
2.4.2.1 Record voter selections	c. Prohibit the voter from accessing or viewing any information on the display screen that has not been authorized and preprogrammed into the voting system (i.e., no potential for display of external information or linking to other information sources);	Agree with Requirement
2.4.2.1 Record voter selections	d. Allow the voter to change a vote within a contest before advancing to the next contest;	Agree with Requirement

Section	*Requirements*	*SLI Comments*
2.4.2.1 Record voter selections	e. Provide unambiguous feedback regarding the voter's selection, such as displaying a checkmark beside the selected option or conspicuously changing its appearance;	Agree with Requirement
2.4.2.1 Record voter selections	f. Indicate to the voter when no selection, or an insufficient number of selections, has been made for a contest (e.g., undervotes);	Recommend that this requirement is made more specific as to notifying voter of potential undervote prior to casting of ballot (as opposed to when going from one contest (or screen) to another).
2.4.2.1 Record voter selections	g. Provide the voter the opportunity to correct the ballot for an undervote before the ballot is cast;	Agree with Requirement
2.4.2.1 Record voter selections	h. Allow the voter, at the voter's choice, to submit an undervoted ballot without correction.	Agree with Requirement
2.4.2.1 Record voter selections	i. Prevent the voter from making more than the allowable number of selections for any contest (e.g., overvotes); and	Agree with Requirement
2.4.2.1 Record voter selections	j. In the event of a failure of the main power supply external to the voting system, provide the capability for any voter who is voting at the time to complete casting a ballot, allow for the successful shutdown of the voting system without loss or degradation of the voting and audit data, and allow voters to resume voting once the voting system has reverted to back-up power.	This may not be feasible in a remote session environment. Depending on where the power failure occurs, as well as the duration, will dictate if a ballot can be recorded within the voting system without loss or degradation of voting/audit data. The "… allow voters to resume voting..." clause would inherently cause some kind of voter data to be resident on the vote capture device, which would potentially violate other Security requirements (5.4.1.3)
2.4.2.2 Verify voter selections	The voting system SHALL:	
2.4.2.2 Verify voter selections	a. Produce a paper record each time the confirmation screen is displayed;	Would recommend that a paper record is generated only when the ballot is cast and not each time the confirmation screen is accessed.
2.4.2.2 Verify voter selections	b. Generate a paper record identifier. This SHALL be a random identifier that uniquely links the paper record with the cast vote record;	Agree with Requirement
2.4.2.2 Verify voter selections	c. Allow the voter to either cast the ballot or return to the vote selection process to make changes after reviewing the confirmation screen and paper record; and	Recommend removing "… and paper record", see comment to "a" above.

Section	Requirements	SLI Comments
2.4.2.2 Verify voter selections	d. Prompt the voter to confirm his choices before casting the ballot, signifying to the voter that casting the ballot is irrevocable and directing the voter to confirm his intention to cast the ballot.	Agree with Requirement
2.4.2.3 Cast ballot	The voting system SHALL:	Recommend renaming requirement to "Post Cast Ballot Process"
2.4.2.3 Cast ballot	a. Store all cast ballots in a random order; logically separated by, and only accessible to, the appropriate state local jurisdictions;	Agree with Requirement
2.4.2.3 Cast ballot	b. Notify the voter after the vote has been stored persistently that the ballot has been cast;	Recommend defining "persistently" to more detail. In a full electronic system, "persistently" would indicate that the central server has received the vote record and stored it. In a ballot delivery system, "persistently" would indicate the printing of a physical ballot, or creation of a pdf.
2.4.2.3 Cast ballot	c. Notify the voter that the ballot has not been cast successfully if it is not stored successfully, and provide clear instruction as to steps the voter should take to cast his ballot should this event occur; and	Recommend enumerating this requirement to c.i and c.ii
2.4.2.3 Cast ballot	d. Prohibit access to voted ballots until such time as state law allows for processing of absentee ballots.	Agree with Requirement
2.4.2.4 Ballot linking to voter identification		
2.4.2.4.1 Absentee model	The cast ballot SHALL be linked to the voter's identity without violating the privacy of the voter.	Agree with Requirement
2.4.2.4.2 Early voting model	The cast ballot SHALL NOT be linked to the voter's identity.	Agree with Requirement
2.4.3 Vote Secrecy		
2.4.3.1 Link to voter	The voting system SHALL be capable of producing a cast vote record that does not contain any information that would link the record to the voter.	In the Glossary, cast vote record needs a better definition, such that it is differentiated from the cast ballot more explicitly. Should indicate that it is the record stored in the voting system, as opposed to the cast ballot that is produced by the vote capture device. In the Absentee model the cast ballot contains links to the voters identity, where the cast vote record should not.
2.4.3.2 Voting session records	The voting system SHALL NOT store any information related to the actions performed by the voter during the voting session.	Audit logs would record when the voter accessed ballot, as well as when they cast the ballot, but no information that would link stored information to individual voter
2.5 Post Voting Capabilities		

Section	*Requirements*	*SLI Comments*
2.5.1 Ballot Box Retrieval and Tabulation		An additional requirement is recommended that explicitly deals with encryption of electronic ballot box upon closure of the voting period, in order to prevent voter data (private information and vote data) from being exposed in even a read only manner. "Seal" in 2.5.1.1 may be used to cover this concept. But then should be broken out to a seperate requirement from the "sign"
2.5.1.1 Seal and sign the electronic ballot box	The voting system SHALL seal and sign each jurisdiction's electronic ballot box, by means of a digital signature, to protect the integrity of its contents.	Would recommend that the term "seal" be more explicitly defined. "Seal" is historically more of a physical concept, whereas in this instance it is a logical concept. May want to define as making the electronic ballot box "read only", with corresponding time stamp or something similar.
2.5.1.2 Electronic ballot box retrieval	The voting system SHALL allow each jurisdiction to retrieve its electronic ballot box.	Agree with Requirement
2.5.1.3 Electronic ballot box integrity check	The voting system SHALL perform an integrity check on the electronic ballot box verifying that it has not been tampered with or modified before opening.	See comments in 2.5.1 and 2.5.1.1, as would pertain to this requirement
2.5.2 Tabulation		
2.5.2.1 Tabulation device connectivity	The tabulation device SHALL be physically, electrically, and electromagnetically isolated from any other computer network.	Enumerate the activities
2.5.2.2 Open ballot box	The tabulation device SHALL allow only an authorized entity to open the ballot box.	Recommend adding "voting system" in front of "authorized entity"
2.5.2.3 Absentee model		
2.5.2.3.1 Adjudication	The tabulation device SHALL allow the designation of electronic ballots as "accepted" or "not accepted" by an authorized entity.	1) See comment in 2.5.2.2 2) "electronic ballots" is not a defined term. Recommend using the term "Cast Ballot"
2.5.2.4 Ballot decryption	The tabulation device decryption process SHALL remove all layers of encryption and breaking all correlation between the voter and the ballot, producing a record that is in clear text.	Decryption process may be different that what is used to break all correlations between voter and ballot. This requirement should be broken out. The breaking of the correlation should only be done after the adjudication is completed. The decryption process may be involved at multiple points of this overall process.
2.5.2.5 Tabulation report format	The tabulation device SHALL have the capability to generate a tabulation report of voting results in an open and non-proprietary format.	Agree with Requirement

Section	*Requirements*	*SLI Comments*
2.6 Audit and Accountability		Assumption is that 2.6.1 and 2.6.2 are "header" sections that should not have any actionable events. The "Shall" in 2.6.2 should be removed.
2.6.1 Scope	The intention is to provide for independent verification of the agreement of the paper record and electronic tabulation results. These audits could be conducted on the entire set of records or on a sampling basis, depending on the preferences of state/local jurisdictions:	
2.6.1 Scope	a. Hand audit – Validation of electronic tabulation results via comparison with results of a hand tally of paper records; and	
2.6.1 Scope	b. Comparison of ballot images and the corresponding paper records.	
2.6.2 Electronic Records	In order to support independent auditing, a voting system SHALL be able to produce electronic records that contain the necessary information in a secure and usable manner. Typically, this includes records such as: - Vote counts; - Counts of ballots recorded; - Paper record identifier; - Event logs and other records of important events; and - Election archive information.	1) Recommend using appropriate NIST standard, and/or VVSG section 2.1.5, in place of "secure and usable manner". 2) Recommend removing "Typically", and rephrasing to something like, "this includes, but is not limited to:" 3) Enumerate bullets such that they are referenceable. 4) Remove "Shall" as it causes need for actionable event.Recommend more explicity defining "important events"
2.6.2 Electronic Records	The following requirements apply to records produced by the voting system for any exchange of information between devices, support of auditing procedures, or reporting of final results:	Enumerate in relation to above subsection
2.6.2 Electronic Records	a. Requirements for electronic records to be produced by tabulation devices; and	The pertinent requirements associated to this sub requirement should be explicitly called out. A vague reference will only create gaps in coverage.
2.6.2 Electronic Records	b. Requirements for printed reports to support auditing steps.	The pertinent requirements associated to this sub requirement should be explicitly called out. A vague reference will only create gaps in coverage.
2.6.2.1 All records capable of being exported	The voting system SHALL provide the capability to export its electronic records in an open format, such as XML, or include a utility to export log data into a publicly documented format.	Agree with Requirement

Section	*Requirements*	*SLI Comments*
2.6.2.2 Ballot images	The voting system SHALL have the capability to generate ballot images in a human readable format.	Agree with Requirement
2.6.2.3 Ballot image content	The voting system SHALL be capable of producing a ballot image that includes:	Does this requirement need a complementary requirement, similar to how 2.6.3.2 has 2.6.3.3 Privacy?
2.6.2.3 Ballot image content	a. Election title and date of election;	
2.6.2.3 Ballot image content	b. Jurisdiction identifier;	
2.6.2.3 Ballot image content	c. Ballot style;	
2.6.2.3 Ballot image content	d. Paper record identifier; and	
2.6.2.3 Ballot image content	e. For each contest and ballot question:	
2.6.2.3 Ballot image content	i. The choice recorded, including write-ins; and	
2.6.2.3 Ballot image content	ii. Information about each write-in.	
2.6.2.4 All records capable of being printed	The tabulation device SHALL provide the ability to produce printed forms of its electronic records. The printed forms SHALL retain all required information as specified for each record type other than digital signatures.	Should be enumerated or split out
2.6.2.5 Summary count record	The voting system SHALL produce a summary count record including the following:	Agree with Requirement
2.6.2.5 Summary count record	a. Time and date of summary record; and	
2.6.2.5 Summary count record	b. The following, both in total and broken down by ballot style and voting location:	
2.6.2.5 Summary count record	i. Number of received ballots	
2.6.2.5 Summary count record	ii. Number of counted ballots	
2.6.2.5 Summary count record	iii. Number of rejected electronic CVRs	
2.6.2.5 Summary count record	iv. Number of write-in votes	
2.6.2.5 Summary count record	v. Number of undervotes.	
2.6.3 Paper Records	The vote capture device is required to produce a paper record for each ballot cast. This record SHALL be available to the voter to review and verify, and SHALL be retained for later auditing or recounts, as specified by state law. Paper records provide an independent record of the voter's choices that can be used to verify the correctness of the electronic record created by the vote capture device.	Need to remove "Shall" from header
2.6.3.1 Paper record creation	Each vote capture device SHALL print a human readable paper record.	Agree with Requirement
2.6.3.2 Paper record contents	Each paper record SHALL contain at least:	2.6.2.3 and 2.6.3.2 test for the same thing, but one if Test Method Inspection and the other is Functional. Should be consistent. Recommend making both Inspection.

Section	Requirements	SLI Comments
2.6.3.2 Paper record contents	a. Election title and date of election;	
2.6.3.2 Paper record contents	b. Voting location;	
2.6.3.2 Paper record contents	c. Jurisdiction identifier;	
2.6.3.2 Paper record contents	d. Ballot style;	
2.6.3.2 Paper record contents	e. Paper record identifier; and	
2.6.3.2 Paper record contents	f. For each contest and ballot question:	
2.6.3.2 Paper record contents	i. The recorded choice, including write-ins; and	
2.6.3.2 Paper record contents	ii. Information about each write-in.	
2.6.3.3 Privacy	The vote capture device SHALL be capable of producing a paper record that does not contain any information that could link the record to the voter.	Agree with Requirement
2.6.3.4 Multiple pages	When a single paper record spans multiple pages, each page SHALL include the voting location, ballot style, date of election, and page number and total number of the pages (e.g., page 1 of 4).	Enumerate the activities
2.6.3.5 Machine-readable part contains same information as human-readable part	If a non-human-readable encoding is used on the paper record, it SHALL contain the entirety of the human-readable information on the record	Agree with Requirement
2.6.3.6 Format for paper record non-human-readable data	Any non-human-readable information on the paper record SHALL be presented in a non-proprietary format.	Agree with Requirement
2.6.3.7 Linking the electronic CVR to the paper record	The paper record SHALL:	
2.6.3.7 Linking the electronic CVR to the paper record	a. Contain the paper record identifier; and	
2.6.3.7 Linking the electronic CVR to the paper record	b. Identify whether the paper record represents the ballot that was cast.	Recommend replacing "Identify" with "Validates"
2.7 Performance Monitoring		
2.7.1 Voting system and Network Status		
2.7.1.1 Network monitoring	The system server SHALL provide for system and network monitoring during the voting period.	More detail should be added as to what level of monitoring should be taking place. This could be as minimal as, "the light is green, the system is up".
2.7.1.2 Tool access	The system and network monitoring functionality SHALL only be accessible to authorized personnel from restricted consoles.	Agree with Requirement

Section	*Requirements*	*SLI Comments*
2.7.1.3 Tool privacy	System and network monitoring functionality SHALL NOT have the capability to compromise voter privacy or election integrity.	Agree with Requirement

Appendix D – Changes to the VSTL Standard Testing Methodology for UPPTR

Step	VSTL Standard Methodology	Changes to meet UPPTR	Risks
a.	Initial examination of the system and the technical documentation provided by the vendor to ensure that all components and documentation needed to conduct testing have been submitted, and to help determine the scope and level of effort of testing needed. TDP Review.	Technical Data Package (TDP) was Not Required.	VSTLs may find it difficult to design new test cases or to modify existing test cases; to conduct complete testing or to adequately scope project.
b.	Examination of the vendor's Quality Assurance Program and Configuration Management Plan.	Not Required	Vendor may deliver wrong configuration of voting system to VSTL for testing.
c.	Development of a detailed system test plan that reflects the scope and complexity of the system, and the status of system certification (i.e., initial certification or a recertification to incorporate modifications).	Test Plan in VSTLs format.	Scope of testing and effort may not be completely defined and controlled.
d.	Code review for selected software components.	Not Required	VSTL may not adequately assess the need for additional test cases; may not define white-box test cases for security testing.
e.	Witnessing of a system 'build' conducted by the vendor to conclusively establish the system version and components being tested.	Not Required	VSTL may not be able to test all functionality if not included in build.
f.	Operational testing of hardware components, including environmental tests, to ensure that operational performance requirements are achieved.	Not Required	
g.	Functional and performance testing of hardware components.	Not Required	
h.	System installation testing and testing of related documentation for system installation and diagnostic testing.	Not Required	May cause test environment set-up delays; for remote system testing and diagnosis, this could be significant schedule impact to testing.
i.	Functional and performance testing of software components.	Not Required	May not be able to completely test security features. May not catch capacity problems (e.g., number of concurrent users) until later in testing.

Step	VSTL Standard Methodology	Changes to meet UPPTR	Risks
j.	Functional and performance testing of the integrated system, including testing of the full scope of system functionality, performance tests for telecommunications and security; and examination and testing of the System Operations Manual.	Functional testing only. No System Operations Manual was required.	Without an adequate number of test cases, the complete testing of functionality would not be performed.
k.	Examination of the system maintenance manual.	Not Required	May miss security risks to test for.
l.	Preparation of the National Certification Test Report.	Not Required	
	Final test report including any discrepancies found during testing would be sent to each vendor; only a redacted report without any test discrepancies would be submitted.	In VSTLs format	
	Final test report includes the laboratories' comments on suitability and testability of the requirements as well as any recommendations for improvement.	In VSTLs format	
m.	Delivery of the National Certification Test Report to the EAC.	Not Required	

Appendix E – SLI Global Solutions Test Report

Test Report

UOCAVA Testing Requirements Pilot Program

Test Report Rev 04

July 19th, 2011

Prepared for:

Client Name	*Federal Voting Assistance Program*
Representative Organization	*CALIBRE*

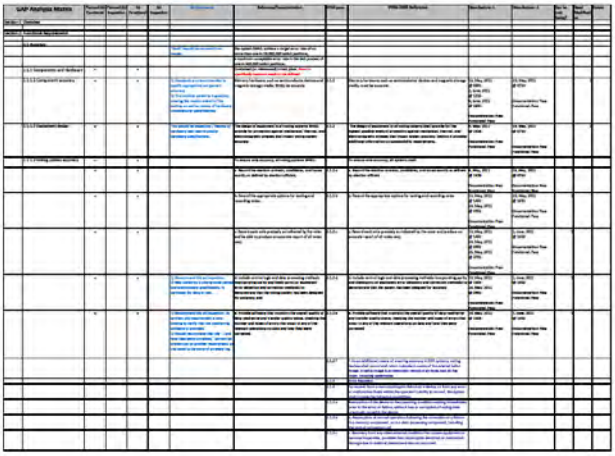
Prepared by:

216 16th St.
Suite 700
Denver, CO 80202
303-575-6881
www.SLIGlobalsolutions.com

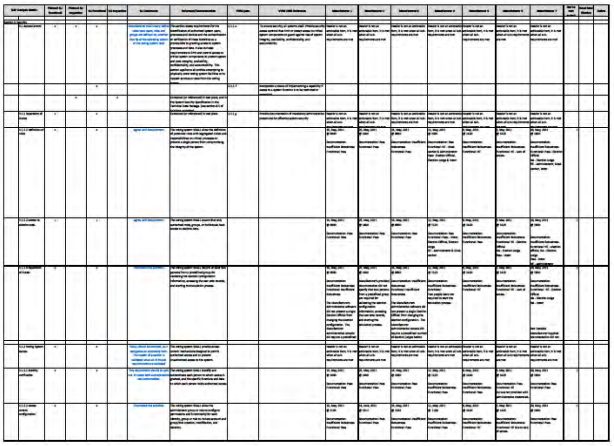
NVLAP LAB CODE 200755-0

Accredited by the National Institute of Standards and Technology (NIST) National Voluntary Lab Accreditation Program (NVLAP), and accredited by the Election Assistance Commission (EAC) for VSTL status.

SLI Global Solutions' Gap Analysis Matrix – Section 2



SLI Global Solutions' Gap Analysis Matrix – Section 5



Test Report

UOCAVA Testing Requirements Pilot Program

Test Report Rev 04

July 19th, 2011

Prepared for:

Client Name	*Federal Voting Assistance Program*
Representative Organization	*CALIBRE*

Prepared by:

216 16th St.
Suite 700
Denver, CO 80202
303-575-6881
www.SLIGlobalsolutions.com

NVLAP LAB CODE 200733-0

Accredited by the National Institute of Standards and Technology (NIST) National Voluntary Lab Accreditation Program (NVLAP), and accredited by the Election Assistance Commission (EAC) for VSTL status.

Revision History

Release	Author	Revisions
Rev 01	M. Santos	Initial Release
Rev 02	M. Santos	2nd Release, incorporating update requests from Calibre
Rev 03	M. Santos	Updated with test result definitions, included percentages to results
Rev 04	M. Santos	Added tables that show percentages of requirements passed, failed, not tested, and not applicable. Requirements defined as a section that contains a shall. Estimates of how many requirements could be met if everything needed was provided. Estimate of what could be met with incorporation of recommended requirement modifications.

Disclaimer

The Certification Test results reported herein must not be used by the client to claim product certification, approval, or endorsement by NVLAP, NIST, or any agency of the Federal Government. Results herein relate only to the items tested.

The tests referenced in this document were performed in a controlled environment using specific systems and data sets, and results are related to the specific items tested. Actual results in other environments may vary.

TABLE OF CONTENTS

1 Introduction

SLI Global Solutions is submitting this report as a summary of the testing efforts and requirements review for the Federal Voting Assistance Program (FVAP) UOCAVA Test Requirements Pilot Program.

Within the scope of this project, each manufacturer was requested to provide either an implementation of, or access to, an iteration of their system. Provision of documentation was not a requirement of the project, from the manufacturer point of view. SLI did make requests to each manufacturer for any available information with regard to the implemented system, especially from a security point of view. Recognizing that each manufacturer may be in a different phase of developing their production level systems, SLI acknowledges that not all documentation that would be in place for a formal certification effort may have been ready for this pilot project. As such, SLI reviewed what documentation was provided, and noted areas that are in need of documentation and/or further refinement. We believe it is important to note that with the volunteer aspect of this project on the part of the manufacturers, this project in many ways resembled a “Beta” project. With other projects ongoing internally, many of the manufacturers often attempted to assist in the project, but many times could not make the appropriate resources available.

This effort included documentation review of each manufacturer’s Technical Data Package, to the extent provided, as well as testing of the manufacturer’s internet based voting system. Testing consisted of the creation, validation, and execution of sets of tests prepared by SLI. The review and testing was performed at SLI’s Denver, Colorado facility.

As directed by CALIBRE, the primary focus of this project was the evaluation of the requirement set, which included Sections 2 and 5 of UOCAVA Pilot Program Testing Requirements for full systems and Section 5 of UOCAVA Pilot Program Testing Requirements for Electronic Voting Support Wizards (EVSWs), against the submitted voting systems. SLI has taken the approach to not only evaluate each pertinent requirement against the manufacturer’s system but to evaluate the requirement itself. Each requirement has been critiqued to determine its applicability and to determine if any gaps or ambiguities exist.

SLI is a full service third party testing facility, founded in May 1996, from a software test-consulting firm. The specific system testing services offered include:

- Test Planning and Test Management
- eBusiness, Client-Server and Stand-alone Application Functional, Compatibility and Regression Testing
- eBusiness and Client-Server Load and Performance Testing

- Automated Regression Test Development, Consulting, Scripting and Execution
- Complex, Integrated Test Solutions and Automated Test Harnesses
- Independent Verification and Validation
- EAC approved and NIST NVLAP accredited Voting System Test Laboratory

1.1 References

1. Federal Voting Assistance Program Uniformed and Overseas Citizens Absentee Voting Act, August 25, 2010
2. SLI Quality System Manual, Revision Rev. 1.12, prepared by SLI, dated February 24, 2011.

1.2 Document Overview

This document contains:

- The Introduction, which discusses the project scope
- The Test Background, which discusses the testing process
- The Requirements Analysis section, which provides a summary of how the requirements pertain to the UOCAVA environment
- The Recommendations section, which contains the final analysis of the testing effort
- The Systems Overview, which discusses the different types of systems evaluated in the project
- The Test Results Summary, which discusses how the systems fared against the requirements set
- Attachments as follows:
    - Attachment A – FVAP Test Requirements matrix
    - Attachment B – Documentation and Information Requests

2 Testing Methodologies Employed

2.1 Formal Certification

In a formal certification test campaign, SLI would expect a production level system delivered for testing. This encompasses any and all hardware, consumables, source code, and applications; all documentation relevant to how the system is architected and implemented; a declaration of the functionality supported by the system; and documentation of how the system is employed by a jurisdiction.

A certification test campaign is broken out into 6 main phases, each phase building upon the preceding phases.

The first phase deals with receipt of the system's components and applicable documentation. The manufacturer is requested to provide training on the various aspects of the system under test. Additionally, the first phase encompasses reviewing the documentation provided against the applicable requirements to verify that all needed information is appropriately conveyed. Source code review is also begun in this phase. At the end of the first phase, with a more in-depth understanding of the system based on the documentation review, a test plan is begun that details the variations of the system to be tested, as well as how the test suites will be constructed for testing the declared supported functionality.

The second phase deals with creation of a readiness test, which demonstrates that the system is installed and running correctly at a basic level and prepared for use in other tests to be run. Additionally, the content of each test suite to be executed is determined, at a high level, in this phase.

The third phase deals with the creation of the individual test modules that, when brought together within a suite, will execute each piece of functionality within the system under test.

The fourth phase deals with the incorporation of each module into the respective suites that will utilize it and validating the correctness of each module within each suite. This phase can be iterative until all modules within every suite are determined to be correct in implementation. In this phase a Trusted Build is done, where SLI follows the manufacturer's prescribed build process to create binaries that will compromise the voting system.

The fifth phase deals with the formal execution of each test suite, as prescribed in the test plan.

Note that each of the first five phases is considered to be iterative in that if an issue is identified, discrepancies are written and reported to the manufacturer with the

expectation that the issue will be resolved such that the pertinent requirement is met. This, at times, will take several iterations and potentially consultation with the EAC.

The sixth phase deals with creation, submission and acceptance of the certification test report.

2.2 UOCAVA Pilot Project

Generally speaking, the six phases outlined in the preceding section were followed, with modifications due to differences of expected deliverables, as outlined in this section.

For the first phase, source code was not mandated to be delivered; neither was a full technical documentation set, nor necessarily hardware. Not all manufacturers provided training on how their respective system worked.

Both full system manufacturers provided election creation/importation documentation, relative to Section 2, Functional Requirements, as well as back office environments for SLI's local use, as did one ESVW manufacturer.

In terms of documentation of security implementations, which was the main topic of this project, only two manufacturers delivered any documentation related to how security was implemented in their system. Two manufacturers asserted that the technologies used to implement their system inherently made the system secure. One example is a manufacturer who implements their system through the Azure cloud. They claim that Azure provides all security aspects needed. We would tend to disagree. Regardless of how the Azure cloud handles security, if the manufacturer does not call processes in the correct manner, the security aspect may well be circumvented. Regardless of technologies being implemented, each manufacturer must understand that they must have a formally documented security architecture in place.

Only one manufacturer provided a "kiosk location" setup. All other manufacturers only provided URLs to websites, with SLI providing hardware to simulate the vote capture device.

In terms of the training provided, the manufacturers who did provide training gave an overview of the functionality provided by their system. While helpful, this was of somewhat limited value when taking into consideration that the primary focus of most of the systems reviewed was security. When this was brought up, most of the manufacturers appeared somewhat surprised and perplexed by SLI's line of questioning.

Taking what was delivered by each manufacturer, SLI began to review the provided documentation. As gaps were determined, we made requests to the manufacturers for additional information. In some instances we received some additional detail, but many times we did not. In a formal certification effort we would have written discrepancies and kept them open until the requirement was fully satisfied. In this situation, dealing with volunteers we would request additional details two or three times, then move on. In several cases, we would simply not receive any response.

For the second phase, readiness tests were created for each of the full systems, to verify the system's ability to go through the election process. For the determination of the suites to be used, SLI determined to implement the functional testing on election cycle flows, and security testing based on the requirement sections.

For the third phase, we created test modules for each vendor to determine how well they met each requirement individually. In many cases this was problematic, as from a physical (hardware) perspective, many of the manufacturers declared their use of commercial off the shelf devices to act as the vote capture device. Several of the manufacturers take the approach that individual voters will provide the vote capture device, instead of utilizing a kiosk location. From a programmatic perspective, many of the manufacturers did not have a formally documented approach or an implementation description of how they logically met the applicable security considerations. Whereas in a formal certification we would normally follow the documented processes for the system, in this situation, with so little provided documentation, we took the approach of working with the system to determine how functionality was applied.

For the fourth phase, for the full systems SLI validated the full election cycle test suites that had been created, as well as other functional tests. For the security testing, a review of documentation and how the modules were written comprised the majority of the validation effort.

The fifth phase was a final execution of the test suites and modules with a determination of the requirements being met by each vendor, or insufficient robustness of the documentation or implementation.

The sixth phase consists of writing a redacted project summary report for Calibre/FVAP, as well as individual reports for each participating manufacturer.

3 Test Background

3.1 Initial Considerations

Provision of documentation was not a requirement of the project, from the manufacturer point of view. SLI did make requests to each manufacturer for any available information with regard to the implemented system, especially from a security point of view. Recognizing that each manufacturer may be in a different phase of developing their production level systems, SLI acknowledges that not all documentation that would be in place for a formal certification effort may have been ready for this pilot project. As such, SLI reviewed what documentation was provided, and noted areas that are in need of documentation and/or further refinement.

3.2 Review of Documentation

Documentation submitted by each manufacturer was reviewed against the FVAP UOCAVA Pilot Program Testing Requirements in order to determine sufficiency with regard to the requirements.

In the review of documentation, the scope of the review was determined by the type of system under review. Full systems were subject to sections 2 and 5, and wizards subject to only section 5.

3.3 Functional Testing

SLI's Test Suites were customized for each voting system and conducted in conjunction with the inspection/functional testing, as prescribed in the FVAP UOCAVA Pilot Program Testing Requirements, and as applicable given the type of system under review, whether a full system subject to sections 2 and 5, or a wizard subject to only section 5.

For a full system, simulations of entire election cycles were conducted, from election definition or importation to casting of ballots during voting periods to post voting activities, including any associated "back office" operations. These simulations were conducted to demonstrate a beginning-to-end business use case process for the voting system.

For wizard implementations, simulations of voting periods and post casting activities that are applicable to the wizard were examined from a section 5, Security, perspective.

For the wizard implementations, most were hosted remotely. As such, SLI endeavored to work with each manufacturer to perform remote location testing. In this remote testing, during a video/teleconference “back office” operations were examined to determine the sufficiency in accordance with the pertinent Security requirements. This type of testing requires interactions with manufacturer personnel for 4-6 hours. Not all manufacturers were able to accommodate this resource allocation.

4 Requirements Analysis

SLI reviewed the requirements from the viewpoint of a functioning VSTL. Based on past experiences performing test campaigns for federal certifications under both NASED and the EAC, SLI evaluated the requirements for applicability, robustness and layout.

We asked if the requirement was reasonable and necessary for an internet based environment voting system. We took into consideration that internet technology and the implementation of a voting system in that environment constitutes a very different approach in comparison to a traditional voting system. The traditional system employs much more hardware in more isolated environments and is subject to less potential exposure.

Then we examined the requirement to see if it covered all necessary aspects that the requirement was attempting to validate. If we determined that some aspect of the voting system wasn’t being adequately addressed, we made recommendations accordingly. In a number of instances, we noted where the requirement was vague or ambiguous as to how it should be adequately met. We often recommended that NIST SP’s be referenced in order to create consistency in how the requirement would be met.

Layout of requirements, in terms of how they are enumerated, was also reviewed. As a VSTL, our preference is to be able to explicitly reference any particular requirement. Any “Shall” and/or accompanying “and” is usually preferred to be enumerated. We use the term “enumerate” in the sense of itemizing items with an explicitly unique and reference-able number/letter sequence. The requirements that we commented on relative to formatting, we leave for review in Attachment A.

In the following subsections we will quantify how many of the UOCAVA requirements can be met by all manufacturers today. We will also look at what requirements we believe should be modified, or removed, in order for manufacturers to be able to meet the intended criteria.

4.1 Number of UOCAVA requirements that could be met today

In looking at the requirements within the UOCAVA Pilot Program Testing Requirements document, we limit the discussion to Section 2 – Functional Requirements, and Section 5 – Security. In reviewing the requirements for their applicability within the program and the extent to which they can be met, we looked at requirements that are “actionable”, in the sense that something can be done to ascertain an answer to the sufficiency of a voting system meeting the requirement. In this way we removed headers that have sub-requirements that if all are fully met, imply that the header portion of the requirement is met. In this analysis we discuss the requirements in terms of their content, not formatting. Within Attachment A, we note requirements that would benefit from updates to formatting. This topic is an important area for the program in that it assists all stakeholders in being to discretely address every actionable item within the requirements set in such a way that removes ambiguity. With the main intent of this project to determine the applicability of the requirement content, we will refrain from addressing the formatting aspect in detail and instead ask the reader to review Attachment A.

In reviewing the requirements using this methodology, we determined that there are 124 actionable requirements in Section 2 – Functional Requirements, and 168 actionable requirements in Section 5 – Security.

In our review of Section 2 - Functional Requirements, our analysis led SLI to the conclusion that the requirement set is written such that 96 (78%) of the requirements can be met today, while 25 (20%) requirements need modification to be testable, and 2 (2%) requirements are such that they can be considered for deletion.

In our review of Section 5 - Security, our analysis led SLI to the conclusion that the requirement set is written such that 147 (87%) of the requirements can be met today, while 15 (9%) requirements need modification to be testable, and 7 (4%) requirements are such that they can be considered for deletion.

By second level subsection, these metrics, in terms of percentage of requirements within the subsection, break out as follows:

Subsection	Percentage of Requirements can be met today	Percentage of Requirements needs modification prior to being testable	Percentage of Requirements should be considered for deletion
2.1	40%	50%	10%
2.2	85%	15%	0%
2.3	100%	0%	0%
2.4	88%	12%	0%
2.5	56%	44%	0%
2.6	87%	13%	0%
2.7	67%	33%	0%
5.1	94%	6%	0%
5.2	95%	5%	0%
5.3	77%	23%	0%
5.4	63%	37%	0%
5.5	78%	22%	0%
5.6	94%	6%	0%
5.7	100%	0%	0%
5.8	100%	0%	0%
5.9	56%	5%	39%

The conclusions are in line with what we expected based on our preliminary analysis. The requirement set contains new and untested requirements, as well as some requirements conceived for more traditional voting systems rather than an internet environment. Considering this fact and also with the use of both proven technologies as well as some of the latest, cutting edge technologies and environments, we anticipated areas that would need adjustment or removal.

4.2 Requirements that could be modified to better meet UOCAVA needs

In this section we look at specific requirements that SLI believes might be modified in order to better set out what is needed by an internet voting system. We will address only those requirements that we have comments on relative to content. The requirements that we commented on relative to formatting are left for review in Attachment A.

For the requirement 2.1 Accuracy, which states, “the system SHALL achieve a target error rate of no more than one in 10,000,000 ballot positions, a maximum acceptable error rate in the test process of one in 500,000 ballot positions.”, SLI believes that "Shall" should be removed from the header, as actionable items should be included in the requirement, not the header.

For the requirement 2.1.1.1 Component accuracy, which states, “Memory hardware, such as semiconductor devices and magnetic storage media, SHALL be accurate”, SLI believes that “…SHALL be accurate” is too ambiguous; references to relevant standards are recommended to specify appropriate component accuracy. Also, we believe that this is better suited to inspection, viewing the overall results of the testing, as well as review of hardware manufacturer specifications.

For the requirement 2.1.1.2 Equipment Design, which states, “The design of equipment in all voting systems SHALL provide for protection against mechanical, thermal, and electromagnetic stresses that impact voting system accuracy”, SLI believes that this should be Inspection / Review of hardware test reports and/or hardware specifications.

For the requirement 2.1.1.3.d Voting System Accuracy, which states, “Voting System Accuracy - Include control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) to demonstrate that the voting system has been designed for accuracy”, SLI believes that this requirement is better suited as an Inspection test method. SLI believes that this requirement is best suited for a source code review and environment specification, in particular for data at rest.

For the requirement 2.1.1.3.e Voting System, which states, “Provide software that monitors the overall quality of data read-write and transfer quality status, checking

the number and types of errors that occur in any of the relevant operations on data and how they were corrected", SLI believes that this requirement is better suited as an Inspection test method. As written, this requirement is only looking to verify that the monitoring software is provided. SLI would also recommend that the "…and how they were corrected" portion be broken out to another requirement, as this looks to be more of an event log.

For the requirement 2.1.2 Environmental Range, which states, "All voting systems SHALL meet the accuracy requirements over manufacturer specified operating conditions and after storage under non-operating conditions", SLI believes that this requirement should be an Inspection test method.

For the requirement 2.1.3.1 Election management system accuracy, which states, "Voting systems SHALL accurately record all election management data entered by the user, including election officials or their designees", SLI believes that this requirement contains a high degree of ambiguity. Each type of EM data should be enumerated.

For the requirement 2.1.3.2.b Recording Accuracy, which states, "Accurately interpret voter selection(s) and record them correctly to memory", SLI believes that the "… to memory" is potentially too specific a data recording method and would recommend this portion be removed.

For the requirement 2.1.3.2.c Recording Accuracy, which states, "Verify the correctness of detection of the user selections and the addition of the selections correctly to memory", SLI is concerned that it is not clear how this requirement is examining anything different from part b.

For the requirement 2.1.3.2.d Recording Accuracy, which states, "Verify the correctness of detection of data entered directly by the user and the addition of the selections correctly to memory", SLI believes that this requirement is testing write-ins as opposed to selecting choices, as in b and c. These sub-requirements (b, c and d) need to be clarified as to their specific intents, with any redundancies removed.

For the requirement 2.1.3.2.e Recording Accuracy, which states, “Preserve the integrity of election management data stored in memory against corruption by stray electromagnetic emissions, and internally generated spurious electrical signals”, SLI believes that would be covered under EMC testing, and as such would recommend the test method be Inspection for this requirement.

For the requirement 2.1.5 Accuracy Test Content, which states, “Voting system accuracy SHALL be verified by a specific test conducted for this objective. The overall test approach is described in Appendix C.”, SLI believes that for a true internet voting system that uses a web browser implementation for capturing votes, the accuracy test is whether or not the election is coded correctly. The technologies involved are mature, proven and robust.

For a true internet voting system that employs physical devices such as a touch screen, the accuracy test would be similar to that of a ballot delivery system, in that the touch screen is dependent on the prescribed maintenance cycle of the device. For a ballot delivery system, where the cast ballot is potentially returned in any of a number or ways (fax, email, printed/scanned), the accuracy is dependent on the device used, within the confines of the prescribed maintenance cycles of the device.

For the requirement 2.1.5.2 Ballots, which states, “Ballots used for accuracy testing SHALL include all the supported types (i.e., rotation, alternative languages) of contests and election types (primary, general)”, SLI believes that the applicability of the ballot types to accuracy testing is not relevant. Accuracy testing concerns itself with accuracy with regard to the scanning/reading of each possible ballot position on a given size ballot. The ability of the system to correctly handle the various supported voting variations is addressed in other tests.

For the requirement 2.1.6 Reporting Accuracy, which states, “The voting systems SHALL produce reports that are consistent, with no discrepancy among reports of voting data”, SLI believes that this requirement is too high level. We would like to see some specific metrics called out to ensure reporting accuracy, similar to v1.0 VVSG volume 1, sections 2.4.2 and 2.4.3

For the requirement 2.2.1 Maximum Capacities, which states, “The manufacturer SHALL specify at least the following maximum operating capacities for the voting system (i.e. server, vote capture device, tabulation device, and communications links)”, SLI would recommend that this section look at capacities more in terms of

minimums that need to be met (as specified by NIST/FVAP), rather than as stated maximum capacities that a manufacturer claims they can accommodate. We have observed that manufacturers often list an unrealistically high number for many of these categories. SLI believes that a minimum standard will create a more meaningful and consistent baseline for all manufacturers.

For the requirement 2.2.1.1 Capacity Testing, which states, “The voting system SHALL achieve the maximum operating capacities stated by the manufacturer in section 2.2.1”, SLI would recommend having this requirement meet some minimum level of acceptability, as defined by FVAP/NIST. The maximum levels are often unrealistically high and of reduced meaningfulness to jurisdictions.

For the requirement 2.2.3 Simultaneous transmissions, which states, “The voting system SHALL protect against the loss of votes due to simultaneous transmissions”, SLI would recommend making the Test Method for this item Inspection/Functional. Some instances can be impractical to functionally validate.

SLI would also recommend that an expected capacity of simultaneous transmissions be defined, as any minimum value is ambiguous as written. As written, two simultaneous transmissions would technically meet the requirement, even though we don’t believe that would meet the intent.

For the requirement 2.4.2.1.f Record voter selections, which states, “Indicate to the voter when no selection, or an insufficient number of selections, has been made for a contest (e.g., undervotes)”, SLI would recommend that this requirement be made more specific as to notifying the voter of a potential undervote prior to casting of the ballot (as opposed to when the voter is going from one contest (or screen) to another).

For the requirement 2.4.2.1.j Record voter selections, which states, “In the event of a failure of the main power supply external to the voting system, provide the capability for any voter who is voting at the time to complete casting a ballot, allow for the successful shutdown of the voting system without loss or degradation of the voting and audit data, and allow voters to resume voting once the voting system has reverted to back-up power”, SLI believes that this may not be feasible in a remote session environment. Where the power failure occurs, as well as the duration, will dictate if a ballot can be recorded within the voting system without loss or degradation of voting/audit data.

The "… allow voters to resume voting..." clause would inherently cause some kind of voter data to be resident on the vote capture device, which would potentially violate other Security requirements (5.4.1.3).

For the requirement 2.4.2.2.a Verify voter selections, which states, “Produce a paper record each time the confirmation screen is displayed”, SLI would recommend that a paper record is generated only when the ballot is cast and not each time the confirmation screen is accessed.

For the requirement 2.4.2.2.c Verify voter selections, which states, “Allow the voter to either cast the ballot or return to the vote selection process to make changes after reviewing the confirmation screen and paper record”, SLI would recommend removing "… and paper record"; see comment to "a" above.

For the requirement 2.4.2.3 Cast ballot, SLI would recommend renaming requirement to “Post Cast Ballot Process”.

For the requirement 2.4.2.3.b Cast ballot, which states, “Notify the voter after the vote has been stored persistently that the ballot has been cast”, SLI recommends defining "persistently" to more detail.

In a full electronic system, "persistently" would indicate that the central server has received the vote record and stored it.

In a ballot delivery system, "persistently" would indicate the printing of a physical ballot, or creation of a pdf.

For the requirement 2.4.3.1 Link to voter, which states, “The voting system SHALL be capable of producing a cast vote record that does not contain any information that would link the record to the voter”, SLI believes that in the Glossary, “Cast Vote Record” needs a better definition so it is differentiated more explicitly from “Cast Ballot”. The definition for “Cast Vote Record” should indicate that it is the record stored in the voting system, as opposed to the cast ballot that is produced by the vote capture device. In the Absentee model the cast ballot contains links to the voter’s identity, where the cast vote record should not.

For the requirement 2.5.1 Ballot Box Retrieval and Tabulation, SLI believes that an additional requirement is recommended that explicitly deals with encryption of the electronic ballot box upon closure of the voting period, in order to prevent voter data (private information and vote data) from being exposed, even in a read-only manner. "Seal" in 2.5.1.1 may be used to cover this concept but then should be broken out to a separate requirement from the "sign" portion.

For the requirement 2.5.1.1 Seal and sign the electronic ballot box, which states, “The voting system SHALL seal and sign each jurisdiction’s electronic ballot box, by means of a digital signature, to protect the integrity of its contents”, SLI would recommend that the term "seal" be more explicitly defined. "Seal" is historically more of a physical concept, whereas in this instance it is a logical concept. A suggestion is to define it as making the electronic ballot box "read only", with a corresponding time stamp or something similar.

For the requirement 2.5.1.3 Electronic ballot box integrity check, which states, “The voting system SHALL perform an integrity check on the electronic ballot box verifying that it has not been tampered with or modified before opening”, SLI believes that the comments in 2.5.1 and 2.5.1.1 pertain to this requirement as well.

For the requirement 2.5.2.2 Open ballot box, which states, “The tabulation device SHALL allow only an authorized entity to open the ballot box”, SLI would recommend adding "voting system" in front of "authorized entity".

For the requirement 2.5.2.3.1 Adjudication, which states, “The tabulation device SHALL allow the designation of electronic ballots as “accepted” or “not accepted” by an authorized entity”, SLI would recommend adding "voting system" in front of "authorized entity". Also, "electronic ballots" is not a defined term. We recommend using the term "Cast Ballot" instead.

For the requirement 2.6.2 Electronic Records, which states, “In order to support independent auditing, a voting system SHALL be able to produce electronic records that contain the necessary information in a secure and usable manner”, SLI would recommend using the appropriate NIST standard, and/or VVSG section 2.1.5, in place of "secure and usable manner". Also, we would recommend removing "Typically", and rephrasing it to something like, "this includes, but is not limited to:" Additionally we would like to see this requirement broken out of the header and

enumerated for actionable events. ("Shall" in the header indicates need for an actionable event.)

For the requirement 2.6.2 Electronic Records, which states, “- Event logs and other records of important events”, SLI would recommend more explicitly defining "important events".

For the requirement 2.6.2 Electronic Records, which states, “The following requirements apply to records produced by the voting system for any exchange of information between devices, support of auditing procedures, or reporting of final results: a. Requirements for electronic records to be produced by tabulation devices”, SLI believes that the pertinent requirements associated to this sub-requirement should be explicitly called out. A vague reference will only create gaps in coverage.

For the requirement 2.6.2 Electronic Records, which states, “The following requirements apply to records produced by the voting system for any exchange of information between devices, support of auditing procedures, or reporting of final results: b. Requirements for printed reports to support auditing steps”, SLI believes that the pertinent requirements associated to this sub-requirement should be explicitly called out. A vague reference will only create gaps in coverage.

For the requirements 2.6.2.3, which states, “The voting system SHALL be capable of producing a ballot image”, SLI believes that the test method should be such that it is consistent with 2.6.3.2, which is a similar requirement for paper record contents. As the expectation is the same for both, only the media format is different—the test method should be the same.

For the requirement 2.6.3.7.b Linking the electronic CVR to the paper record, which states, “Identify whether the paper record represents the ballot that was cast”, SLI would recommend replacing "Identify" with "Validate", as “Identify” seems somewhat ambiguous as phrased.

For the requirement 2.7.1.1 Network Monitoring, which states, “The system server SHALL provide for system and network monitoring during the voting period”, SLI

believes that more detail should be added as to what level of monitoring should be taking place. As written, this could be as minimal as, "the light is green, the system is up".

For the requirement 5.1.2.7 Monitoring voting system access, which states, “The (voting system) SHALL provide tools for monitoring access to the system. These tools SHALL provide specific users real time display of persons accessing the system as well as reports from logs”, SLI has concern for this requirement regarding whether it is feasible to monitor a globally distributed system, with potentially a very large set of users, especially to be done “real time”. A recommendation may be to verify that this data is captured in a log file.

For the requirement 5.1.2.11 Screen lock, which states, “Authenticated sessions on critical processes SHALL have a screen-lock functionality that can be manually invoked”, SLI believes that a related requirement is needed that calls out the need for re-authentication in order to re-access.

For the requirement 5.2.1.1 Strength of authentication, which states, “Authentication mechanisms supported by the voting system SHALL support authentication strength of at least 1/1,000,000”, SLI believes that this requirement should be referring to appropriate NIST SP, NIST 800-63 Electronic Authentication Guideline Standards.

For the requirement 5.2.1.5 Password reset, which states, “The voting system SHALL provide a mechanism to reset a password if it is forgotten, in accordance with the system access/security policy”, SLI believes that this covers passwords only. What if there are alternative methods of authentication? Consideration should be given to other potential authentication methods.

For the requirement 5.2.1.6 Password strength configuration, which states, “The voting system SHALL allow the administrator group or role to specify password strength for all accounts including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters per NIST 800-63 Electronic Authentication Guideline Standards”, SLI believes that this requirement should specify the authentication level as defined in the referenced NIST SP.

For the requirement 5.2.1.12 Message authentication, which states, “Message authentication SHALL be used for applications to protect the integrity of the message content using a schema with 112 bits of security”, SLI believes that the requirement needs to better define what is a "message", as used in the context of this requirement. The requirement should also specify if all data transmissions need to be authenticated, or just some subset.

For the requirement 5.2.1.13 Message authentication mechanisms, which states, “IPsec, SSL, or TLS and MAC mechanisms SHALL all be configured to be compliant with FIPS 140-2 using approved algorithm suites and protocols”, is the intent here to use current certified communication methodologies? If so, SLI believes this requirement would be better suited as an Inspection test method.

For the requirement 5.3.1.1 Cryptographic functionality, which states, “All cryptographic functionality SHALL be implemented using NIST-approved cryptographic algorithms/schemas, or use published and credible cryptographic algorithms/schemas/protocols”, SLI believes that "… or use published and credible cryptographic algorithms/schemas/protocols", is something that should be qualified by FVAP/NIST. Our preference is to not leave it to a VSTL to determine, or leave as a loophole for a manufacturer to argue.

For the requirement 5.3.2.4 Use NIST-approved key generation methods for communications, which states, “Cryptographic keys used to protect information in-transit over public telecommunication networks SHALL use NIST-approved key generation methods. If the approved key generation method requires input from a random number generator, then an approved (FIPS 140-2) random number generator SHALL be used”, SLI would like to see some verbiage regarding the use of third party Certificate Authorities, as we are concerned that manufacturers using a third party implementation will not be able to obtain the necessary documentation/proof, though providers like Verisign would normally be considered an industry standard.

For the requirement 5.4 Voting System Integrity Management, which states, “ This section addresses the secure deployment and operation of the voting system…”, SLI believes that this section does not adequately take “ballot delivery systems” into account. It would work better to have 5.4.1 be specific to vote capture devices, then have a section 5.4.2 that pertains to both vote capture devices and ballot delivery

systems, such as ballot integrity and Personally Identifiable Information (PII), and then a section 4.5.3 that accounts for all aspects of a voting system.

For the current requirement 5.4.1 Protecting the Integrity of the Voting System, SLI believes that an additional sub-requirement for non-repudiation issues is needed.

For the requirement 5.4.1.3 Cast vote storage, which states, “Cast vote data SHALL NOT be permanently stored on the vote capture device”, SLI believes that for the kiosk environment this requirement is adequate, though if this is ever applied beyond section 1.1.3 to personal computers being used as the vote capture device, there will likely be issues with regards to how the configuration is regulated.

For the requirement 5.4.1.4 Electronic ballot box integrity, which states, “The integrity and authenticity of the electronic ballot box SHALL be protected by means of a digital signature”, SLI believes additional definition detail of "electronic ballot box" is needed.

For the requirement 5.4.1.5 Malware detection, which states, “The voting system SHALL use malware detection software to protect against known malware that targets the operating system, services, and applications”, SLI believes that more definition is needed to quantify the level of protection needed. This should potentially address a hardware/software malware detection solution, instead of just software.

For the requirement 5.4.1.6 Updating malware detection, which states, “The voting system SHALL provide a mechanism for updating malware detection signatures”, SLI believes that a follow-on requirement would be to have the manufacturer specify in their documentation (i.e., an Inspection test method) the recommended interval for requiring updated signatures.

For the requirement 5.4.1.7 Validating software on kiosk voting devices, which states, “The voting system SHALL provide the capability for kiosk workers to validate the software used on the vote capture devices as part of the daily initiation of kiosk operations”, SLI believes this requirement needs to be expanded to cover

all associated devices at the kiosk location. Some systems contain additional devices.

For the requirement 5.5 Communications Security, which states, “This section provides requirements for communications security. These requirements address ensuring the integrity of transmitted information and protecting the voting system from external communications-based threats”, SLI believes that some of the requirements in this section appear to explicitly call out specific communication protocols, which could be interpreted to exclude all other like communication protocols, such as 5.5.1.2, 5.5.1.3.

For the requirement 5.5.1.1 Data integrity protection, which states, “Voting systems that transmit data over communications links SHALL provide integrity protection for data in transit through the generation of integrity data (digital signatures and/or message authentication codes) for outbound traffic and verification of the integrity data for inbound traffic”, SLI believes that this requirement should be broken out to handle outbound versus inbound traffic separately.

For the requirement 5.5.1.5 Mutual authentication required, which states, “Each device SHALL mutually strongly authenticate using the system identifier before additional network data packets are processed”, SLI believes that appropriate NIST publication (SP 800-63) should be referenced to more clearly define "mutually strongly authenticate".

For the requirement 5.5.1.6 Secrecy of ballot data, which states, “Data transmission SHALL preserve the secrecy of voters’ ballot selections and SHALL prevent the violation of ballot secrecy and integrity”, SLI believes that it should be more clearly stated that voter data is to be encrypted. "Preserve the secrecy …", creates ambiguity.

For the requirement 5.5.2.2 Minimizing interfaces, which states, “The number of active ports and associated network services and protocols SHALL be restricted to the minimum required for the voting system to function”, SLI believes that the test method “Inspection/Vulnerability” needs to be defined, as Vulnerability is not listed anywhere; only Inspection and Functional are currently defined.

For the requirement 5.6.1.1 Default settings, which states, “The voting system SHALL implement default settings for secure log management activities, including log generation, transmission, storage, analysis, and disposal”, SLI believes the term "default settings" is ambiguous, and that it should be replaced with "minimal settings" as per NIST SP 800-92.

For the requirement 5.6.1.2 Log access, which states, “Logs SHALL only be accessible to authorized roles”, SLI believes the term "authorized roles" is undefined within the requirements. This should be more clearly defined as to what types of roles should be considered authorized.

For the requirement 5.6.1.3 Log access, which states, “The voting system SHALL restrict log access to append-only for privileged logging processes and read-only for authorized roles”, SLI believes the term "privileged logging processes" is undefined within the requirements. This should be more clearly defined as to which logging processes should be considered privileged, versus which ones are not.

For the requirement 5.6.1.8 Log preservation, which states, “All logs SHALL be preserved in a useable manner prior to voting system decommissioning”, SLI believes the term "prior to voting system decommissioning" is ambiguous. We believe the intent is that the log data remains intact for the life cycle of the given election data for a particular election. This may be defined at the jurisdictional level.

For the requirement 5.6.1.12 System clock security, which states, “Only the system administrator SHALL be permitted to set the system clock”, SLI would recommend that the "system administrator" role be changed to indicate an appropriately authorized election official.

For the requirement 5.6.2.2 Log content, which states, “The communications log SHALL contain at least the following entries”, SLI believes that the Test Method should be Inspection, as this deals more with what the systems does each time as opposed to what can be made to happen given a certain set of circumstances.

For the requirement 5.6.3.2 Critical events, which states, “All critical events SHALL be recorded in the system event log”, SLI believes that definition of a critical event is

needed. The requirement as it is now leaves room for interpretation in regards to the scope of the requirement. The opportunity for ambiguity should be removed as much as possible.

For the requirement 5.6.3.3 System events, which states, “At a minimum the voting system SHALL log the events described in Table 5-2”, the requirement only states "voting system", which is a broad scope of equipment and software. This should clarify whether this applies to the operating system, the voting system application, or both. If applicable to the operating system, some of these events will generate very large files that will tend to be unusable.

A general recommendation for the requirement 5.6.3.3 table is that the term "include but not limited to" be avoided, as this term creates ambiguity and potential for inconsistent interpretation of the requirement.

A general recommendation for the requirement 5.6.3.3 table would be to enumerate each discrete item. Making reference to items in the current format is very difficult.

For the requirement 5.6.3.3, the System Event, Critical system status messages, needs more detail. Criteria are needed to define what is considered critical; "includes but not limited to" creates a large potential for gaps to occur, as well as disagreements by a manufacturer as to what is deemed critical. Also, diagnostics and status messages upon startup do not seem to be critical type messages. Items such as physical security violations, failed login attempts to system critical applications, communications failures, database crc type failures, attempts to exceed privileges, etc. would seem to be critical type messages.

For the requirement 5.6.3.3, the System Event, - Non-critical status messages “Non-critical status messages that are generated by the data quality monitor or by software and hardware condition monitors”, SLI believes there is a need for better criteria for determining what are non-critical versus what are critical status messages.

Also, there is a need for clarification as to what is meant by "data quality monitor". This term seems open to interpretation and is likely to cause significant disagreement as to what is included.

For the requirement 5.6.3.3, the System Event, Shutdown and restarts “Both normal and abnormal shutdowns and restarts”, SLI would recommend adding "Power up" to this line item.

For the requirement 5.6.3.3, the System Event, Changes to system configuration settings, “configuration settings include but are not limited to registry keys, kernel settings, logging settings, and other system configuration settings”, SLI would recommend additional specificity, rather than alluding to "…other system configuration settings".

For the requirement 5.6.3.3, the System Event, The addition and deletion of files, which states, “Files added or deleted from the system”, SLI would recommend additional detail as to file types. The blanket statement of any and all files within a system, if interpreted at the operating system level would encompass transitory type files. We would not recommend having to track temporary files that are automatically handled within the system.

For the requirement 5.6.3.3, the System Event, Access control related events, which states, “Includes but not limited to: …”, SLI would recommend removal of "and underlying system resources" in the third bullet, as this is beyond the scope of the voting system application’s logging scope. Attempting to log all access attempts to all system resources will generate huge files that will be unusable.

For the requirement 5.6.3.3, the System Event, Installation, upgrading, patching, or modification of software or firmware, which states, “Logging for installation, upgrading, patching, or modification of software or firmware include logging what was installed, upgraded, or modified as well as a cryptographic hash or other secure identifier of the old and new versions of the data”, SLI notes that the potential scope is very large. In an initial certification upgrading, patching, and /or modification may well not be available. Additionally, "Cryptographic hash" needs to be defined. SLI would recommend using "hash code" instead, as it is a more accurate description of what should be produced. Also, the term “data” needs to be defined in the context of the requirement, as it is not necessarily clear what the target data is. This can be seen as the different versions of the software or firmware, or different versions of data that were modified during the install or upgrade process, or potentially something else.

For the requirement 5.6.3.3, the System Event, Changes to configuration settings “Changes to configuration settings Includes but not limited to: Changes to critical function settings. At a minimum critical function settings include location of ballot definition file, contents of the ballot definition file, vote reporting, location of logs, and system configuration settings”, SLI believes this requirement should be split out to more explicitly address either voting system applications or the underlying operating system.

For the requirement 5.6.3.3, the System Event, Changes to cryptographic keys, which states, “At a minimum critical cryptographic settings include key addition, key removal, and re-keying”, SLI would recommend adding "key zeroization".

For the requirement 5.6.3.3, the System Event, Voting events, Includes: Opening and closing the voting period”, SLI would recommend including successful delivery of the appropriate ballot style to the voter.

For the requirement 5.7.1.1 Critical events, which states, “Manufacturers SHALL document what types of system operations or security events (e.g., failure of critical component, detection of malicious code, unauthorized access to restricted data) are classified as critical”, SLI would recommend that NIST/FVAP list minimum criteria of what should be classified as critical, in order to create consistency for this requirement. Also, we recommend removal of "e.g." and giving specific criteria that must be met.

For the requirement 5.8 Physical and Environmental Security, SLI would recommend that additional specificity be added to explicitly call out whether each requirement is for the voting system (election creation machines and accumulation /tallying central servers included), or just the vote capture device.

For the requirement 5.8.2.1 Non-essential ports, which states, “The voting system SHALL disable physical ports and access points that are not essential to voting operations, testing, and auditing”, SLI would recommend that "testing" be removed, as in a production environment, one would not want "test" ports/access points enabled.

For the requirement 5.8.3.1 Physical port shutdown requirement, which states, “If a physical connection between the vote capture device and a component is broken, the affected vote capture device port SHALL be automatically disabled”, SLI would recommend changing Test Method to Functional.

For the requirement 5.8.3.2 Physical component alarm requirement, which states, “The voting system SHALL produce a visual alarm if a connected component is physically disconnected”, SLI would recommend changing Test Method to Functional.

For the requirement 5.8.3.5 Physical port restriction requirement, which states, “Vote capture devices SHALL be designed with the capability to restrict physical access to voting device ports that accommodate removable media with the exception of ports used to activate a voting session”, SLI would note that if implementing with custom designed vote capture device this requirement is applicable. If implementing with COTS products, this would not be applicable.

For the requirement 5.8.3.6 Physical port tamper evidence requirement, which states, “Vote capture devices SHALL be designed to give a physical indication of tampering or unauthorized access to ports and all other access points, if used as described in the manufacturer’s documentation”, SLI would note that if implementing with custom designed vote capture device this requirement is applicable. If implementing with COTS products, this would not be applicable.

For the requirement 5.8.3.7 Physical port disabling capability requirement, which states, “Vote capture devices SHALL be designed such that physical ports can be manually disable by an authorized administrator”, SLI would note that if implementing with custom designed vote capture device this requirement is applicable. If implementing with COTS products, this would not be applicable.

For the requirement 5.8.6.1 Secure physical lock access requirement, which states, “voting equipment SHALL be designed with countermeasures that provide physical indication that unauthorized attempts have been made to access locks installed for security purposes”, SLI would note that if implementing with custom designed voting equipment this requirement is applicable. If implementing with COTS products, this would not be applicable. Also, “voting equipment” should be defined as to whether

this is only vote capture device equipment, or every piece of equipment within the voting system.

For the requirement 5.8.7 Media Protection, which states, “These requirements apply to all media, both paper and digital, that contain personal privacy related data or other protected or sensitive types of information”, SLI would recommend changing "personal privacy related data" to "personally identifiable information (PII)", which is a common industry term. Additionally, SLI would recommend changing the term “digital” to “electronic”, as it is more encompassing than “digital”, which by its definition excludes analog.

For the requirement/section 5.9 Penetration Resistance, SLI would recommend referencing a NIST Special Publication dealing with hardening.

For the requirement 5.9.1.1 Resistant to attempts, which states, “The voting system SHALL be resistant to attempts to penetrate the system by any remote unauthorized entity”, SLI would recommend defining resistance levels more definitively, utilizing appropriate NIST SP, and enumerating by device types and environments within a voting system.

For the requirement 5.9.1.2 System information disclosure, which states, “The voting system SHALL be configured to minimize ports, responses and information disclosure about the system while still providing appropriate functionality”, SLI would recommend defining "appropriate functionality" by device types and environments within a voting system. Also, we would recommend referencing a NIST SP dealing with hardening.

For the requirement 5.9.1.4 Interfaces, which states, “All interfaces SHALL be penetration resistant including TCP/IP, wireless, and modems from any point in the system”, SLI would recommend closing all ports and shutting down all services not needed to perform voting activities.

For the requirement 5.9.2 Penetration Resistance Test and Evaluation, SLI believes this section is oriented to the VSTL. As such, SLI would recommend that it not be in

the requirements document that manufacturers are held to, but in a "Program Manual" that outlines the scope of a certification campaign.

For the requirement 5.9.2.2 Test environment, which states, “Penetration testing SHALL be conducted on a voting system set up in a controlled lab environment. Setup and configuration SHALL be conducted in accordance with the TDP, and SHALL replicate the real world environment in which the voting system will be used”, SLI believes this requirement to be oriented to the VSTL, not the manufacturer. As such, SLI would recommend that it not be in the requirements document that manufacturers are held to, but in a "Program Manual" that outlines the scope of a certification campaign. Also, this may not be feasible for all systems. SLI has encountered systems that are cloud based, for example, which will be challenging to set up in a controlled lab environment.

For the requirement 5.9.2.3 White box testing, which states, “The penetration testing team SHALL conduct white box testing using manufacturer supplied documentation and voting system architecture information. Documentation includes the TDP and user documentation. The testing team SHALL have access to any relevant information regarding the voting system configuration. This includes, but is not limited to, network layout and Internet Protocol addresses for system devices and components. The testing team SHALL be provided any source code included in the TDP”, SLI believes this requirement to be oriented to the VSTL, not the manufacturer. As such, SLI would recommend that it not be in the requirements document that manufacturers are held to, but in a "Program Manual" that outlines the scope of a certification campaign.

For the requirement 5.9.2.4 Focus and priorities, which states, “Penetration testing seeks out vulnerabilities in the voting system that might be used to change the outcome of an election, interfere with voter ability to cast ballots, ballot counting, or compromise ballot secrecy. The penetration testing team SHALL prioritize testing efforts based on the following:…”, SLI believes this requirement to be oriented to the VSTL, not the manufacturer. As such, SLI would recommend that it not be in the requirements document that manufacturers are held to, but in a "Program Manual" that outlines the scope of a certification campaign.

The following comments/observations are not directly tied to a comment, but are a higher level recommendation.

For Accuracy testing, SLI would recommend that from a physical level, accuracy is determined by ensuring that the device accurately records data input over vendor specified maintenance cycles. Examples include touch screen inputs for the number of ballots cast specified by the vendor prior to the need for recalibration; the maximum number of ballots scanned prior to needing to clean the optical scanner; or, the maximum number of ballots printed by a printer prior to replacing toner.

SLI would recommend creating accuracy requirements that deal with a more focused approach: creating election/ballots, accurate for full marks, accurate for partial marks (NIST defined minimum acceptable % of oval), each device, etc.

SLI would recommend that all devices within a voting system, including items such as Smart card and bar code readers should also be validated for accuracy and performance against vendor specified maintenance cycles.

SLI would recommend Central Count scanners be considered for ballot delivery systems.

SLI would recommend consideration in requirements accounting for differences between internet software vote capture implementations versus physical hardware based vote capture, or a hybrid of the two. (Consider printer, FAX and email, as well as scanning and automatic internet transmission).

SLI would recommend that for operating capacities, FVAP specify minimums for both polling place environments (e.g., clients) as well as at central count locations (e.g., servers). Consideration should be given to concurrent jurisdictions and users, as well as minimal acceptable response times. Potentially different classes of servers and how they scale up should also be considered.

SLI would recommend maximum capacities be defined for each component in the system in terms of realistic numbers that take into account limiting factors such as memory, throughput, disk space, etc. Too often manufacturers will claim a

maximum that is based on a theoretical limit, for example a double byte variable, which would put the maximum in the millions.

4.3 What Documentation is needed and why

In this section, we look at how documentation affects the ability to validate the requirements, whether the test method is Inspection or Functional. The intention of this section is to highlight the critical nature of adequate documentation in a formal compliance campaign. The level of complexity employed by today's internet voting systems only increases the need for appropriate documentation. Nowhere is this more visible than in the area of security. The ability to determine how security is implemented in every aspect of a voting system is greatly influenced by the documentation and how it outlines processes, procedures, methodologies, standards and algorithms employed.

In the ensuing discussions, we use the terms "logical review" and "physical review". "Logical review" is used to mean referencing of documentation to gain an understanding of the voting system under test. "Physical review" refers to the validation of a requirement, whether the test method is Inspection or Functional.

4.3.1 Section 2.1 Functional Requirements, Accuracy

This subsection contains logical as well as physical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine many aspects of the Accuracy requirements that are dependent on sufficient documentation to allow an election to be accurately created and render correct results. Several of the requirements need documentation that describes how hardware aspects of the system will meet accuracy requirements. There are additional physical reviews within this section that are dependent on documentation to detail what shall be recorded accurately as well as reported accurately, i.e. not only will voters' selections be accurately recorded, but accumulated votes will be accurately reported, etc. While many of the requirements have test methods that read as Functional, the ability to functionally test these requirements relies heavily on appropriate documentation that details how the pertinent aspect of the requirement is met, as implemented by the specific manufacturer.

4.3.2 Section 2.2 Functional Requirements, Operating Capacities

This subsection contains logical as well as physical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine the maximum operating capacities of various aspects of the system so they can be validated. There are additional physical reviews

within this section that are dependent on documentation that details how notice is provided when a capacity limit is being approached, how the system prevents data loss in the event of simultaneous transmissions, etc. While many of the requirements have test methods that read as Functional, the ability to functionally test these requirements relies heavily on appropriate documentation that details how the pertinent aspect of the requirement is met, as implemented by the specific manufacturer.

4.3.3 Section 2.3 Functional Requirements, Pre-Voting Capabilities

This subsection contains logical as well as physical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine how jurisdictional data is kept separate, how data is imported, what features are supported by the system, and how the data is protected. There are additional physical reviews within this section that are dependent on documentation that details how test modes are provided such that the system can be validated for readiness of use, and how the test data is to be segregated from actual vote data, etc. While many of the requirements have test methods that read as Functional, the ability to functionally test these requirements relies heavily on appropriate documentation that details how the pertinent aspect of the requirement is met, as implemented by the specific manufacturer.

4.3.4 Section 2.4 Functional Requirements, Voting Capabilities

This subsection contains logical as well as physical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine how the voting period is opened, how the voter receives their ballot, what their options are while voting, how selections are verified prior to casting of the ballot, and how the ballot is cast. There are additional physical reviews within this section that are dependent on documentation that details how voter identification is linked, or not linked, to their ballot, and how the links are removed, as well as when. While many of the requirements have test methods that read as Functional, the ability to functionally test these requirements relies heavily on appropriate documentation that details how the pertinent aspect of the requirement is met, as implemented by the specific manufacturer.

4.3.5 Section 2.5 Functional Requirements, Post-Voting Capabilities

This subsection contains logical as well as physical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine how the vote data is stored in the electronic ballot box, how the box is retrieved, and how the data is accumulated. There are

additional physical reviews within this section that are dependent on documentation that details how tabulated data is reported and in what format. While many of the requirements have test methods that read as Functional, the ability to functionally test these requirements relies heavily on appropriate documentation that details how the pertinent aspect of the requirement is met, as implemented by the specific manufacturer.

4.3.6 Section 2.6 Functional Requirements, Audit and Accountability

This subsection contains logical as well as physical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine what types of records are kept with what data such that any and all events of an election can be reproduced. While many of the requirements have test methods that read as Functional, the ability to functionally test these requirements relies heavily on appropriate documentation that details how the pertinent aspect of the requirement is met, as implemented by the specific manufacturer.

4.3.7 Section 2.7 Functional Requirements, Performance Monitoring

This subsection contains logical as well as physical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine how the system is monitored, what specifically is monitored, as well as how private or sensitive data is protected from access. The ability to functionally test these requirements relies heavily on appropriate documentation that details how the pertinent aspect of the requirement is met, as implemented by the specific manufacturer.

4.3.8 Section 5.1 Security, Access Control

4.3.8.1 Subsection 5.1.1 Separation of duties

This subsection contains logical as well as physical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine who has what duties and the limitations of each role/group/user. There are additional physical reviews within this section that are dependent on documentation that details how the system will conduct its processes and procedures that are applicable to access control, i.e. what control mechanisms are implemented, and how they are implemented to allow authorized access by what groups to election data, as well as how multiple personnel will be employed to access critical data and processes, etc. While many of the requirements have test methods that read as Functional, the ability to functionally test these requirements relies

heavily on appropriate documentation that details how the pertinent aspect of the requirement is met, as implemented by the specific manufacturer.

4.3.8.2 Subsection 5.1.2 Voting System Access

This subsection contains logical as well as physical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine how the system will identify and authenticate users/roles/groups. There are additional physical reviews within this section that are dependent on documentation that details how the system will conduct its processes and procedures that are applicable to access control, i.e. what control mechanisms are implemented, and how they are implemented to allow authorized access, as well as prevent unauthorized, or how is privilege escalation prevented, what types of events are to be logged and where they are is logged, how access failures are handled by the system, etc. While many of the requirements have test methods that read as Functional, the ability to functionally test these requirements relies heavily on appropriate documentation that details how the pertinent aspect of the requirement is met, as implemented by the specific manufacturer.

4.3.9 Section 5.2 Security, Identification and Authentication

4.3.9.1 Subsection 5.2.1 Authentication

This subsection, while consisting of Functional test methods, contains logical as well as physical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine what types of authentication mechanisms are in place, strength of those mechanisms, and authentication methods employed for each defined group or role. Detail is also needed to understand how passwords are employed within the system as well as how any related data is stored. There are additional physical reviews within this section that are dependent on documentation that details how devices are protected by authentication, how networks are protected and how all messaging over those networks is authenticated. This documentation is required before any functional test can be created. The ability to functionally test these requirements relies heavily on appropriate documentation that details how the pertinent aspect of the requirement is met, as implemented by the specific manufacturer.

4.3.10 Section 5.3 Security, Cryptography

4.3.10.1 Subsection 5.3.1 General Cryptography Requirements

This subsection contains primarily logical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine how cryptography is implemented, what are the pertinent standards followed, as well as the strength employed. The ability to test these requirements, by Inspection relies heavily on appropriate documentation that details how the pertinent aspect of the requirement is met, as implemented by the specific manufacturer.

4.3.10.2 Subsection 5.3.2 Key Management

This subsection contains primarily logical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine how keys are generated, what strength generation methods are deployed, what are the pertinent standards followed, as well as how they are employed. The ability to test these requirements by Inspection relies heavily on appropriate documentation that details how the pertinent aspect of the requirement is met, as implemented by the specific manufacturer.

4.3.10.3 Subsection 5.3.3 Key Establishment

This subsection contains primarily logical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine how keys are established within the system. The ability to test these requirements by Inspection relies heavily on appropriate documentation that details how the pertinent aspect of the requirement is met, as implemented by the specific manufacturer.

4.3.10.4 Subsection 5.3.4 Key Handling

This subsection contains logical as well as physical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine how keys are stored and zeroed out as well as how keys can be reset. The ability to test these requirements, by Inspection or Functional test, relies heavily on appropriate documentation that details how the pertinent aspect of the requirement is met, as implemented by the specific manufacturer.

4.3.11 Section 5.4 Security, Voting System Integrity Management

4.3.11.1 Subsection 5.4.1 Protecting the Integrity of the Voting System

This subsection contains logical as well as physical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine how vote data is protected during transmissions and while in storage, as well as where it can and cannot be stored. There are additional physical reviews within this section that are dependent on documentation that details how malware is detected as well as how that malware protection is updated, i.e., what voting system devices are applicable, and how they are implemented to each device. While many of the requirements have test methods that read as Functional, the ability to functionally test these requirements relies heavily on appropriate documentation that details how the pertinent aspect of the requirement is met, as implemented by the specific manufacturer.

4.3.12 Section 5.5 Security, Communications Security

4.3.12.1 Subsection 5.5.1 Data Transmission Integrity

This subsection contains logical as well as physical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine how the data is protected during transmission, what types of protocols are implemented. There are additional physical reviews within this section that are dependent on documentation that details how standards are implemented, how each device within a system utilizes unique identifiers, how mutual authentication is employed, i.e., what identifiers are used to logically and uniquely identify a vote capture device, and how they are implemented to be utilized as part of the mutual authentication process when data is be transmitted, etc. While many of the requirements have test methods that read as Functional, the ability to functionally test these requirements relies heavily on appropriate documentation that details how the pertinent aspect of the requirement is met, as implemented by the specific manufacturer.

4.3.12.2 Subsection 5.5.2 External Threats

This subsection contains logical as well as physical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine what protections are used to protect the voting system against external threats and how they are implemented. There are additional physical reviews within this section that are dependent on documentation that details how interfaces are minimized and disabled, i.e.

what port is used to transmit data, and how other ports are disabled to prevent unauthorized access, etc. While many of the requirements have test methods that read as Functional, the ability to functionally test these requirements relies heavily on appropriate documentation that details how the pertinent aspect of the requirement is met, as implemented by the specific manufacturer.

4.3.13 Section 5.6 Security, Logging

4.3.13.1 Subsection 5.6.1 Log Management

This subsection contains logical as well as physical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine what information is to be logged, where it is to be logged, how it is logged and who has access to view the logs. There are additional physical reviews within this section that are dependent on documentation that details how logs are to be separated by jurisdiction, how they will be preserved, as well as what types of events are to be logged. While many of the requirements have test methods that read as Functional, the ability to functionally test these requirements relies heavily on appropriate documentation that details how the pertinent aspect of the requirement is met, as implemented by the specific manufacturer.

4.3.13.2 Subsection 5.6.2 Communications Logging

This subsection contains logical as well as physical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine what types of communications are logged, how they are logged, what is logged and where they are logged. While many of the requirements have test methods that read as Functional, the ability to functionally test these requirements relies heavily on appropriate documentation that details how the pertinent aspect of the requirement is met, as implemented by the specific manufacturer.

4.3.13.3 Subsection 5.6.3 System Event Logging

This subsection contains logical as well as physical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine what events are logged and how they are described, as well as what their status is considered within the voting system. There are additional physical reviews within this section that are dependent on documentation that details where the logs are kept, how they

can be accessed and what content is expected in each log, i.e. what is critical versus what is communication versus what is an error or exception message, and how they are implemented to which log, as well as any codes that identify the issue, etc. While many of the requirements have test methods that read as Functional, the ability to functionally test these requirements relies heavily on appropriate documentation that details how the pertinent aspect of the requirement is met, as implemented by the specific manufacturer.

4.3.14 Section 5.7 Security, Incident Response

4.3.14.1 Subsection 5.7.1 Incident Response Support

This subsection contains logical as well as physical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine what system operations or security events the voting system considers to be a critical event, as well as how appropriate personnel will be notified of a critical event occurrence. The ability to functionally test these requirements relies heavily on appropriate documentation that details how the pertinent aspect of the requirement is met, as implemented by the specific manufacturer.

4.3.15 Section 5.8 Security, Physical and Environmental Security

4.3.15.1 Subsection 5.8.1 Physical Access

This subsection contains logical as well as physical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine what manner of physical evidence is produced to determine unauthorized access. The ability to functionally test these requirements relies heavily on appropriate documentation that details how the pertinent aspect of the requirement is met, as implemented by the specific manufacturer.

4.3.15.2 Subsection 5.8.2 Physical Ports and Access Ports

This subsection contains logical as well as physical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine what ports on devices within the voting system are essential for each activity within the system and which are not, and how to disable the nonessential. The ability to functionally test these requirements relies heavily on appropriate documentation that details how the pertinent

aspect of the requirement is met, as implemented by the specific manufacturer.

4.3.15.3 Subsection 5.8.3 Physical Port Protection

This subsection contains logical as well as physical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine how a port is shut down if a disconnection occurs, how appropriate personnel will be notified, how and what will be logged in an appropriate log file, as well as how a port can be reactivated by authorized personnel. There are additional physical reviews within this section that are dependent on documentation that details how ports can be manually disabled by authorized personnel, etc. The ability to functionally test these requirements relies heavily on appropriate documentation that details how the pertinent aspect of the requirement is met, as implemented by the specific manufacturer.

4.3.15.4 Subsection 5.8.4 Door Cover and Panel Security

This subsection contains logical as well as physical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine how a vote capture device is configured to prevent and detect tampering attempts such that workers can monitor the kiosk location. The ability to functionally test these requirements relies heavily on appropriate documentation that details how the pertinent aspect of the requirement is met, as implemented by the specific manufacturer.

4.3.15.5 Subsection 5.8.5 Secure Paper Record Receptacle

This subsection contains logical as well as physical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine how the receptacle is configured to provide physical evidence of unauthorized access attempts. The ability to functionally test these requirements relies heavily on appropriate documentation that details how the pertinent aspect of the requirement is met, as implemented by the specific manufacturer.

4.3.15.6 Subsection 5.8.6 Secure Physical Lock and Key

This subsection contains logical as well as physical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine how and where locks are employed, as well as how they are configured to provide physical evidence of any tampering attempts. The ability to functionally test these requirements relies heavily on

appropriate documentation that details how the pertinent aspect of the requirement is met, as implemented by the specific manufacturer.

4.3.15.7 Subsection 5.8.7 Media Protection

This subsection contains logical as well as physical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine how all forms of media that contain sensitive data are protected from unauthorized access, modification or disclosure. The ability to functionally test these requirements relies heavily on appropriate documentation that details how the pertinent aspect of the requirement is met, as implemented by the specific manufacturer.

4.3.16 Section 5.9 Security, Penetration Resistance

4.3.16.1 Subsection 5.9.1 Resistance to Penetration Attempts

This subsection contains logical as well as physical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine resistance to unauthorized access attempts, disclosure of all system information, as well as resistance of ports to all unauthorized penetration attempts. The ability to functionally test these requirements relies heavily on appropriate documentation that details how the pertinent aspect of the requirement is met, as implemented by the specific manufacturer.

4.3.16.2 Subsection 5.9.2 Penetration Resistance Test and Evaluation

This subsection contains logical as well as physical reviews of the requirements. The logical review occurs where appropriate documentation is needed to determine potential access points within the voting system. A lack of documentation prevents the reviewer from fully understanding how the system is implemented, thereby reducing the effectiveness of the penetration test attempts. The ability to fully functionally test these requirements relies heavily on appropriate documentation that details how the pertinent aspect of the requirement is met, as implemented by the specific manufacturer.

4.4 Full Systems

For this project, two manufacturers delivered systems for full, in-house, system testing, which consisted of evaluation of each system against sections 2 (Functional) and 5 (Security). The two systems submitted were in several important ways a study in different technologies employed.

Both full systems contained the ability to import/create/modify election definitions, as well as conducting the voting, accumulating and tallying of results. Each portion of the system was subjected to Sections 2 and 5, as applicable.

Manufacturer 1 delivered 3 basic functionality documents and 2 security documents.

Manufacturer 2 delivered 9 basic functionality documents and 9 security documents.

4.5 EVSWs

For this project five systems were delivered for testing, which consisted of evaluation of each system against section 5 (Security). Two manufacturers provided "back office" environments, upon which their server side applications run. Three manufacturers provided only remote access to their systems, one with limited access to their back office applications. None of the manufacturers supplied kiosk location hardware setups. SLI used our own hardware as vote capture devices, in conjunction with each manufacturer's voting implementation. All the EVSW manufacturers are relying on commercial off the shelf products to be supplied as the voter capture device. Only one EVSW manufacturer had any documentation on hardening of the vote capture device.

Manufacturer 3 did provide a setup for their back office applications that was used locally by SLI, though not all applications or features were made available. In some instances the user roles made available had limited access to functionality such that we were not able to fully execute all functionality within the system.

Manufacturer 3 delivered 3 basic functionality documents and 2 security documents.

Manufacturer 4 did not provide a setup for their back office applications to be used locally by SLI. Manufacturer 4 did supply some credentials to access their system remotely, though not all applications or features were made available. In some instances the user roles made available had limited access to functionality such that we were not able to fully execute all functionality within the system.

Manufacturer 4 delivered 5 basic functionality documents and 0 security documents. Manufacturer 4 stated that the environment is secure due to the operating system employed.

Manufacturer 5 did not provide a setup for their back office applications to be used locally by SLI. Manufacturer 5 did supply some credentials to access their system remotely, though not all applications or features were made available. In some instances the user roles made available had limited access to functionality such that we were not able to fully execute all functionality within the system.

Manufacturer 5 delivered 2 basic functionality documents and 0 security documents. Manufacturer 5 did deliver one third party white paper that gave high level concepts of security implemented within the provided environment, in which the manufacturer's application resides. Manufacturer 5 was not able to meet with SLI for remote support testing.

Manufacturer 6 did not provide a setup for their back office applications to be used locally by SLI. Manufacturer 6 did not supply credentials to access their system remotely and consequently we were not able to fully execute all functionality within the system.

Manufacturer 6 delivered 2 basic functionality documents and 0 security documents. Manufacturer 6 did deliver one 2-page document, in response to our request for Security documentation, that touched on how the technologies used in their system inherently provide security such that they had no need for further implementations

or documentation. Manufacturer 6 was not able to meet with SLI for remote support testing.

Manufacturer 7 did provide a setup for their back office applications that was used locally by SLI, though not all applications or features were made available. In some instances the user roles made available had limited access to functionality such that we were not able to fully execute all functionality within the system.

Manufacturer 7 delivered 3 basic functionality documents and 1 security document. Manufacturer 7's delivered security documentation did not provide all the needed information. Manufacturer 7 did meet with SLI for a limited remote support testing.

4.6 Test Results Summary

SLI reviewed each manufacturer's provided documentation to assess its contents in regards to the requirements, in **UOCAVA Pilot Program Testing Requirements** Section 2: Functional Requirements and Section 5: Security for the full systems, and Section 5 for the EVSWs.

The review was conducted for adequate content and format of the systems' features in regards to creating/importing election definitions. The intent here was to provide the manufacturer with an assessment of the state of their documentation in regards to what would be expected in an actual certification.

SLI performed tests on each manufacturer's provided system. The testing incorporated end-to-end election scenarios testing the functionality supported by the manufacturer.

The following results were used in both the documentation review and the functional testing to describe the outcome of the pertinent review.

- Passed indicates that sufficient functionality was found such that the requirement is considered met.

- Insufficient Robustness indicates that a sufficient amount of functionality was not found such that the requirement is not considered to be fully met. In a strict pass/fail environment, this would be seen as a fail.
- Not Tested indicates that while functionality should be in place to cover the requirement, either access to the functionality was not provided, or documentation was insufficient for indicating where and how the functionality was implemented.
- Not Applicable indicates that functionality was not in place, nor was required.

The following two tables break out the requirements to a level 2 heading (i.e. 2.1, 2.2, …) section. For each requirement, as defined by a requirement entry that contains a “SHALL”, we assigned percentages for “Passed”, “Failed”, “Untested” and “Not Applicable (NA)”. For any requirement to pass, it had to fully pass, including any pertinent sub requirements. If any sub requirement failed, the whole requirement failed.

The following table enumerates how each manufacturer fared against the section 2 Functional Requirements section

	Manufacturer 1	**Manufacturer 2**
2.1	% Passed: 88 % Failed: 0 % Untested: 12 % N/A: 0	% Passed: 88 % Failed: 0 % Untested: 12 % N/A: 0
2.2	% Passed: 75 % Failed: 25 % Untested: 0 % N/A: 0	% Passed: 75 % Failed: 25 % Untested: 0 % N/A: 0
2.3	% Passed: 50 % Failed: 50 % Untested: 0 % N/A: 0	% Passed: 50 % Failed: 50 % Untested: 0 % N/A: 0
2.4	% Passed: 67 % Failed: 22 % Untested: 0 % N/A: 11 Beyond scope (early voting)	% Passed: 67 % Failed: 22 % Untested: 0 % N/A: 11 Beyond scope (early voting)
2.5	% Passed: 100 % Failed: 0 % Untested: 0 % N/A: 0	% Passed: 100 % Failed: 0 % Untested: 0 % N/A: 0
2.6	% Passed: 46 % Failed: 8 % Untested: 46 No paper funcitonality % N/A: 0	% Passed: 75 % Failed: 8 % Untested: 17 Lack of information % N/A: 0
2.7	% Passed: 67 % Failed: 33 % Untested: 0 % N/A: 0	% Passed: 67 % Failed: 33 % Untested: 0 % N/A: 0

The following table enumerates how each manufacturer fared against the section 5 Security section:

	Manufacturer 1	Manufacturer 2	Manufacturer 3	Manufacturer 4	Manufacturer 5	Manufacturer 6	Manufacturer 7
5.1	% Passed: 42 % Failed: 53 % Untested: 5 % N/A: 0	% Passed:84 % Failed: 16 % Untested: 0 % N/A: 0	% Passed: 42 % Failed: 53 % Untested: 5 % N/A: 0	% Passed: 32 % Failed: 21 % Untested: 47 Lack of access % N/A: 0	% Passed: 37 % Failed: 5 % Untested: 58 Lack of access % N/A: 0	% Passed: 0 % Failed: 0 % Untested: 100 No Access Lack of access % N/A: 0	% Passed: 32 % Failed: 11 % Untested: 57 Lack of access % N/A:
5.2	% Passed: 8 % Failed: 46 % Untested: 38 Lack of Information % N/A: 8 No VPN	% Passed: 54 % Failed: 38 % Untested: 8 Time constraint % N/A: 0	% Passed: 8 % Failed: 46 % Untested: 38 Lack of Information % N/A: 8 No VPN	% Passed: 16 % Failed: 38 % Untested: 38 Lack of Information % N/A: 8 No VPN	% Passed: 8 % Failed: 38 % Untested: 46 Lack of Information % N/A: 8 No VPN	% Passed:16 % Failed: 16 % Untested: 60 Lack of Information Time constraint % N/A: 8 No VPN	% Passed: 38 % Failed: 11 % Untested: 23 Lack of Information % N/A: 8 No VPN
5.3	% Passed: 0 % Failed: 23 % Untested: 77 Lack of Information Lack of access % N/A: 0	% Passed: 0 % Failed: 23 % Untested: 77 Lack of Information Lack of access % N/A: 0	% Passed: 0 % Failed: 23 % Untested: 77 Lack of Information Lack of access % N/A: 0	% Passed: 54 % Failed: 0 % Untested: 46 Lack of Information Lack of access % N/A: 0	% Passed: 0 % Failed: 0 % Untested: 100 Lack of Information Lack of access % N/A: 0	% Passed: 0 % Failed: 0 % Untested: 100 Lack of Information Lack of access % N/A: 0	% Passed: 69 % Failed: % Untested: 31 Lack of Information Lack of access % N/A: 0
5.4	% Passed: 0 % Failed: 71 % Untested: 29 Lack of access % N/A: 0	% Passed: 23 % Failed: 77 % Untested: 0 % N/A: 0	% Passed: 0 % Failed: 71 % Untested: 29 Lack of access % N/A: 0	% Passed: 0 % Failed:43 % Untested: 57 Lack of Access % N/A: 0	% Passed: 57 % Failed: 0 % Untested: 0 % N/A: 43 Ballot Delivery System	% Passed: 0 % Failed: 71 % Untested: 0 % N/A: 29 Ballot Deliver System	% Passed: 0 % Failed: 14 % Untested: 43 Lack of access % N/A: 43 Ballot Deliver System

5.5	% Passed: 60 % Failed: 10 % Untested: 20 Lack of Information % N/A: 10 No VPN	% Passed: 30 % Failed: 10 % Untested: 60 VPN Block % N/A: 0	% Passed: 60 % Failed: 10 % Untested: 20 Lack of Information % N/A: 10 No VPN	% Passed: 30 % Failed: 10 % Untested: 50 Lack of access % N/A: 10 No VPN	% Passed: 40 % Failed: 10 % Untested: 40 Lackof Information % N/A: 10 No VPN	% Passed: 0 % Failed: 0 % Untested: 100 Lack of information % N/A: 0	% Passed: 40 % Failed: 0 % Untested: 70 Lack of access % N/A: 10 No VPN
5.6	% Passed: 24 % Failed: 71 % Untested: 5 Lack of access % N/A: 0	% Passed: 59 % Failed: 29 % Untested: 12 Lack of access % N/A:	% Passed: 24 % Failed: 71 % Untested: 5 Lack of access % N/A: 0	% Passed: 29 % Failed: 47 % Untested: 24 Lack of Information Lack of access % N/A: 0	% Passed: 18 % Failed: 47 % Untested: 35 Lack of Information Lack of access % N/A: 0	% Passed: 12 % Failed: 41 % Untested: 47 Lack of Information Lack of access % N/A: 0	% Passed: 35 % Failed: 30 % Untested: 35 Lack of Information Lack of access % N/A: 0
5.7	% Passed: 0% Failed: 100% Untested: 0% N/A: 0	% Passed: 50% Failed: 50 % Untested: 0% N/A: 0	% Passed: 0% Failed: 100% Untested: 0% N/A: 0	% Passed: 0% Failed: 100% Untested: 0% N/A: 0	% Passed: 0% Failed: 100% Untested: 0% N/A: 0	% Passed: 0% Failed: 100% Untested: 0% N/A: 0	% Passed: 0% Failed: 100% Untested: 0% N/A: 0
5.8	% Passed: 7 % Failed: 71 % Untested: 7 No Kiosk equipment % N/A: 15 No peripheral devices	% Passed: 50 % Failed: 29 % Untested: 21 No peripheral devices % N/A: 0	% Passed: 7 % Failed: 71 % Untested: 7 No Kiosk equipment % N/A: 15 No peripheral devices	% Passed: 0 % Failed: 7 % Untested: 86 Lack of Information Lack of Access No kiosk equipment % N/A: 7 Ballot Delivery system	% Passed: 14 % Failed: 29 % Untested: 50 Lack of Information Lack of Access No kiosk equipment % N/A: 7 Ballot Delivery system	% Passed: 0 % Failed: 0 % Untested: 93 Lack of Information Lack of Access No kiosk equipment % N/A: 7 Ballot Delivery system	% Passed: 0 % Failed: 14 % Untested: 79 Lack of Information Lack of Access No kiosk equipment % N/A: 7 Ballot Delivery system
5.9	% Passed: 75 % Failed: 8 % Untested: 0 % N/A: 17 VSTL oriented requirements	% Passed: 75 % Failed: 8 % Untested: 0 % N/A: 17 VSTL oriented requirements	% Passed: 75 % Failed: 8 % Untested: 0 % N/A: 17 VSTL oriented requirements	% Passed: 0 % Failed: 8 % Untested: 75 Lack of access % N/A: 17 VSTL oriented requirements	% Passed: 75 % Failed: 8 % Untested: 0 % N/A: 17 VSTL oriented requirements	% Passed: 0 % Failed: 8 % Untested: 75 Lack of access % N/A: 17 VSTL oriented requirements	% Passed: 0 % Failed: 8 % Untested: 75 Lack of access % N/A: 17 VSTL oriented requirements

Had all the needed documentation been received, as well as appropriate access to the entire environment, our expectation is that 80-85 percent of the current requirement set could be met as is. One item to take into consideration is the concept of the “Ballot Delivery System”. These types of systems will cause some of the requirement set to not be applicable, since they do not retrieve and store vote data.

We believe that with the incorporation of our recommended modifications, that 100 percent of the resulting requirement set could be met. Combining our previous experience as an EAC VSTL, testing traditional voting systems, with the experience of the hands on testing and review of the participating manufacturers, we have been to analyze the trends of this industry. As such, we took what we learned and made our recommendations for modifications to the requirement set, in an attempt to make the set more meaningful and applicable to the environment(s) which we see this industry moving towards.

4.6.1 Manufacturer 1

4.6.1.1 Evaluation of Testing

SLI performed tests on Manufacturer 1's provided system. The testing incorporated end-to-end election scenarios which tested the functionality denoted in section 2 of the requirements as implemented by Manufacturer 1.

The execution of the following test suites in relation to Manufacturer 1 included the following:

4.6.1.1.1 Readiness of the Voting System

This test is designed to validate, at a higher level, that the core functionality of a voting system is intact and functioning in a manner consistent with the expected implementation. The Readiness Test creates a baseline election and executes it in a basic Election Day scenario. This includes opening polls, voting ballots, closing polls, printing reports, transmitting results to pertinent locations unique to each system, and tallying results.

Testing was conducted to verify overall system readiness along with verifying the base level creation of an election definition, successful transmission and processing of ballot data. The testing successfully verified the system's capability of creating election data, opening polls, voting ballots, closing polls, printing reports, transmitting results and tallying. Additionally, ballot selections using write-ins, under votes, and voter updates were successfully cast and counted without error.

4.6.1.1.2 Section 2.1 - Accuracy

Data content accuracy was successfully verified in multiple stages ranging from creation/import of election definition, contest selections for each voter, and

verification with the final vote tabulation reports. This also included a close review of the consistency of content in which the automatic options, write-ins, and under-votes were confirmed to match in each stage. At no point was the voter identity made available as verified in the event logs.

For the given implementation, SLI was able to automate this test, such that a high volume of data was able to be processed. The implementation of Manufacturer 1's system, utilizing username/password combinations, allowed scripts to be created to interact with the system.

4.6.1.1.3 Section 2.2 – Operating Capacities

With the implementation of automated scripts, SLI was able to achieve high levels of data presentation to the accumulation center of Manufacturer 1, as was provided locally to SLI. The implementation used was not a production level system, and as such was not as fully robust a deployment as would be seen in a production environment. Nonetheless, while exercising the system for capacities, a situation was encountered where an accumulation application gave no indication that the tool was about to run out of memory, nor any indication that the file was too large for current operating parameters of the tool, when trying to decrypt a large file.

4.6.1.1.4 Section 2.3 – Pre-Voting Capabilities

The testing successfully verified the system's capability to create / import election data, ballot instructions and election rules. This process started with a clean laptop used for the generation of Public and Private Keys as well as the decryption of votes. The only programs installed on the hard drive are those required to encrypt and decrypt. Because this was a virtual testing environment it required the laptop be connected to the internet.

Before the election can be created/imported, it requires secure credential generation handle through a proprietary application, provided by Manufacturer 1. Manufacturer 1's application also handles the encryption and decryption of user credentials, election keys, and votes.

All necessary applications and third party products were successfully installed. Step-by-step procedures included:

- Installation of Manufacturer 1's application
- Installation of all third party applications
- Generation of all needed Credentials

- Election Key Generation
- Uploading New Voter Credentials to Manufacturer 1's application
- Create / Import Election (updates to Election)
- Access Election / Vote

One documentation issue encountered was that the documentation does not specify how to import the election definition. As such, we would recommend that Manufacturer 1 ensure that such documentation is in place prior to a certification effort.

4.6.1.1.5 Section 2.4 – Voting Capabilities

The testing successfully verified the system's capability to open polls, access the ballot, verify voter selections, and cast ballots. This was confirmed by a deployed voting verification service, which is a feature that enables a voter to confirm their vote has been received and counted. When a voter casts their ballot a receipt is displayed from which the voter is asked to note a confirmation number.

The vote verification service becomes available when the election reaches its reporting time after votes have been decrypted. The voters can return to the same URL they used to vote and instead of the election they will have the option of using the vote verification service system. The voter enters their pass code then compares the receipt displayed to them by the vote verification service with the one they were given when they voted. The two should match exactly. If the voter's receipt is re-created exactly as they saw it, then they can be confident that the Electoral Returning Officer and his/her official quorum of observers have decrypted the votes and counted them.

At no point was the voter identity made available as verified in the event logs. Voters in the event logs cannot be identified, nor votes viewed.

The decrypted ballots can be accessed and decrypted while the absentee election is still open, and if configured with an access time for counting the decrypted ballots, they can be uploaded, counted and partial totals posted while the election is still open. It can also be configured to not allow this to occur.

4.6.1.1.6 Section 2.5 – Post Voting Capabilities

While votes can be read and results obtained once the system finishes the decryption process, at no point could an individual's identity be traced to their ballot. It was not possible to determine a voter's selections before, during, or

after decryption. During the vote decryption process, after the close of voting, the private key was combined with other reference files to unlock the votes and produce readable election results. Reporting accuracy was confirmed by using the voter credentials against the expected returns to validate accuracy.

After election closed the post election process begins:

- Downloading the Encrypted Votes
- Vote Decryption
- Counting the Decrypted Votes
- Vote Tabulation
- Publishing the Report

Manufacturer 1 does encrypt with a public key. They are not using a digital signature but the process does check the integrity of the ballot box.

There is no specific procedure listed for the jurisdiction to access the electronic ballot box. They do require encryption judges to decrypt the votes.

4.6.1.1.7 Section 2.6 – Audit and Accountability

Manufacturer 1 does implement significant logging for audit and accountability, though some deficiencies were noted. In contests with multiple write-in fields, the totals of the names entered in each write-in field are tallied separately, and the totals from those multiple write-in fields are not tallied together. Another issue seen was that the system also records info in the HTTP logs on the Web Server, which are not set up with log rollover capabilities. Additionally, some of Manufacturer 1's tools do not implement log files, thus the tasks performed are not logged. For some of Manufacturer 1's applications, the logs saved do not record important events, e.g. poll opening/closings, IP addresses of accessing systems, and some errors.

There are two types of election in Manufacturer 1's system. The first type implements an election where the voter's choices are not transmitted to the back-end system, but must be printed or saved and then the printout is faxed, emailed or mailed in to be counted. The second type is an election where the voters' choices are automatically transmitted, via the internet, to the back-end system, but are not printed. As such, a paper record and its identifier will only exist if the first type of election is used.

Manufacturer 1's system's creation of a summary count record does not display a time, date, ballot type, voting location, or number of write-ins. There appears to be no means to support both a ballot printout, and electronically transmit the ballot to the Election Authority.

4.6.1.1.8 Section 2.7 – Performance Monitoring

Manufacturer 1's system did not provide any specific application for monitoring the network beyond the basic operating system tools Monitor Windows Server and Resource. As such, it was left to the operating system's inherent roles access features to prevent any unauthorized monitoring. No examples of being able to compromise either voter privacy or data integrity were discovered.

4.6.1.1.9 Section 3 - Access/Usability/Reliability

This portion of our review may be considered beyond the scope of review and results may not necessarily be indicative of actual system implementation.

Manufacturer 1's documentation details various distinct styles of elections conducted over the internet. Regardless of the access mechanism, the document states that the election and credentials are created in the same manner. Manufacturer 1 does not provide software or hardware to support a kiosk. No documentation provided addresses vote capture device accessibility. Manufacturer 1's documentation did not detail access to the voting system for voters with disabilities. No specification for floor space as related to the voting station is provided. The voting system does not provide the voter with the option to select black text on white background vs. white text on black background.

Manufacturer 1's internet voting interface provides visual instructions, not tactile. The vote capture device does provide instructions for all of its valid operations. Warnings and alerts issued by Manufacturer 1's vote capture device are distinguishable from other information and clearly state the nature of the problem, whether the voter has performed an invalid operation or whether the vote capture device has malfunctioned, and the set of responses available to the voter. Each distinct instruction is separated spatially from other instructions for visual interfaces. The use of color agrees with common conventions.

4.6.1.1.10 Section 5.1 Security, Access Control

Manufacturer 1's system supplied insufficient documentation to create user roles within the system. Manufacturer 1's system does not address the kiosk site. As

such, we would recommend that Manufacturer 1 ensure that such documentation is in place prior to a certification effort.

Voters could access their jurisdiction's election ballots and cast their vote at election time. The system implemented appropriate access control over each defined user/role/group.

While the requirements specify that the voting system shall require at least two persons from a predefined group for validating the election configuration information, accessing the cast vote records, and starting the tabulation process, Manufacturer 1's system allowed a single Election Official to change the election configuration.

Manufacturer 1's system did not time out an inactive voter following a specified period of inactivity; similarly with back office applications, an administrator was also allowed to remain logged into the application. The system also failed to log successful and unsuccessful logons. There was no preset number of logon failures to restrict access when the number of logon failures was exceeded.

4.6.1.1.11 Section 5.2 Security, Identification and Authentication

Documentation was provided that detailed authentication mechanisms implemented to support the voting system, though messaging schemas, algorithms or protocols lacked sufficient detail. Documentation was not sufficient for detailing secure storage of authentication data. As such, we would recommend that Manufacturer 3 ensure that such documentation is in place prior to a certification effort.

Functionally, two-factor authentication was not sufficient in some areas within the system. Password reset was of sufficient robustness. Password controls including password expiration, password history and password strength were insufficient or not verifiable.

4.6.1.1.12 Section 5.3 Security, Cryptography

Manufacturer 1's voting system documentation was insufficient in describing the cryptographic functionality used. As such, we would recommend that Manufacturer 1 ensure that such documentation is in place prior to a certification effort.

Additionally, other issues were found in Manufacturer 1's implementation of cryptography. The voting system uses a combination of Bouncy Castle and OpenSSL. Bouncy Castle does not currently hold a FIPS certification, which in

an actual UOCAVA certification effort would cause the voting system to not be compliant. The OpenSSL module does have several certifications from FIPS but information could not be acquired to adequately determine the certification in effect. The keys used on the voting system all comply with the required length of 112 bits.

The communications of the voting system use a Digital Certificate generated by one of the top commercial Certificate Authorities (CA). SLI recognizes these top commercial CAs to be accredited Certification Authorities (CAs) and therefore practicing within industry standards in regards to cryptographic functions performed internally by these commercial CAs.

Due to lack of specific information, the key generation methods, security of the key and Random Number Generator (RNG), seed key generation, communications key generation, health tests for the RNG, and key zeroization could not be adequately determined for compliance.

The system uses a manual key generation process; therefore, keys can be and are imputed and exported in plaintext. All keys are placed in a key container and are encrypted. Re-keying is supported within the election design software.

4.6.1.1.13 Section 5.4 Security, Integrity Management

Manufacturer 1 provided only limited information for Integrity Management. Vote integrity was not fully covered to adequately fulfill requirements. Storage and electronic ballot box integrity were not fully addressed. No documentation was provided on the handling of malware detection or upgrade capability. Validation of kiosk vote capture device software was not addressed. As such, we would recommend that Manufacturer 1 ensure that such documentation is in place prior to a certification effort.

Functionally, Manufacturer 1 did not provide adequate transmission integrity or storage of cast vote data. Access to remote server location was not provided, such that neither cast vote storage nor electronic ballot box integrity checks could be validated. Neither were checks for malware detection or upgrade mechanisms implemented as per Manufacturer 1. As such, we would recommend that Manufacturer 1 ensure that such environments are available for appropriate inspection in a certification effort.

4.6.1.1.14 Section 5.5 Communications Security

Manufacturer 1's documentation was not sufficient in detailing how the data transmission integrity is protected in terms of protocols, mutual authentication

methods, or interface protections. As such, we would recommend that Manufacturer 1 ensure that such documentation is in place prior to a certification effort.

Functionally, Manufacturer 1 did implement appropriate protocols and authentication methods.

4.6.1.1.15 Section 5.6 Security, Logging

Manufacturer 1's voting system documentation set did not sufficiently describe all system auditing procedures, configurations, or locations of the system audit logs. As such, we would recommend that Manufacturer 1 ensure that such documentation is in place prior to a certification effort.

The voting system is compliant logging power failures, abnormal shutdowns and restarts, removable media events, logon and logoff events, password changes, use of privileges, attempts to exceed privileges, access attempts to underlying resources, addition and deletion of users, format of logs, maintaining voter privacy, timekeeping mechanisms, and opening and closing Polls.

The voting system did not exhibit full compliance in logging error and exception messages, communications, critical system status messages, displaying the status of transmissions, events requiring election official intervention, changes to system configuration settings, integrity checks, addition or deletion of files, system readiness results, backup and restore, authentication events, access control events, user account activity, installing and upgrading software, changes to configuration settings, abnormal process exits, database events, changes to cryptographic keys, and voting events.

4.6.1.1.16 Section 5.7 Security, Incident Response

Manufacturer 1's documentation did provide a 'System Security Specifications' document, but there was no comprehensive list identifying what types of system operations or security events are classified as critical. As such, we would recommend that Manufacturer 1 ensure that such documentation is in place prior to a certification effort.

Manufacturer 1's system did not provide any alarms to be triggered during functional testing. With the current implementation of a browser implementation on a commercial off the shelf hardware component, in the kiosk location setup, this was not unexpected.

4.6.1.1.17 Section 5.8 Security, Physical and Environmental

Manufacturer 1's provided documentation did not include sufficient detail. Items lacking in the documentation include: there was neither comprehensive list identifying critical central server components nor the means by which unauthorized physical access could be recognized. There was no mention of disabling non-essential physical ports or access points. The documentation did not identify an event log or any event that would cause an entry to be written to an event log. The documentation did not provide guidelines for restricting physical access to ports supporting removable media which are not essential to the voting session. The documentation did not provide guidelines related to the recognition of physical tampering or unauthorized access to ports and all other access points.

The documentation did not include any guidelines as to the physical disabling of ports. The documentation provided did not detail the use of tamper evident or tamper resistant countermeasures. The documentation provided did not include guidelines related to physical security, tampering or tampering countermeasures. As such, we would recommend that Manufacturer 1 ensure that such documentation is in place prior to a certification effort.

During functional testing, disabled ports could only be re-enabled by an authorized administrator. An issue was discovered when a flash drive was plugged into an unused port and the device was accessible. The ability for the vote capture device to be automatically disabled if connections were broken with peripheral components was not able to be evidenced, as kiosk location equipment was not provided. Similarly for locks and seals--without delivered kiosk equipment, the placement of these items was not evidenced. As such, we would recommend that Manufacturer 1 be prepared to provide a full system environment, including hardware and all pertinent documentation, in a certification effort.

4.6.1.1.18 Section 5.9 Security, Penetration Resistance

With regard to the Penetration Resistance documentation, processes and procedures implemented by Manufacturer 1, resources provided were limited. No documentation was provided on how a system would be configured such that it would be resistant to unauthorized penetration attempts. As such, we would recommend that Manufacturer 1 ensure that such documentation is in place prior to a certification effort.

From a Functional perspective, Manufacturer 1 did not provide kiosk oriented hardware. Therefore, we were not able to exercise testing against a hardened

physical environment as would be recommended by Manufacturer 1. As such, we would recommend that Manufacturer 1 ensure such hardware is available for appropriate inspection in a certification effort.

From a Functional perspective, Manufacturer 1 was able to provide a local server, “backend” system for SLI to perform penetration testing. The system performed well. Only a minimal port set was left open, and those were configured in an appropriately positive manner to block exploitation attempts. 215 known exploits were successfully rebuffed. In terms of System Access and Interfaces, similar results were obtained: 253 exploits were attempted, with all being rebuffed. In terms of System Disclosure, when probed, the system did disclose the make and version of its web server. As such, we would recommend that Manufacturer 1 be prepared to provide a full system environment in a certification effort, though the testing that was performed on the provided equipment was successful overall in its security deployment.

White box testing was not implemented, as Manufacturer 1 did not provide source code to be reviewed as part of the white box testing effort.

4.6.1.1.19 Analysis of Manufacturer Assessment to the Requirements

For section 2 in terms of documentation, Manufacturer provided adequate documentation such that 88% of the requirements under review, would be considered to be met.

In terms of functionality, Manufacturer was evaluated at the following levels, for percentages of requirements being evaluated:

Passed: 87%

Insufficient Robustness: 12%

Not Tested: 1%

Not Applicable: 0%

In terms of documentation, Manufacturer provided adequate documentation such that 18% of the requirements under review, which consisted of Section 5, would be considered to be met.

In terms of functionality, Manufacturer was evaluated at the following levels, for percentages of requirements being evaluated:

Passed: 23%

Insufficient Robustness: 38%

Not Tested: 36%

Not Applicable: 3%

- Passed indicates that sufficient functionality was found such that the requirement is considered met.
- Insufficient Robustness indicates that a sufficient amount of functionality was not found such that the requirement is not considered to be fully met.
- Not Tested indicates that while functionality should be in place to cover the requirement, either access to the functionality was not provided, or documentation was insufficient for indicating where and how the functionality was implemented.
- Not Applicable indicates that functionality was not in place, nor was required.

4.6.2 Manufacturer 2

4.6.2.1 Evaluation of Testing

4.6.2.1.1 Readiness

This test is designed to validate, at a higher level, that the core functionality of a voting system is intact and functioning in a manner consistent with the expected implementation. The Readiness Test creates a baseline election and executes it in a basic Election Day scenario. This includes opening polls, voting ballots, transmitting results, closing polls, tallying results and printing reports.

Testing was conducted to verify overall system readiness along with verifying the base level creation of an election definition and successful transmission and processing of ballot data. The testing successfully verified the system's capability of creating election data, opening polls, voting ballots, closing polls, printing reports and transmitting results to the back end server for the final accumulation and tallying. Additionally, testing was successfully conducted with voters in multiple precincts in a single jurisdiction, provided a different set of races for each precinct. Lastly, ballot selections using write-ins and voter updates were successfully cast and counted without error.

4.6.2.1.2 Section 2.1 - Accuracy

Accuracy in this section pertains to the hardware, telecommunication, and the data content. Data content accuracy was successfully verified in multiple stages

ranging from comparisons of contest selections on the voting kiosk touch screen with the final paper printout for each voter to the printouts verified with the final tally. This also included a close review of the consistency of content in which both the automatic options and write-ins were confirmed to match in each stage. At no point was the voter identity made available and ballots were successfully provided in multiple languages and styles. Given the requirement of applying voting smartcards, it was not possible to automate the system, and as such all testing was performed manually.

4.6.2.1.3 Section 2.2 – Operating Capacities

Without the implementation of automated scripts, SLI was not able to achieve high levels of data presentation to the accumulation center of Manufacturer 2, as was provided locally to SLI. As such, while exercising the system for capacities, no situation was encountered that caused issues of concern to be raised.

4.6.2.1.4 Section 2.3 – Pre-Voting Capabilities

Import and verification of election detail was successful for the jurisdiction available for testing. Ballot content for different voters of different precincts was confirmed to be consistent with that defined for each associated precinct. Also, the ballot styles defined for each voter were consistent with that appearing in the authentication laptop when searching on voter IDs. Ballots cast during checking were successfully confirmed to appear in the separate database table, while the normal election votes appeared only in the results table of the same database. Lastly, the system tested did not support the use of image files.

4.6.2.1.5 Section 2.4 – Voting Capabilities

Ballots were successfully cast (and confirmed by the Log Viewer application), revoked and then unrevoked. Up to three changes were allowed in a ballot before the voter was required to submit a ballot. The behavior of the GUI was user-friendly when selecting and changing options in each race. A review of each group of selections produced a single sheet of paper listing the selections made, which matched the expected result.

When the selections were reviewed and printed, a single-character designation was incremented from A to B to C. This matched with that appearing on the final ballot receipt once cast. With each ballot cast there was a paper receipt for confirmation, instructions as to what to provide the voting official at the polling

location, and a unique ID to be used later for verifying the receipt of the vote by the casting board.

Tests of a single voter attempting to vote more than once generated the expected result on the voting kiosk. Prior to the back end service, the means was not available in the system to prevent a voter from casting a vote when an absentee ballot had already been processed for the same voter. Attempting to vote before the election opened or following the close of the election both produced appropriate error messaging. Otherwise, a timeout on the voting kiosk and other unsuccessful ballots cast generated error codes with no details as to what caused them. The only follow-through instructions provided to the voter were to contact an operator. One example was when a voter logged in before the election closed, made a few selections and then attempted to cast their ballot after the election closed.

For each voter logging onto the voting kiosk and casting a ballot, three records were generated in the database running on the back office laptop, which was confirmed through the Log Viewer GUI application running on the same laptop. The actions and voter identification associated with each record are correctly encrypted as viewed through both the Log Viewer and in the Results table of the database.

4.6.2.1.6 Section 2.5 – Post Voting Capabilities

The ballot box file generated on the back office laptop was successfully signed and sealed, then transported via USB flash drive to a second back office laptop where it was then processed and finally tabulated. The system did not provide a direct application for checking the ballot box integrity. However, the back office partially provides some of this functionality. Had the encrypted file been tampered with, the back office process would have failed.

Applying the closing token, along with the required service passwords, to open and decrypt the ballots worked successfully. The final tally file was successfully generated and is in a format easily viewed in any browser or migrated to many common applications for modification, and printed.

4.6.2.1.7 Section 2.6 – Audit and Accountability

The tallying process on the back office laptop successfully generated an HTML file, viewable in any browser, that lists the number of votes for each contest according to each precinct. That is, the HTML file lists a table for each precinct and in each table lists the votes for the contests that were available in the

associated precinct. The set of contests identified for each precinct in the HTML tally file matched with those identified in the paper printouts for the voters associated with the same precincts. Also, the vote count from the HTML tally file matched the vote count from the paper printouts for the accepted ballots minus the votes from the revoked ballots. Using the print option from the browser, the HTML tally file could easily be printed in an easily readable format matching that appearing on the computer screen. The tallying application could not directly print out the tally details.

Issues encountered included that the final tally file displayed a ballot count per precinct at the top of each precinct table, but did not differentiate whether they were the number received or counted. The final tally file did not display the number of rejected electronic cast vote records. Nor did the final tally file display the sum total of ballots counted and received for all of the precincts combined.

4.6.2.1.8 Section 2.7 – Performance Monitoring

Beyond the basic operating system tools available on each laptop there is no application for monitoring the network. Given this, a user with the logon and password combination to the back office laptops can apply the operating system commands necessary to view network activity. Applying passive monitoring commands will not compromise either voter privacy or election integrity. Applying commands that alter network service, like stopping the web server or altering the firewall configuration on the back office laptop, would only disrupt the service, but would neither jeopardize voter privacy nor the election integrity.

4.6.2.1.9 Section 3 - Usability/Accessibility/Privacy

This portion of our review may be considered beyond the scope of review and results may not necessarily be indicative of actual system implementation.

Manufacturer 2's provided documentation does not detail any particular support for disabled voters. Voting is conducted on a touch-screen which can also present a visual keyboard to allow voters to enter the name of an unlisted candidate. There is no provisioning for blind voters or those with impaired motor skills.

Manufacturer 2's voting system generates a voter's choice record which prints on the printer attached to the voting Laptop. No other means of providing this information is documented. Manufacturer 2's vote capture device does not provide audio output. The voting system requires tactile input in order to vote.

Voting selections are made via a touch-screen. Manufacturer 2's documentation does not detail any auditory interface to the voting system.

Manufacturer 2's voting system does generate a paper record of the voter's choices; however, there is no provisioning of a mechanism that can read that record and generate an audio representation of its contents.

The voter can not adjust the color saturation on the touch screen monitor. No options were available to select black text on white background or white text on black background. No specification for floor space as related to the voting station is provided.

4.6.2.1.10 Section 5.1 Security, Access Control

Manufacturer 2's documentation included detail on the definition of personnel roles with segregated duties and responsibilities on critical processes to prevent a single person from compromising the integrity of the system. The documentation did not specify that two persons from a predefined group are required for validating the election configuration information, whether or not its execution required an operating system privileged account, indicate the logging of all personnel access whether successful or unsuccessful, the restriction of accounts following failed logins after a preset number of logins, the logging of access restriction when an account is locked out, or the logging of access restriction when an account is locked out. As such, we would recommend that Manufacturer 2 ensure that such documentation is in place prior to a certification effort.

Functionally, Manufacturer 2's voting system has no log in authentication on the Election Administration application. The administrative application on the back end server did not time-out the user after fifteen minutes of inactivity nor did the voter interface time-out a voter after fifteen minutes of inactivity. The system did allow the user to screen lock while using the voting interface and the backend servers. The system allows the administrator group to configure permissions and functionality for each identity, group or role to include account and group/role creation, modification, and deletion.

4.6.2.1.11 Section 5.2 Security, Identification and Authentication

Manufacturer 2's documentation provided some detail for authentication of users, as well as protection of authentication data. Password details were somewhat lacking for proper understanding of the implementation. Documentation dealing with networking and message authentication was not as sufficiently robust as would be ideal. As such, we would recommend that Manufacturer 2 ensure that such documentation is in place prior to a certification effort.

Functionally, the system provided sufficient strength of authentication and employed adequate password management.

4.6.2.1.12 Section 5.3 Security, Cryptography

The Manufacturer 2 voting system documentation does not sufficiently describe the cryptographic functionality used. A combination of Bouncy Castle and OpenSSL cryptographic modules are used. Bouncy Castle does not have a FIPS certification and OpenSSL v0.9.8g Works only with Red Hat Enterprise Linux (RHEL) v5.4. The Manufacturer 2 system uses v3.4. Both modules are found to be non-compliant. The keys used in the system all meet the 112 bits security requirement except for one key with only 80 bits of security. Due to the lack of information, the component in which the non-compliant key is implemented could not be determined. The communications of the system is running OpenVPN and a Digital Certificate. OpenVPN does not have a FIPS certification but can be used in conjunction with OpenSSL running in FIPS mode. Due to the lack of information the OpenVPN module could not be determined to be compliant. No information was received from Manufacturer 2 in regards to the Digital Certificate used for the communications of the systems. Due to a lack of proper information the Key generation methods, Security of the key and Random number generator (RNG), seed key generation, Health tests for the RNG, Communications key generation, and Key Zeroization could not adequately be determined to be compliant. All keys are generated using automated methods and do not leave either the system or the tokens; therefore, encryption during import or export is not required. All keys stored within the voting system are kept within a PKCS#12 encrypted key containers. The voting system does not have the ability to "re-key" the system during an election. To re-key the system an election would have to be re-created.

4.6.2.1.13 Section 5.4 Security, Integrity Management

Manufacturer 2 provided only limited information for Integrity Management. Vote integrity was not fully covered to adequately fulfill requirements. Storage and electronic ballot box integrity were not fully addressed. No documentation was provided on the handling of malware detection or upgrade capability. Validation of kiosk vote capture device software was not addressed. As such, we would recommend that Manufacturer 2 ensure that such documentation is in place prior to a certification effort.

Functionally, Manufacturer 2 did provide adequate transmission integrity or storage of cast vote data. Cast vote storage and electronic ballot box integrity checks were sufficient. Checks for malware detection or upgrade mechanisms are not sufficiently implemented. As such, we would recommend that Manufacturer 2 ensure that such environments are available for appropriate inspection in a certification effort.

4.6.2.1.14 Section 5.5 Communications Security

Manufacturer 2's documentation was not sufficient in detailing how communications security was implemented, including usage of VPN, usage of TLS/SSL and mutual authentication. As such, we would recommend that Manufacturer 2 ensure that such documentation is in place prior to a certification effort.

Functionally, the VPN credentials could not be verified to meet the required standards. Additionally, the usage of the VPN precluded us from being able to determine how data was being encrypted.

4.6.2.1.15 Section 5.6 Security, Logging

Manufacturer 2's voting system documentation set did not sufficiently describe all system auditing procedure, configurations, or locations of the system audit logs. As such, we would recommend that Manufacturer 2 ensure that such documentation is in place prior to a certification effort.

The voting system is compliant logging power failures, abnormal shutdowns and restarts, removable media events, logon and logoff events, password changes, use of privileges, attempts to exceed privileges, access attempts to underlying resources, format of logs, maintaining voter privacy, timekeeping mechanisms, addition and deletion of users, and opening and closing Polls.

The voting system did not exhibit full compliance in logging error and exception messages, communications, displaying the status of transmissions, critical system status messages, events requiring election official intervention, changes

to system configuration settings, integrity checks, addition or deletion of files, system readiness results, backup and restore, authentication events, access control events, user account activity, installing and upgrading software, changes to configuration settings, abnormal process exits, database events, changes to cryptographic keys, and voting events.

4.6.2.1.16 Section 5.7 Security, Incident Response

Manufacturer 2's documentation did provide a sufficient list identifying what types of system operations or security events are classified as critical.

Manufacturer 2's system did not provide any alarms to be triggered during functional testing.

4.6.2.1.17 Section 5.8 Security, Physical and Environmental

Manufacturer 2 provided documentation but did not provide sufficient detail. Items lacking in the documentation include: there was no comprehensive list identifying critical central server components or the means by which unauthorized physical access could be recognized or prevented. The documentation did not identify an event log or any event that would cause an entry to be written to an event log. For the kiosk location there is not sufficient documentation to indicate that the disconnection of a component from the vote capture device would cause its port to become disabled. Neither is there sufficient detail to determine how attempts to modify the vote capture device would be detected and reported. The documentation does discuss the use of seals and locks to prevent tampering.

As such, we would recommend that Manufacturer 2 ensure that such documentation is in place prior to a certification effort.

During functional testing, disabled ports could only be re-enabled by an authorized administrator. An issue was discovered when a flash drive was plugged into an unused port in the back office and the device was accessible. The ability for the vote capture device to be automatically disabled if connections were broken with peripheral components was able to be evidenced when the smartcard reader was removed and the system disabled the port. For locks and seals, the placement of these items was not evidenced, as the seals were not delivered. As such, we would recommend that Manufacturer 2 be prepared to provide a full system environment, including hardware and all pertinent documentation, in a certification effort.

4.6.2.1.18 Section 5.9 Security, Penetration Resistance

With regard to the Penetration Resistance documentation, processes and procedures were implemented by Manufacturer 2, and resources provided were sufficient. Documentation was provided on how a system would be configured such that it would be resistant to unauthorized penetration attempts.

From a Functional perspective, Manufacturer 2 did provide kiosk oriented hardware.

From a Functional perspective, Manufacturer 2 was able to provide a locally located server, “backend” system for SLI to perform penetration testing. The back end consists of a suite of multiple devices. The system performed well. Generally, only a minimal port set was left open, and those were configured in an appropriately positive manner to prevent exploitation attempts. One back office device did provide an exception in that it did have several open ports, not all of which were in use. However, all ports did resist all exploitation attempts. 35 known exploits were successfully rebuffed. In terms of System Access and Interfaces, similar results were obtained: 35 exploits were attempted, with all being rebuffed. In terms of System Disclosure, when probed, the system did disclose the make and version of its SSH server. The testing that was performed on the provided equipment was successful overall in its security deployment.

White box testing was not implemented, as Manufacturer 2 did not provide source code to be reviewed as part of the white box testing effort.

4.6.2.1.19 Analysis of Manufacturer Assessment to the Requirements

For section 2 in terms of documentation, Manufacturer provided adequate documentation such that 97% of the requirements under review, would be considered to be met.

In terms of functionality, Manufacturer was evaluated at the following levels, for percentages of requirements being evaluated:

Passed: 96%

Insufficient Robustness: <4%

Not Tested: <1%

Not Applicable: 0%

In terms of documentation, Manufacturer provided adequate documentation such that 42% of the requirements under review, which consisted of Section 5, would be considered to be met.

In terms of functionality, Manufacturer was evaluated at the following levels, for percentages of requirements being evaluated:

Passed: 41%

Insufficient Robustness: 19%

Not Tested: 37%

Not Applicable: 3%

Note here that due to ongoing issues keeping this system up, not all tests were able to be run.

- Passed indicates that sufficient functionality was found such that the requirement is considered met.
- Insufficient Robustness indicates that a sufficient amount of functionality was not found such that the requirement is not considered to be fully met.
- Not Tested indicates that while functionality should be in place to cover the requirement, either access to the functionality was not provided, or documentation was insufficient for indicating where and how the functionality was implemented.
- Not Applicable indicates that functionality was not in place, nor was required.

4.6.3 Manufacturer 3

4.6.3.1 Evaluation of Testing

4.6.3.1.1 Section 5.1 Security, Access Control

Manufacturer 3's system supplied insufficient documentation for SLI to create user roles within the system. Manufacturer 3's system does not address the Kiosk site. As such, we would recommend that Manufacturer 3 ensure that such documentation is in place prior to a certification effort.

Voters could access their jurisdiction's election ballots and cast their vote at election time. The system implemented appropriate access control over each defined user/role/group.

While the requirements specify that the voting system shall require at least two persons from a predefined group for validating the election configuration information, accessing the cast vote records, and starting the tabulation process, Manufacturer 3's system allowed a single Election Official to change the election configuration.

Manufacturer 3's system did not time out an inactive voter following a specified period of inactivity; similarly with back office applications, an administrator was also allowed to remain logged into the application. The system also failed to log successful and unsuccessful logons. There was no preset number of logon failures to restrict access when the number of logon failures was exceeded.

4.6.3.1.2 Section 5.2 Security, Identification and Authentication

Documentation was provided that detailed authentication mechanisms implemented to support the voting system, though messaging schemas, algorithms or protocols lacked sufficient detail. Detail supplied on secure storage of authentication data. Documentation was not sufficient for detailing secure storage of authentication data. As such, we would recommend that Manufacturer 3 ensure that such documentation is in place prior to a certification effort.

Functionally, two-factor authentication was not sufficient in some areas within the system. Password reset was of sufficient robustness. Password controls including password expiration, password history and password strength were insufficient or not verifiable.

4.6.3.1.3 Section 5.3 Security, Cryptography

Manufacturer 3's voting system documentation was insufficient in describing the cryptographic functionality used. As such, we would recommend that Manufacturer 3 ensure that such documentation is in place prior to a certification effort.

Additionally, other issues were found in Manufacturer 3's implementation of cryptography. The voting system uses a combination of Bouncy Castle and OpenSSL. Bouncy Castle does not currently hold a FIPS certification, which in an actual UOCAVA certification effort would cause the voting system to not be compliant. The OpenSSL module does have several certifications from FIPS but information could not be acquired to adequately determine the certification in effect. The keys used on the voting system all comply with the required length of 112 bits.

The communications of the voting system uses a Digital Certificate generated by one of the top commercial Certificate Authorities (CA). SLI recognizes these top commercial CAs to be accredited Certification Authorities (CAs) and therefore practicing within industry standards in regards to cryptographic functions performed internally by these commercial CAs.

Due to lack of specific information, the key generation methods, security of the key and Random Number Generator (RNG), seed key generation, communications key generation, health tests for the RNG, and key zeroization could not be adequately determined for compliance.

The system uses a manual key generation process; therefore, keys can be and are imputed and exported in plaintext. All keys are placed in a key container and are encrypted. Re-keying is supported within the election design software.

4.6.3.1.4 Section 5.4 Security, Integrity Management

Manufacturer 3 provided only limited information for Integrity Management. Vote integrity was not fully covered to adequately fulfill requirements. Storage and electronic ballot box integrity were not fully addressed. No documentation was provided on the handling of malware detection or upgrade capability. Validation of kiosk vote capture device software was not addressed. As such, we would recommend that Manufacturer 3 ensure that such documentation is in place prior to a certification effort.

Functionally, Manufacturer 3 did not provide adequate transmission integrity or storage of cast vote data. Access to remote server location was not provided, such that neither cast vote storage nor electronic ballot box integrity checks

could be validated. Neither were checks for malware detection or upgrade mechanisms are implemented as per Manufacturer 3. As such, we would recommend that Manufacturer 3 ensure that such environments are available for appropriate inspection in a certification effort.

4.6.3.1.5 Section 5.5 Communications Security

Manufacturer 3's documentation was not sufficient in detailing how the data transmission integrity is protected in terms of protocols, mutual authentication methods, or interface protections. As such, we would recommend that Manufacturer 3 ensure that such documentation is in place prior to a certification effort.

Functionally, Manufacturer 3 did implement appropriate protocols and authentication methods.

4.6.3.1.6 Section 5.6 Security, Logging

Manufacturer 3's voting system documentation set did not sufficiently describe all system auditing procedure, configurations, or locations of the system audit logs. As such, we would recommend that Manufacturer 3 ensure that such documentation is in place prior to a certification effort.

The voting system is compliant logging power failures, abnormal shutdowns and restarts, removable media events, logon and logoff events, password changes, use of privileges, attempts to exceed privileges, access attempts to underlying resources, addition and deletion of users, and opening and closing Polls.

The voting system did not exhibit full compliance in logging error and exception messages, communications, critical system status messages, events requiring election official intervention, changes to system configuration settings, integrity checks, addition or deletion of files, system readiness results, backup and restore, authentication events, access control events, user account activity, installing and upgrading software, changes to configuration settings, abnormal process exits, database events, changes to cryptographic keys, and voting events.

4.6.3.1.7 Section 5.7 Security, Incident Response

Manufacturer 3's documentation did provide a 'System Security Specifications' document, but there was no comprehensive list identifying what types of system

operations or security events are classified as critical. As such, we would recommend that Manufacturer 3 ensure that such documentation is in place prior to a certification effort.

Manufacturer 3's system did not provide any alarms to be triggered during functional testing. With the current implementation of a browser implementation on a commercial off the shelf hardware component, in the kiosk location setup, this was not unexpected.

4.6.3.1.8 Section 5.8 Security, Physical and Environmental

Manufacturer 3's provided documentation did not provide sufficient detail. Items lacking in the documentation include: there was neither a comprehensive list identifying critical central server components nor the means by which unauthorized physical access could be recognized. There was no mention of disabling non-essential physical ports or access points. The documentation did not identify an event log or any event that would cause an entry to be written to an event log. The documentation did not provide guidelines for restricting physical access to ports supporting removable media which are not essential to the voting session. The documentation did not provide guidelines related to the recognition of physical tampering or unauthorized access to ports and all other access points.

The documentation did not include any guidelines as to the physical disabling of ports. The documentation provided did not detail the use of tamper evident or tamper resistant countermeasures. The documentation provided did not include guidelines related to physical security, tampering or tampering countermeasures. As such, we would recommend that Manufacturer 3 ensure that such documentation is in place prior to a certification effort.

During functional testing, disabled ports could only be re-enabled by an authorized administrator. An issue was discovered when a flash drive was plugged into an unused port and the device was accessible. The ability for the vote capture device to be automatically disabled if connections were broken with peripheral components was not able to be evidenced, as kiosk location equipment was not provided. Similarly for locks and seals, without delivered kiosk equipment, the placement of these items was not evidenced. As such, we would recommend that Manufacturer 4 be prepared to provide a full system environment, including hardware and all pertinent documentation, in a certification effort.

4.6.3.1.9 Section 5.9 Security, Penetration Resistance

With regard to the Penetration Resistance documentation, processes and procedures implemented by Manufacturer 3, resources provided were limited. No documentation was provided on how a system would be configured such that it would be resistant to unauthorized penetration attempts. As such, we would recommend that Manufacturer 3 ensure that such documentation is in place prior to a certification effort.

From a Functional perspective, Manufacturer 3 did not provide kiosk oriented hardware. Therefore, we were not able to exercise testing against a Manufacturer 3 hardened physical environment. As such, we would recommend that Manufacturer 3 ensure that such hardware is available for appropriate inspection in a certification effort.

From a Functional perspective, Manufacturer 3 was able to provide a locally located server, “backend” system for SLI to perform penetration testing. The system performed well. Only a minimal port set was left open, and those were configured in an appropriately positive manner to prevent exploitation attempts. 215 known exploits were successfully rebuffed. In terms of System Access and Interfaces, similar results were obtained: 253 exploits were attempted, with all being rebuffed. In terms of System Disclosure, when probed, the system did disclose the make and version of its web server. As such, we would recommend that Manufacturer 3 be prepared to provide a full system environment in a certification effort, though the testing that was performed on the provided equipment was successful overall in its security deployment.

White box testing was not implemented, as Manufacturer 3 did not provide source code to be reviewed as part of the white box testing effort.

4.6.3.1.10 Analysis of Manufacturer Assessment to the Requirements

In terms of documentation, Manufacturer provided documentation such that 18% of the requirements under review, which consisted of Section 5, would be considered to be met.

In terms of functionality, Manufacturer was evaluated at the following levels, for percentages of requirements being evaluated:

Passed: 23%

Insufficient Robustness: 38%

Not Tested: 36%

Not Applicable: 3%

- Passed indicates that sufficient functionality was found such that the requirement is considered met.
- Insufficient Robustness indicates that a sufficient amount of functionality was not found such that the requirement is not considered to be fully met.
- Not Tested indicates that while functionality should be in place to cover the requirement, either access to the functionality was not provided, or documentation was insufficient for indicating where and how the functionality was implemented.
- Not Applicable indicates that functionality was not in place, nor was required.

4.6.4 Manufacturer 4

4.6.4.1 Evaluation of Testing

4.6.4.1.1 Section 5.1 Security, Access Control

Manufacturer 4's supplied documentation included procedures to create appropriate users, roles and groups, though the role of kiosk workers was not detailed. Documentation for the verification default access control, prevention of escalation, session timeouts account lockouts or handling of login failures also was not provided. Documentation did not include information on the logging of an event in the system event log of successful or unsuccessful attempts to access the system, nor did the documentation include any information related to restricting access to the system after a preset number of logon failures. As such, we would recommend that Manufacturer 4 ensure that such documentation is in place prior to a certification effort.

Functionally, Manufacturer 4's voting system generally implemented access controls for each level of user within the system, though a few exceptions were noted, as some back office roles were able to access vote data records that would not be expected to be within the scope of their roles. Basic personnel definitions and access controls were in place, such that users/roles/groups are only allowed access to their respective duties. Both the administrative console and the voting application allowed for a screen lockout mechanism that could be manually invoked requiring re-authentication to access the system. The tabulation process was not properly configured, so multiple authorized users were not required to access the tabulation process. Voters were logged out following a five-minute inactivity period, but personnel logged on to back office applications were not logged out following periods of inactivity.

4.6.4.1.2 Section 5.2 Security, Identification and Authentication

Documentation was provided that detailed authentication mechanisms implemented to support the voting system; this included any messaging schemas, algorithms or protocols. Documentation was not sufficient for detailing secure storage of authentication data. As such, we would recommend that Manufacturer 7 ensure that such documentation is in place prior to a certification effort.

Functionally, credentials were not supplied in order to verify that authentication was properly employed within the system. Handling of passwords, including reset and configuration expiration were insufficient; as password strength could not be verified, password history protection was insufficient. Nor do administrator passwords expire. Device, network and message authentication were of sufficient implementation.

4.6.4.1.3 Section 5.3 Security, Cryptography

The Manufacturer 4 voting system documentation does not sufficiently describe the Cryptographic functionality used. For non-communications cryptography OpenSSL v1.2 is used. The module is running on Microsoft Windows Server 2008 R2 (Server 08). OpenSSL v1.2 running on Server 08 has received FIPS certificate #1111. The manufacturer did not provide enough information to adequately evaluate if the module is adhering to the System Security Plan (SSP) associated with the FIPS certification. The communications of the voting system uses a Digital Certificate generated by one of the top commercial Certificate Authorities (CA). SLI recognizes these top commercial CAs to be accredited Certification Authorities (CAs) and therefore practicing within industry standards in regards to cryptographic functions performed internally by these commercial CAs.

All keys used for cryptographic functions are of the required key strength of 112 bits of security. All cryptographic Keys, key generation methods both in communication and non-communication, seed key generation, and Random Number Generator (RNG) health tests are NIST approved under the FIPS certificate for the OpenSSL module. All keys are contained internally to the voting system. Adequate information on the storage of keys in encrypted containers was not received from the manufacturer. Keys are destroyed after they are generated and the voting system allows for re-keying within the Election software. As such, we would recommend that Manufacturer 4 ensure that such documentation is in place prior to a certification effort.

4.6.4.1.4 Section 5.4 Security, Integrity Management

Manufacturer 4 provided only limited information for Integrity Management. Vote integrity was not fully covered to adequately fulfill requirements. Storage and electronic ballot box integrity were not fully addressed. No documentation was provided on the handling of malware detection or upgrade capability. Validation of kiosk vote capture device software was not addressed. As such, we would recommend that Manufacturer 4 ensure that such documentation is in place prior to a certification effort.

Functionally, Manufacturer 4 did not provide adequate transmission integrity or storage of cast vote data. Access to a remote server location was not provided, so neither cast vote storage nor electronic ballot box integrity checks could be validated. Neither were checks for malware detection or upgrade mechanisms available, due to lack of access to back end servers. As such, we would recommend that Manufacturer 4 ensure that such environments are available for appropriate inspection in a certification effort.

4.6.4.1.5 Section 5.5 Communications Security

Manufacturer 4 provided only limited information for Integrity Management. Vote integrity was not fully covered to adequately fulfill requirements. Information regarding data integrity protection, strength of protocols, as well as how data transmission preserves secrecy and privacy is needed. Additionally, documentation on security implementations to deal with external threats such as minimization and disabling of interfaces to prevent channels of attack is needed. As such, we would recommend that Manufacturer 4 ensure that such documentation is in place prior to a certification effort.

Functionally, each requirement proved to be implemented, as applicable to devices and applications within the system. Sufficient unique identifiers are in place, along with appropriate mutual authentication. Interfaces were appropriately minimized to prevent authorized access attempts.

4.6.4.1.6 Section 5.6 Security, Logging

Manufacturer 4 did provide a sufficient amount of documentation regarding storage format of data, time keeping of log events, and restriction of access to authorized roles. Documentation was insufficient in the areas of Log Management in terms of append-only access separation of each jurisdiction's event logs or setting of the system clock for at least a portion of the system

implemented, as well as implementation of default settings for log management activities, or how log related activities get logged, or the preservation of logs prior to system decommissioning. As such, we would recommend that Manufacturer 4 ensure that such documentation is in place prior to a certification effort.

Functionally, Manufacturer 4's system did provide sufficient functionality in the logging of events, the ability to view the logs, time keeping that enables recreation of events, as well as access restriction to proper user levels. The system did not meet requirements within Log Management in terms of append-only access separation of each jurisdiction's event logs or setting of the system clock for at least a portion of the system implemented. Nor did the system sufficiently cover how communications are activated and deactivated, what services were accessed, identification of the device which data was transmitted to or received from Identification of authorized entity, as well as successful and unsuccessful attempts to access communications or services.

The Manufacturer 4 voting system is hosted remotely. A remote testing session was requested by SLI but not granted by the manufacturer to gain access to the underlying operating system. Without access or a remote testing session the requirements in this section cannot be adequately assessed. As such, we would recommend that Manufacturer 4 ensure that such documentation is in place prior to a certification effort.

4.6.4.1.7 Section 5.7 Security, Incident Response

For Manufacturer 4, no documentation was provided related to the hardening of kiosk location hardware, nor the kiosk locations hardware handling of critical events. As such, we would recommend that Manufacturer 4 ensure that such documentation is in place prior to a certification effort.

As Manufacturer 4 did not provide kiosk location hardware, no test could be executed against a manufacturer recommended hardware deployment. As such, we would recommend that Manufacturer 4 be prepared to provide a full system environment, including hardware and all pertinent documentation, in a certification effort.

4.6.4.1.8 Section 5.8 Security, Physical and Environmental

For Manufacturer 4, no documentation was provided related to physical security and the recognition of unauthorized events, nor the disabling of non-essential ports, the protection of ports on the vote capture device, either not in use or

when a connection is lost, or how it would be logged. Nor were tamper evident/resistant physical locks covered in any detail within provided documentation, nor did it appropriately describe the tabulation process to be configured such that multiple authorized users were required to access the tabulation process. Protection of media and kiosk location equipment was not adequately addressed within provided documentation. As such, we would recommend that Manufacturer 4 ensure that such documentation is in place prior to a certification effort.

Functionally, Manufacturer 4 did not provide kiosk location equipment for review on this project, nor access to the remote back end server environment. Thus we were unable to inspect an empirical implementation of a vote capture device, with appropriate physical port protection, any logging, tamper evident/resistance or implementation of physical locks. As such, we would recommend that Manufacturer 4 ensure that such environments are available for appropriate inspection in a certification effort.

4.6.4.1.9 Section 5.9 Security, Penetration Resistance

With regard to the Penetration Resistance documentation, processes and procedures implemented by Manufacturer 4, resources provided were limited. No documentation was provided on how a system would be configured such that it would be resistant to unauthorized penetration attempts. As such, we would recommend that Manufacturer 4 ensure that such documentation is in place prior to a certification effort.

From a Functional perspective, Manufacturer 4 did not provide kiosk oriented hardware. Therefore, we were not able to exercise testing against a Manufacturer 4 hardened physical environment. As such, we would recommend that Manufacturer 4 ensure that such hardware is available for appropriate inspection in a certification effort.

From a Functional perspective, Manufacturer 4 was not able to provide a locally located server, “backend” system for SLI to perform penetration testing. The potential legal concerns of attempting invasive penetration attempts over public domains precluded the testing from occurring. As such, we would recommend that Manufacturer 4 be prepared to provide a full system environment in a certification effort.

White box testing was not implemented, as Manufacturer 4 did not provide source code to be reviewed as part of the white box testing effort.

4.6.4.1.10 Analysis of Manufacturer Assessment to the Requirements

In terms of documentation, Manufacturer provided documentation such that 8% of the requirements under review, which consisted of Section 5, would be considered to be met.

In terms of functionality, Manufacturer was evaluated at the following levels, for percentages of requirements being evaluated:

Passed: 14%

Insufficient Robustness: 7%

Not Tested: 74%

Not Applicable: 6%

- Passed indicates that sufficient functionality was found such that the requirement is considered met.
- Insufficient Robustness indicates that a sufficient amount of functionality was not found such that the requirement is not considered to be fully met.
- Not Tested indicates that while functionality should be in place to cover the requirement, either access to the functionality was not provided, or documentation was insufficient for indicating where and how the functionality was implemented.
- Not Applicable indicates that functionality was not in place, nor was required.

4.6.5 Manufacturer 5

4.6.5.1 Evaluation of Testing

4.6.5.1.1 Section 5.1 Security, Access Control

Manufacturer 5's supplied documentation did not include procedures to create appropriate users, roles and groups, Documentation for the verification default access control, prevention of escalation, session timeouts account lockouts or handling of login failures, also was not provided. Documentation did not include information that included procedures on the logging of an event in the system event log of successful or unsuccessful attempts to access the system nor did the documentation include any information related to restricting access to the system after a preset number of logon failures, nor did it appropriately describe the tabulation process to be configured such that multiple authorized users were required to access the tabulation process. Documentation did not detail tools for

monitoring access to the voting system in real time as well as via log reports. As such, we would recommend that Manufacturer 5 ensure that such documentation is in place prior to a certification effort.

Functionally, Manufacturer 5's voting system appropriately implemented access controls for each level of user within the system. Basic personnel definitions and access controls were in place, such that users/roles/groups are only allowed access to their respective duties. Both the administrative console and the voting application allowed for a screen lockout mechanism that could be manually invoked requiring re-authentication to access the system. The tabulation process was not properly configured such that multiple authorized users were not required to access the tabulation process. Voters and officials were not logged out following an inactivity period.

4.6.5.1.2 Section 5.2 Security, Identification and Authentication

Manufacturer 5 provided only minimal documentation related to the system's implementation of identification or authentication. Documentation was not provided that detailed authentication mechanisms implemented to support the voting system, as well as messaging schemas, algorithms or protocols lacked sufficient detail. Detail supplied on secure storage of authentication data. Documentation was not sufficient for detailing secure storage of authentication data.

As such, we would recommend that Manufacturer 5 ensure that such documentation is in place prior to a certification effort.

Functionally, two-factor authentication was not sufficient in some areas within the system. Password reset was of sufficient robustness. Password controls including password expiration, password history and password strength were insufficient or not verifiable.

4.6.5.1.3 Section 5.3 Security, Cryptography

The Manufacturer 5 system documentation does not properly outline any cryptography in the voting system documentation set. Cryptographic functions are run using the DSSENH module under FIPS certificate #868 and runs on a Microsoft Windows Server 2003. The system follows the Security Policy for the FIPS certificate in running single user mode for all cryptographic functions. The running mode of the module could not be adequately determined without review of portions of the source code to confirm the correct calls are being made when performing cryptographic functions. Keys on the system adhere to the 112 bit

security strength. The communications of the voting system uses a Digital Certificate generated by one of the top commercial Certificate Authorities (CA). SLI recognizes these top commercial CAs to be accredited Certification Authorities (CAs) and therefore practicing within industry standards in regards to cryptographic functions performed internally by these commercial CAs. The key generation methods, security of the key and Random Number Generator (RNG), seed key generation, health tests for the RNG, and key zeroization all are NIST approved through the FIPS certificate #868. Keys are neither exported nor imported into the system. Due to the lack of information on the storage of the keys in encrypted containers, key zeroization and the capability to reset keys could not adequately be assessed. As such, we would recommend that Manufacturer 5 ensure that such documentation is in place prior to a certification effort.

4.6.5.1.4 Section 5.4 Security, Integrity Management

Manufacturer 5 provided only limited information for Integrity Management. Vote integrity was not fully covered to adequately fulfill requirements, nor was storage and electronic ballot box integrity. Documentation was not provided on the handling of malware detection or upgrade capability. Validation of kiosk vote capture device software was not addressed. As such, we would recommend that Manufacturer 5 ensure that such documentation is in place prior to a certification effort.

Functionally, Manufacturer 5 did not provide access to remote server location, such that neither cast vote storage nor electronic ballot box integrity checks could be validated. Neither were checks for malware detection or upgrade mechanisms available, due to lack of access to back end servers. As such, we would recommend that Manufacturer 5 ensure that such environments are available for appropriate inspection in a certification effort.

4.6.5.1.5 Section 5.5 Communications Security

Manufacturer 5 provided documentation for Integrity Management, though not to a level that fully met the requirements. Vote integrity was not fully covered to adequately fulfill requirements. Additional information regarding data integrity protection, strength of protocols, as well as how data transmission preserves secrecy and privacy is needed. Additionally, documentation on security implementations to deal with external threats such minimization and disabling of interfaces to prevent channels of attack is needed. As such, we would

recommend that Manufacturer 5 ensure that such documentation is in place prior to a certification effort.

Functionally, each requirement proved to be implemented, as applicable to devices and applications within the system. Sufficient unique identifiers are in place, along with appropriate mutual authentication. Interfaces were appropriately minimized to prevent authorized access attempts.

4.6.5.1.6 Section 5.6 Security, Logging

Manufacturer 5 did provide sufficient documentation regarding storage format of data, time keeping of log events, and restriction of access to authorized roles. Documentation was insufficient in the areas of Log Management in terms of append-only access separation of each jurisdiction's event logs and setting of the system clock for at least a portion of the system implemented, as well as implementation of default settings for log management activities, how log related activities get logged, and the preservation of logs prior to system decommissioning. As such, we would recommend that Manufacturer 5 ensure that such documentation is in place prior to a certification effort.

Functionally, Manufacturer 5's system did provide sufficient functionality in the logging of events, the ability to view the logs, time keeping that enables recreation of events, access restriction to proper user levels, as well as, partially, logging of communications actions. The system did not meet requirements within Log Management in terms of append-only access separation of each jurisdiction's event logs, voter privacy of data not in logs, or setting of the system clock for at least a portion of the system implemented. Nor did the system sufficiently cover how communications are activated and deactivated, what services were accessed, identification of the device which data was transmitted to or received from, identification of authorized entity, or successful and unsuccessful attempts to access communications or services.

4.6.5.1.7 Section 5.7 Security, Incident Response

For Manufacturer 5, no documentation was provided related to the hardening of kiosk location hardware, nor the kiosk location hardware's handling of critical events. As such, we would recommend that Manufacturer 5 ensure that such documentation is in place prior to a certification effort.

As Manufacturer 5 did not provide kiosk location hardware, no test could be executed against a manufacturer recommended hardware deployment. As such, we would recommend that Manufacturer 5 be prepared to provide a full system

environment, including hardware and all pertinent documentation, in a certification effort.

4.6.5.1.8 Section 5.8 Security, Physical and Environmental

For Manufacturer 5, documentation was partially provided related to physical security and the disabling of non-essential ports, the protection of ports on the vote capture device, either not in use or when a connection is lost. Tamper evident/resistant, physical lock concepts were also partially covered within provided documentation. Protection of media and kiosk location equipment was not adequately addressed within provided documentation. As such, we would recommend that Manufacturer 5 ensure that such documentation is in place prior to a certification effort.

Functionally, Manufacturer 5 did not provide kiosk location equipment for review on this project, nor access to the remote back end server environment. Thus we were unable to inspect an empirical implementation of a vote capture device, with appropriate physical port protection, any logging, tamper evidence/ resistance or implementation of physical locks. As such, we would recommend that Manufacturer 5 ensure that such environments are available for appropriate inspection in a certification effort.

4.6.5.1.9 Section 5.9 Security, Penetration Resistance

With regard to the Penetration Resistance documentation, processes and procedures implemented by Manufacturer 5, resources provided were limited.

No documentation was provided on how a system would be configured such that it would be resistant to unauthorized penetration attempts. As such, we would recommend that Manufacturer 5 ensure that such documentation is in place prior to a certification effort.

From a Functional perspective, Manufacturer 5 did not provide kiosk oriented hardware. Therefore, we were not able to exercise testing against a Manufacturer 5 hardened physical environment. As such, we would recommend that Manufacturer 5 ensure that such hardware is available for appropriate inspection in a certification effort.

From a Functional perspective, Manufacturer 5 was able to provide a local server, “backend” system for SLI to perform penetration testing. The system performed well. Only a minimal port set was left open, and those were configured in an appropriately positive manner to prevent exploitation attempts. Over 200 known exploits were successfully rebuffed. In terms of System Access

and Interfaces, similar results were obtained: 253 exploits were attempted, with all being rebuffed. In terms of System Disclosure, when probed, the system did disclose the make and version of its web server. As such, we would recommend that Manufacturer 5 be prepared to provide a full production system environment in a certification effort, though the testing that was performed on the provided equipment was successful overall in its security deployment.

White box testing was not implemented, as Manufacturer 5 did not provide source code to be reviewed as part of the white box testing effort.

4.6.5.1.10 Analysis of Manufacturer Assessment to the Requirements

In terms of documentation, Manufacturer provided documentation such that 5% of the requirements under review, which consisted of Section 5, would be considered to be met.

In terms of functionality, Manufacturer was evaluated at the following levels, for percentages of requirements being evaluated:

Passed: 29%

Insufficient Robustness: 6%

Not Tested: 59%

Not Applicable: 6%

- Passed indicates that sufficient functionality was found such that the requirement is considered met.
- Insufficient Robustness indicates that a sufficient amount of functionality was not found such that the requirement is not considered to be fully met.
- Not Tested indicates that while functionality should be in place to cover the requirement, either access to the functionality was not provided, or documentation was insufficient for indicating where and how the functionality was implemented.
- Not Applicable indicates that functionality was not in place, nor was required.

4.6.6 Manufacturer 6

4.6.6.1 Evaluation of Testing

4.6.6.1.1 Section 5.1 Security, Access Control

Manufacturer 6's supplied documentation did not include procedures to create appropriate users, roles and groups, or how to prevent a single person from compromising the election's integrity. Documentation for the verification default access control, prevention of escalation, session timeouts account lockouts or handling of login failures, also was not provided. Documentation did not include information on the logging of an event in the system event log of successful or unsuccessful attempts to access the system nor did the documentation include any information related to restricting access to the system after a preset number of logon failures, or how to grant access to accounts that had been locked out. The system did not detail real time monitoring of access, or logging of such. As such, we would recommend that Manufacturer 6 ensure that such documentation is in place prior to a certification effort.

Functionally, Manufacturer 6 appropriately implemented access controls for each accessible level of user within the system. Basic personnel definitions and access controls were in place, such that users/roles/groups are only allowed access to their respective duties. Tabulation process was configured such that multiple authorized users were not required to access the tabulation process. Voters were logged out following a five-minute inactivity window. Back office applications were not reviewed, as they were remotely located and access was not granted. (Note: access was finally granted on June 17th to the back office, but testing concluded on the 18th. As a result, not all back office applications were reviewed.) As such, we would recommend that Manufacturer 6 be prepared to provide a full system environment in a certification effort.

4.6.6.1.2 Section 5.2 Security, Identification and Authentication

Manufacturer 6 did not supply any documentation in this area. No documentation was provided that detailed any authentication mechanisms implemented to support the voting system; this included any messaging schemas, algorithms or protocols. Neither was detail supplied on secure storage of authentication data. As such, we would recommend that Manufacturer 6 ensure that such documentation is in place prior to a certification effort.

Functionally, Manufacturer 6's system was not reviewed to this section's criteria, as time ran out on the project, after a one-month delay in access to the remote system, due to an ongoing live election.

4.6.6.1.3 Section 5.3 Security, Cryptography

Manufacturer 6's voting system documentation does not sufficiently outline its cryptography implementation. Documentation provided alluded to the inherent security implemented by the chosen technologies employed by the system. No detailed explanation of exactly how the cryptography is implemented within the voting system was given. Additionally, the system was under development and running an election at the time of testing. Access to the system and manufacturer support was not available until after the scheduled completion of the project. The system is under re-development and in the future will be placed in the Microsoft Azure environment. Without additional information about the environment and the cryptographic module used, the requirements within this section cannot be adequately assessed for compliance. As such, we would recommend that Manufacturer 6 ensure that such documentation is in place, for all aspects of the system regardless of hosting environment, prior to a certification effort.

4.6.6.1.4 Section 5.4 Security, Integrity Management

Manufacturer 6 provided only limited information for Integrity Management. Documentation was not provided on the handling of malware detection or upgrade capability. Validation of kiosk vote capture device software was not addressed. As such, we would recommend that Manufacturer 6 ensure that such documentation is in place prior to a certification effort.

Functionally, Manufacturer 6 did not provide access to remote server location, such that checks for malware detection or upgrade mechanisms could be made, due to lack of access to back end servers. As such, we would recommend that Manufacturer 6 ensure that such environments are available for appropriate inspection in a certification effort.

4.6.6.1.5 Section 5.5 Communications Security

Manufacturer 6 did not supply any documentation in this area. No documentation was provided that detailed any data transmission integrity implemented to support the voting system, including any messaging schemas, algorithms or protocols. No detail as to disabling of network interfaces,

minimization of interfaces, or blocking of network connections was provided. Neither was detail supplied on secure storage of authentication data. As such, we would recommend that Manufacturer 6 ensure that such documentation is in place prior to a certification effort.

Functionally, Manufacturer 6's system was not reviewed to this section's criteria, as time ran out on the project, after a one-month delay in access to the remote system, due to an ongoing live election.

4.6.6.1.6 Section 5.6 Security, Logging

Manufacturer 6 did not provide sufficient documentation regarding storage format of data, time keeping of log events, and restriction of access to authorized roles. Documentation was insufficient in the areas of Log Management in terms of append-only access separation of each jurisdiction's event logs or setting of the system clock for at least a portion of the system implemented, as well as implementation of default settings for log management activities, or how log related activities get logged, or the preservation of logs prior to system decommissioning. Nor did the system sufficiently cover how communications are activated and deactivated, what services were accessed, identification of the device which data was transmitted to or received from, identification of authorized entity, or successful and unsuccessful attempts to access communications or services. As such, we would recommend that Manufacturer 6 ensure that such documentation is in place prior to a certification effort.

Functionally, Manufacturer 6's system did provide sufficient functionality in the logging of events, the ability to view the logs, time keeping that enables recreation of events, as well as access restriction to proper user levels that were accessible. The system did meet requirements within Log Management in terms of append-only access.

4.6.6.1.7 Section 5.7 Security, Incident Response

For Manufacturer 6, no documentation was provided related to the hardening of kiosk location hardware, nor the kiosk locations hardware handling of critical events. As such, we would recommend that Manufacturer 6 ensure that such documentation is in place prior to a certification effort.

As Manufacturer 6 did not provide kiosk location hardware, no test could be executed against a manufacturer recommended hardware deployment. As such, we would recommend that Manufacturer 6 be prepared to provide a full system

environment, including hardware and all pertinent documentation, in a certification effort.

4.6.6.1.8 Section 5.8 Security, Physical and Environmental

For Manufacturer 6, documentation was minimally provided related to physical security and the disabling of non-essential ports, the protection of ports on the vote capture device, either not in use or when a connection is lost. Tamper evident/resistant, physical lock concepts were not covered within provided documentation. Protection of media and kiosk location equipment was not adequately addressed within provided documentation. As such, we would recommend that Manufacturer 6 ensure that such documentation is in place prior to a certification effort.

Functionally, Manufacturer 6 did not provide kiosk location equipment for review on this project, nor access to the remote back end server environment. Thus we were unable to inspect an empirical implementation of a vote capture device, with appropriate physical port protection, any logging, tamper evident/resistance or implementation of physical locks. As such, we would recommend that Manufacturer 6 ensure that such environments are available for appropriate inspection in a certification effort.

4.6.6.1.9 Section 5.9 Security, Penetration Resistance

With regard to the Penetration Resistance documentation, processes and procedures implemented by Manufacturer 6, resources provided were limited.

No documentation was provided on how a system would be configured such that it would be resistant to unauthorized penetration attempts. As such, we would recommend that Manufacturer 6 ensure that such documentation is in place prior to a certification effort.

From a Functional perspective, Manufacturer 6 did not provide kiosk oriented hardware. Therefore, we were not able to exercise testing against a Manufacturer 6 hardened physical environment. As such, we would recommend that Manufacturer 6 ensure that such hardware is available for appropriate inspection in a certification effort.

From a Functional perspective, Manufacturer 6 was not able to provide a local server, “backend” system for SLI to perform penetration testing. The potential legal concerns of attempting invasive penetration attempts over public domains precluded the testing from occurring. As such, we would recommend that

Manufacturer 6 be prepared to provide a full system environment in a certification effort.

White box testing was not implemented, as Manufacturer 6 did not provide source code to be reviewed as part of the white box testing effort.

4.6.6.1.10 Analysis of Manufacturer Assessment to the Requirements

In terms of documentation, Manufacturer provided documentation such that 1% of the requirements under review, which consisted of Section 5, would be considered to be met.

In terms of functionality, Manufacturer was evaluated at the following levels, for percentages of requirements being evaluated:

Passed: 6%

Insufficient Robustness: 6%

Not Tested: 86%

Not Applicable: 2%

Note here that this system was not available for most of the testing period.

- Passed indicates that sufficient functionality was found such that the requirement is considered met.
- Insufficient Robustness indicates that a sufficient amount of functionality was not found such that the requirement is not considered to be fully met.
- Not Tested indicates that while functionality should be in place to cover the requirement, either access to the functionality was not provided, or documentation was insufficient for indicating where and how the functionality was implemented.
- Not Applicable indicates that functionality was not in place, nor was required.

4.6.7 Manufacturer 7

4.6.7.1 Evaluation of Testing

4.6.7.1.1 Section 5.1 Security, Access Control

The Manufacturer 7 documentation did not include information related to the personnel roles which could be defined within the Voting System nor the duties

and responsibilities associated with those roles. Documentation for the verification default access control, prevention of escalation, session timeouts account lockouts or handling of login failures, also was not provided. As such, we would recommend that Manufacturer 7 ensure that such documentation is in place prior to a certification effort.

Functionally basic personnel definitions and access controls were in place, such that users/roles/groups are only allowed access to their respective duties. Both the administrative console and the voting application allowed for a screen lockout mechanism that could be manually invoked requiring re-authentication to access the system. Administrative and monitoring consoles did not have required inactivity time-out that requires personnel re-authentication when reached. The system did not log either a successful logon or an unsuccessful logon.

4.6.7.1.2 Section 5.2 Security, Identification and Authentication

Manufacturer 7 did not supply any documentation in this area. No documentation was provided that detailed any authentication mechanisms implemented to support the voting system; this included any messaging schemas, algorithms or protocols. Neither was detail supplied on secure storage of authentication data. As such, we would recommend that Manufacturer 7 ensure that such documentation is in place prior to a certification effort.

Functionally, Manufacturer 7's system did not provide required multifactored authentication, sufficient password strength or restrictions, or expirations.

4.6.7.1.3 Section 5.3 Security, Cryptography

Manufacturer 7's voting system documentation does not sufficiently outline cryptography in the voting system documentation set. Additional information was received from Manufacturer 7 stating the system uses OpenSSL in combination with Ruby and Rails. Additionally, Manufacturer 7 has stated that the open source framework employed has been addressing web security issues from the start of its security project. Without additional information about the environment and the cryptographic module used, the requirements within this section cannot be adequately assessed for compliance. As such, we would recommend that Manufacturer 7 ensure that such documentation is in place for all aspects of the system regardless of hosting environment prior to a certification effort.

4.6.7.1.4 Section 5.4 Security, Integrity Management

Manufacturer 7's documentation is not of sufficient detail in the areas of malware detection and updating, as well as for validating the software on kiosk devices. As such, we would recommend that Manufacturer 7 ensure that such documentation is in place, for all aspects of the system, regardless of hosting environment prior to a certification effort.

4.6.7.1.5 Section 5.5 Communications Security

Manufacturer 7's documentation provided with regard to data transmission integrity in terms of protocols, mutual authentication methods, disabling and minimizing of interfaces is not of sufficient detail to adequately determine the implementation. As such, we would recommend that Manufacturer 7 ensure that such documentation is in place, for all aspects of the system, regardless of hosting environment prior to a certification effort.

Functionally, ballots were able to be edited, which was an insufficient integrity protection.

4.6.7.1.6 Section 5.6 Security, Logging

The Manufacturer 7 voting system lacked documentation in the area of communications logging for items such as when implementation of default settings, restrictions of log access, log file logging related functions, storage of data in public formats, separation of jurisdictions data, ability to analyze data, communications are activated and deactivated, what services were accessed, identification of the device which data was transmitted to or received from, identification of authorized entity, as well as successful and unsuccessful attempts to access communications or services. As such, we would recommend that Manufacturer 7 ensure that such documentation is in place prior to a certification effort.

Functionally, however, the system did generally log appropriate system events and all communications actions. The system also implemented appropriate access restrictions and time keeping mechanisms such that the events could be accurately reproduced and that only appropriate personnel would be able to access logs according their granted access rights level.

Manufacturer 7's voting system documentation set does not sufficiently describe any system auditing procedure, configurations, or locations of the system audit logs. As such, we would recommend that Manufacturer 7 ensure that such documentation is in place prior to a certification effort.

The voting system is not fully compliant in logging critical system status messages, shutdown and restarts, changes in system configuration settings, integrity checks, system readiness results, authentication events, access control, user account and role management, installing and upgrading software, changes to configurations, abnormal process exits, successful and failed database connections, and changes to cryptographic keys. The voting system is compliant logging power failures as a exception event, both normal and abnormal shutdowns, kernel setting changes, files added or deleted, removable media events, successful and unsuccessful backups and restores, logon and logoff events, use of privileges, and attempts to exceed privileges.

4.6.7.1.7 Section 5.7 Security, Incident Response

For Manufacturer 7, no documentation was provided related to the hardening of kiosk location hardware, nor the kiosk locations hardware handling of critical events. As such, we would recommend that Manufacturer 7 ensure that such documentation is in place prior to a certification effort.

As Manufacturer 7 did not provide kiosk location hardware, no test could be executed against a manufacturer recommended hardware deployment. As such, we would recommend that Manufacturer 7 be prepared to provide a full system environment, including hardware and all pertinent documentation, in a certification effort.

4.6.7.1.8 Section 5.8 Security, Physical and Environmental

Manufacturer 7 did not provide documentation related to physical or environmental security requirements. No documentation was provided on event logs as related to unauthorized physical access, nor any documentation of alarms or seals as related to unauthorized physical access. As such, we would recommend that Manufacturer 7 ensure that such documentation is in place prior to a certification effort.

Physical inspection of the provided hardware revealed no tamper proof seals on access points. Functional testing allowed unknown media to be inserted into an available USB port and the device was usable, with no alarms to alert personnel to an intrusion. The system did provide that disabled ports could only be re-enabled by authorized administrators.

4.6.7.1.9 Section 5.9 Security, Penetration Resistance

With regard to the Penetration Resistance documentation, processes and procedures implemented by Manufacturer 7, resources provided were limited. No documentation was provided on how a system would be configured such that it would be resistant to unauthorized penetration attempts. As such, we would recommend that Manufacturer 7 ensure that such documentation is in place prior to a certification effort.

From a Functional perspective, Manufacturer 7 did not provide kiosk oriented hardware. Therefore, we were not able to exercise testing against a Manufacturer 7 hardened physical environment. As such, we would recommend that Manufacturer 7 ensure that such hardware is available for appropriate inspection in a certification effort.

From a Functional perspective, Manufacturer 7 was not able to provide a local server, “backend” system for SLI to perform penetration testing. The potential legal concerns of attempting invasive penetration attempts over public domains precluded the testing from occurring. As such, we would recommend that Manufacturer 5 be prepared to provide a full system environment in a certification effort.

White box testing was not implemented, as Manufacturer 7 did not provide source code to be reviewed as part of the white box testing effort.

4.6.7.1.10 Analysis of Manufacturer Assessment to the Requirements

In terms of documentation, Manufacturer provided documentation such that 8% of the requirements under review, which consisted of Section 5, would be considered to be met.

In terms of functionality, Manufacturer was evaluated at the following levels, for percentages of requirements being evaluated:

Passed: 35%

Insufficient Robustness: 8%

Not Tested: 52%

Not Applicable: 5%

- Passed indicates that sufficient functionality was found such that the requirement is considered met.
- Insufficient Robustness indicates that a sufficient amount of functionality was not found such that the requirement is not considered to be fully met.

- Not Tested indicates that while functionality should be in place to cover the requirement, either access to the functionality was not provided, or documentation was insufficient for indicating where and how the functionality was implemented.
- Not Applicable indicates that functionality was not in place, nor was required.

5 Project Summary

The project was broken out into two main stages. The first stage was an analysis of the requirements, as stated in the current iteration of the UOCAVA Pilot Program Testing Requirements document. The second stage dealt with an analysis of how well current internet voting manufacturers understand and conform to the current requirement set with their own current implementation.

In the first stage, we drew on our experience as a longtime ITA/VSTL under the auspices of NASED and then EAC to interpret the requirements and project how each would fare in a real world situation. While a requirement might be theoretically sound, sometimes empirical implementations are not are meaningful, or are cost prohibitive. In addition to the content of the requirement set, we also looked at how the requirements are presented. Well presented requirements remove ambiguity and reduce the time and cost of a certification as all stakeholders can read the same requirement and have the same understanding of what is to be achieved. We expressed these ideas and points of view in section 4 of this document, as well as in the “SLI Comments” column of attachment A. As the UOCAVA program moves forward we believe that attention to these concepts will reap significant dividends.

In the second stage, we reviewed the documentation provided by each vendor and analyzed their respective systems. We determined not only how well their current systems achieved the requirement set, but also determine how well they each understood the intention of the requirements and the program.

In a summary of the full systems, as represented by Manufacturers 1 and 2, with regard to section 2, Functional Requirements, we believe that the manufacturers have a solid grasp of the fundamentals of the conduct of an election. How and what are contained in election definitions, how the election itself is conducted, and how the accumulation and tallying of the results is performed, are understood and well implemented.

In a summary of the ESVWs, with an emphasis on section 5, Security, as represented by Manufacturers 3, 4, 5, 6 and 7, it is our opinion that the industry is overall in a rudimentary phase. While basic security protocols seem to be

understood and generally in place, some of the more intricate aspects are not as well realized. In particular, the implementation of various FIPS compliant algorithms and protocols seems to cause confusion among many of the manufacturers. Several manufacturers expressed the opinion that they were using technologies that are sufficiently robust in terms of security, and as such did not need to concern themselves with how the security is implemented. It did not seem well understood that in the regulatory field it is not enough to claim compliance, but that each requirement must be not only implemented but also proven, whether that be by third party specification, manufacturer documentation, inspection, functional test, or source code review.

Byproducts of this project, which may well need to be addressed by a program manual, include necessities such as the ability to have adequate access to the systems under review. Some systems are self contained and can be delivered to the compliance testing entity for certification, but others are widely distributed as in a cloud environment.

Related to the remote environment issue is the question of how best to validate requirements that may reach into a third party provider's environment. Potential legal issues will need to be addressed, preferably at the Program level. Some tests will not only go through third party internet service providers, but also potentially cross state and international lines. As Certified Information Systems Security Professionals (CISSP), our Security analysts have obligations that could potentially make them liable for unauthorized intrusive testing. An example of this would be penetration testing into a voting system that resides in a cloud environment. SLI limited its penetration testing to in-house systems due to concerns over federal laws such as United States Code (USC) Title 18 Section 1030 "Fraud and related activity in connection with computers", "Computer Fraud and Abuse Act" which also amended USC Title 18 Section 1030, the Digital Millennium Copyright Act". SLI also had discussions with a representative of the FBI's Cyber Division, in which concern was expressed in regards to the penetration testing going over public domains and across international boundaries.

Another area that may need to be addressed at a program level, as well as in the requirements document, is the concept of "ballot delivery" systems. Several of the manufacturers in the pilot project declared their systems as ballot delivery systems in that they only present the ballot to the voter, and once the voter has cast the ballot they have to manually deliver the ballot, whether that is by email, fax or traditional mail. This being the case, the manufacturers were of the opinion that many security requirements did not pertain to them, as in the areas of transmissions and encryption. SLI disagrees with that assessment. During some of our testing we did notice Personally Identifiable Information (PII) was contained in some of the ballot delivery transmissions, which would cause the need for applicable security implementations.

End of Test Report

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
Section 1: Overview														
Section 2: Functional Requirements														
	2.1 Accuracy													
						"Shall" should be removed from header	the system SHALL achieve a target error rate of no more than one in 10,000,000 ballot positions,							
							a maximum acceptable error rate in the test process of one in 500,000 ballot positions.							
	2.1.1 Components and Hardware	x		x			Contained (or referenced) in test plans. How to specifically measure needs to be defined.							
	2.1.1.1 Component accuracy	x		x		1) Standards are recommended to specify appropriate component accuracy 2) This is better suited to Inspection, viewing the results overall of the testing, as well as review of hardware manufacturer specifications	Memory hardware, such as semiconductor devices and magnetic storage media, SHALL be accurate	2.1.2	Memory hardware, such as semiconductor devices and magnetic storage media, must be accurate.	14, May, 2011 @ 0835 2, June, 2011 @ 1318 6, June, 2011 @ 0830 Documentation: Pass Functional: Pass	23, May, 2011 @ 0754 Documentation: Pass Functional: Pass		1	
	2.1.1.2 Equipment design	x		x		This should be Inspection / Review of hardware test reports and/or hardware specifications.	The design of equipment in all voting systems SHALL provide for protection against mechanical, thermal, and electromagnetic stresses that impact voting system accuracy	2.1.2	The design of equipment in all voting systems shall provide for the highest possible levels of protection against mechanical, thermal, and electromagnetic stresses that impact system accuracy. Section 4 provides additional information on susceptibility requirements.	9, May, 2011 @ 1428 Documentation: Pass Functional: Pass	23, May, 2011 @ 0754 Documentation: Pass Functional: Pass		1	
	2.1.1.3 Voting system accuracy	x		x			To ensure vote accuracy, all voting systems SHALL:		To ensure vote accuracy, all systems shall:					
		x		x			a. Record the election contests, candidates, and issues exactly as defined by election officials;	2.1.2 a	a. Record the election contests, candidates, and issues exactly as defined by election officials	9, May, 2011 @ 1428 Documentation: Pass Functional: Pass	23, May, 2011 @ 0754 Documentation: Pass Functional: Pass	1		
		x		x			b. Record the appropriate options for casting and recording votes;	2.1.2 b	b. Record the appropriate options for casting and recording votes	14, May, 2011 @ 1403 24, May, 2011 @ 0932 Documentation: Pass Functional: Pass	23, May, 2011 @ 1335 Documentation: Pass Functional: Pass	1		
		x		x			c. Record each vote precisely as indicated by the voter and be able to produce an accurate report of all votes cast;	2.1.2 c	c. Record each vote precisely as indicated by the voter and produce an accurate report of all votes cast;	14, May, 2011 @ 1403 24, May, 2011 @ 0932 25, May, 2011 @ 0735 Documentation: Pass Functional: Pass	1, June, 2011 @ 1400 Documentation: Pass Functional: Pass	1		
		x		x		1) Recommend this as Inspection. 2) Best suited for a source code review and environment specification, in particular for data at rest.	d. Include control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) to demonstrate that the voting system has been designed for accuracy; and	2.1.2 d	d. Include control logic and data processing methods incorporating parity and checksums (or equivalent error detection and correction methods) to demonstrate that the system has been designed for accuracy	14, May, 2011 @ 1403 24, May, 2011 @ 0932 Documentation: Pass Functional: Pass	1, June, 2011 @ 1400 Documentation: Pass Functional: Pass	1		
		x		x		1) Recommend this as Inspection. As written, this requirement is only looking to verfiy that the monitoring software is provided. 2) Would recommend that the "…and how they were corrected." portion be broken out to another requirement, as this looks to be more of an event log.	e. Provide software that monitors the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected.	2.1.2 e	e. Provide software that monitors the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected	14, May, 2011 @ 1403 Documentation: Pass Functional: Pass	1, June, 2011 @ 1400 Documentation: Pass Functional: Pass	1		
								2.1.2 f	f. As an additional means of ensuring accuracy in DRE systems, voting devices shall record and retain redundant copies of the original ballot image. A ballot image is an electronic record of all votes cast by the voter, including undervotes.					
								2.1.3	Error Recovery.					
								2.1.3	To recover from a non-catastrophic failure of a device, or from any error or malfunction thatis within the operator's ability to correct, the system shall provide the following capabilities:					
								2.1.3 a	Restoration of the device to the operating condition existing immediately prior to the error or failure, without loss or corruption of voting data previously stored in the device					
								2.1.3 b	b. Resumption of normal operation following the correction of a failure in a memory component, or in a data processing component, including the central processing unit					
								2.1.3 c	c. Recovery from any other external condition that causes equipment to become inoperable, provided that catastrophic electrical or mechanical damage due to external phenomena has not occurred					

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
	2.1.2 Environmental Range	x		x		This should be Inspection / Review of hardware test reports and/or hardware specifications. As written this requirement seems to be written more for a traditional voting system than a UOCAVA internet based system.	All voting systems SHALL meet the accuracy requirements over manufacturer specified operating conditions and after storage under non-operating conditions.			Conditions not specified	Conditions not specified		1	
	2.1.3 Content of Data Verified for Accuracy													
								2.1.4	Integrity					
									Integrity measures ensure the physical stability and function of the vote recording and counting processes. To ensure system integrity, all systems shall:					
								2.1.4 a	a. Protect against a single point of failure that would prevent further voting at the polling place					
								2.1.4 b	b. Protect against the interruption of electrical power					
								2.1.4 d	d. Protect against ambient temperature and humidity fluctuations					
								2.1.4 e	e. Protect against the failure of any data input or storage device					
								2.1.4 f	f. Protect against any attempt at improper data entry or retrieval					
								2.1.4 g	g. Record and report the date and time of normal and abnormal events					
								2.1.4 h	h. Maintain a permanent record of all original audit data that cannot be modified or overridden but may be augmented by designated authorized officials in order to adjust for errors or omissions (e.g., during the canvassing process)					
								2.1.4 i	Detect and record every event, including the occurrence of an error condition that the system cannot overcome, and time-dependent or programmed events that occur without the intervention of the voter or a polling place operator					
								2.1.4 j	Include built-in measurement, self-test, and diagnostic software and hardware for detecting and reporting the system's status and degree of operability					
								2.1.4 k	k. For DRE; Maintain a record of each ballot cast using a process and storage location that differs from the main vote detection, interpretation, processing, and reporting path					
								2.1.4 l	l. For DRE; Provide a capability to retrieve ballot images in a form readable by humans					
	2.1.3.1 Election management system accuracy	x		x		As written, this requirement contains a high degree of vagueness. Each type of EM data should be enumerated.	Voting systems SHALL accurately record all election management data entered by the user, including election officials or their designees.	4.1.3	Election Management System Requirements	12, May, 2011 @ 1505 6, June, 2011 @ 1210 Documentation: Pass Functional: Pass	Documentation: Pass Functional: Pass		1	
	2.1.3.2 Recording accuracy	x		x			For recording accuracy, all voting systems SHALL:	4.1.3.1	Recording Requirements. Voting systems shall accurately record all election management data entered by the user,					
		x		x			a. Record every entry made by the user except where it violates voter privacy;	4.1.3.1 a	Record every entry made by the user	12, May, 2011 @ 1505 6, June, 2011 @ 1210 Documentation: Pass Functional: Pass	Documentation: Pass Functional: Pass	1		
		x		x		Recommend that the "... to memory" portion be removed. Is potentially too specific of a data recording method.	b. Accurately interpret voter selection(s) and record them correctly to memory;	4.1.3.1 b	Add permissible voter selections correctly to the memory components of the device	12, May, 2011 @ 1505 6, June, 2011 @ 1210 Documentation: Pass Functional: Pass	Documentation: Pass Functional: Pass		1	
		x		x		It is not clear how this requirement is examining anything different from part b.	c. Verify the correctness of detection of the user selections and the addition of the selections correctly to memory;	4.1.3.1 c	Verify the correctness of detection of the user selections and the addition of the selections correctly to memory	12, May, 2011 @ 1505 6, June, 2011 @ 1210 Documentation: Pass Functional: Pass	Documentation: Pass Functional: Pass	1		
						Our assumption here is that this requirement is testing write-ins as opposed to selecting choices, as in b and c. This requirement (b,c, and d) need to be clarified as to their specific intents, with any redundancies removed.	d. Verify the correctness of detection of data entered directly by the user and the addition of the selections correctly to memory; and	4.1.3.1 e	Verify the correctness of detection of data entered directly by the user and the addition of the selections correctly to memory	12, May, 2011 @ 1505 6, June, 2011 @ 1210 Documentation: Pass Functional: Pass	Documentation: Pass Functional: Pass		1	
		x		x		2.1.3.2.e would be coverd under EMC testing. This should be Inspection / Review of hardware test reports and/or hardware specifications.	e. Preserve the integrity of election management data stored in memory against corruption by stray electromagnetic emissions, and internally generated spurious electrical signals.	4.1.3.1 f	Preserve the integrity of election management data stored in memory against corruption by stray electromagnetic emissions, and internally generated spurious electrical signals	12, May, 2011 @ 1505 6, June, 2011 @ 1210 Documentation: Pass Functional: Pass	Documentation: Pass Functional: Pass			1

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
	2.1.4 Telecommunications Accuracy	x		x		For telecommunications, if TCP/IP protocols are used all transmissions are guaranteed to be accurate. The discussion of one in ten million and one in half a milion is somewhat obfuscated, the requirement should be more clearly defined stated.	The telecommunications components of all voting systems SHALL achieve a target error rate of no more than one in 10,000,000 ballot positions, with a maximum acceptable error rate in the test process of one in 500,000 ballot positions.			12, May, 2011 @ 1505 6, June, 2011 @ 1210 Documentation: Pass Functional: Pass	Documentation: Pass Functional: Pass		1	
	2.1.5 Accuracy Test Content	x		x		For a true internet voting system, that uses a web browser implementation for capturing votes, the accuracy test is whether or not the election is coded correctly. The technologies involved are mature, proven and robust. For a true internet voting system that employs physical devices such as a touch screen, the accuracy test would be similar to that of a ballot delivery system, in that the touch screen is dependent on the prescribed maintenance cycle of the device. For a ballot delivery system, where the cast ballot is potentially returned in any of a number or ways (fax, email, printed/scanned), the accuracy is dependent on the device used, within the confines of the prescribed maintenance cycles of the device.	Voting system accuracy SHALL be verified by a specific test conducted for this objective. The overall test approach is described in Appendix C.			12, May, 2011 @ 1505 6, June, 2011 @ 1210 Documentation: Pass Functional: Pass	Documentation: Pass Functional: Pass		1	
	2.1.5.1 Simulators	x		x		Not a voting system requirement	If a simulator is used, it SHALL be verified independently of the voting system in order to produce ballots as specified for the accuracy testing.	2.2.4 g	Resident test software, external devices, and special purpose test software connected to or installed in voting equipment to simulate operator and voter functions may be used for these tests provided that the following standards are met:					1
	2.1.5.2 Ballots	x		x		Question as to the applicability of the ballot type to accuracy testing. Accuracy testing concerns itself with accuracy with regard to the scanning/reading of each possible ballot position on a given size ballot. The ability of the system to correctly handle the various supported voting variations is addressed in other specific tests.	Ballots used for accuracy testing SHALL include all the supported types (i.e., rotation, alternative languages) of contests and election types (primary, general).	2.2.4 g	g. These elements shall be capable of being tested separately, and shall be proven to be reliable verification tools prior to their use	12, May, 2011 @ 1505 6, June, 2011 @ 1210 Documentation: Pass Functional: Pass	Documentation: Pass Functional: Pass with General election		1	
								4.1.6.2	DRE System Processing Requirements					
	2.1.6 Reporting Accuracy	x		x			Processing accuracy is defined as the ability of the voting system to process stored voting data. Processing includes all operations to consolidate voting data after the voting period has ended.	4.1.6.2 b	Processing accuracy is defined as the ability of the system to process voting data stored in DRE voting devices or in removable memory modules installed in such devices. Processing includes all operations to consolidate voting data after the polls have been closed. DRE voting systems shall:	12, May, 2011 @ 0942 Documentation: Pass Functional: Pass	Documentation: Pass Functional: Pass	1		
		x		x		In general this is a bit high level, would like to see some specific metrics called out to ensure reporting accuracy. Similar v1.0 VVSG volume 1, sections 2.4.2. and 2.4.3	The voting systems SHALL produce reports that are consistent, with no discrepancy among reports of voting data.	4.1.6.2 b.i	Produce reports that are completely consistent, with no discrepancy among reports of voting device data produced at any level	12, May, 2011 @ 0942 Documentation: Pass Functional: Pass	Documentation: Pass Functional: Pass		1	
								4.1.6.2 b.ii	Produce consolidated reports containing absentee, provisional or other voting data that are similarly error-free. Any discrepancy, regardless of source, is resolvable to a procedural error, to the failure of a non-memory device or to an external cause					
												8	10	2
	2.2 Operating capacities													

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
	2.2.1 Maximum Capacities	x		x		Recommend that this section look at capacities more in terms of minimums that need to be met (as specified by NIST/FVAP), rather than as stated maximum capacities that a manufacturer claims they can accommodate. Many times a manufacturer will list an unrealistically high number for many of these categories. A minimum standard will create a consistent baseline for all manufacturers.	The manufacturer SHALL specify at least the following maximum operating capacities for the voting system (i.e. server, vote capture device, tabulation device, and communications links):						1	
		x		x			Throughput,			12, May, 2011 @ 1505 6, June, 2011 @ 1210 Documentation: Pass Functional: Pass Tested, with throughput bottleneck encountered. Though due to less than production equipment	Documentation: Pass Functional: Pass Maximum throughput not achieved without automation.	1		
		x		x			. Memory,			12, May, 2011 @ 1505 6, June, 2011 @ 1210 Documentation: Pass Functional: Pass Tested, with memory bottleneck encountered. Though due to less than production equipment	Documentation: Pass Functional: Pass Maximum memory usage not achieved without automation.	1		
		x		x			. Transaction processing speed, and			12, May, 2011 @ 1505 6, June, 2011 @ 1210 Documentation: Pass Functional: Pass	Documentation: Pass Functional: Pass Maximum transaction processing not achieved without automation.	1		
		x		x			. Election constraints:			12, May, 2011 @ 1505 6, June, 2011 @ 1210 Documentation: Pass Functional: Pass	Documentation: Pass Functional: Pass	1		
		x		x			o Number of jurisdictions			12, May, 2011 @ 1505 6, June, 2011 @ 1210 Documentation: Pass Functional: Pass	Documentation: Pass Functional: Pass	1		
		x		x			o Number of ballot styles per jurisdiction			12, May, 2011 @ 1505 6, June, 2011 @ 1210 Documentation: Pass Functional: Pass	Documentation: Pass Functional: Pass	1		
		x		x			o Number of contests per ballot style			12, May, 2011 @ 1505 6, June, 2011 @ 1210 Documentation: Pass Functional: Pass	Documentation: Pass Functional: Pass	1		
		x		x			o Number of candidates per contest			12, May, 2011 @ 1505 6, June, 2011 @ 1210 Documentation: Pass Functional: Pass	Documentation: Pass Functional: Pass	1		

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
		x		x			o Number of voted ballots			12, May, 2011 @ 1505 6, June, 2011 @ 1210 Documentation: Pass Functional: Pass	Documentation: Pass Functional: Pass	1		
	2.2.1.1 Capacity testing	x		x		Recommend making the Test Method for this item Inspection/Functional. Some instances can be impractical to functionally validate within a reasonable cost/benefit ratio.	The voting system SHALL achieve the maximum operating capacities stated by the manufacturer in section 2.2.1.			12, May, 2011 @ 1505 6, June, 2011 @ 1210 Documentation: Pass Functional: Pass	Documentation: Pass Functional: Pass Tested though not all maximums achieved		1	
	2.2.2 Operating Capacity notification	x		x		Recommend making the Test Method for this item Inspection/Functional. Some instances can be impractical to functionally validate within a reasonable cost/benefit ratio.	The voting system SHALL provide notice when any operating capacity is approaching its limit.			12, May, 2011 @ 1505 6, June, 2011 @ 1210 Tested though no notice provided	Documentation: Pass Functional: Pass Tested though no notice provided	1		
	2.2.3 Simultaneous Transmissions	x		x		Recommend making the Test Method for this item Inspection/Functional. Some instances can be impractical to functionally validate within a reasonable cost/benefit ratio.	The voting system SHALL protect against the loss of votes due to simultaneous transmissions.			12, May, 2011 @ 1505 6, June, 2011 @ 1210 Documentation: Pass Functional: Pass	Documentation: Pass Functional: Pass	1		
												11	2	
	2.3 Pre-Voting Capabilities					For the UOCAVA program, is it needed to include voter registration credentials?		2.2	Pre-voting Capabilities					
								2.2.1	Ballot Preparation					
	2.3.1 Import and Verify Election Definition	x	x	x	x		Contained in test plans; Election Definition and Ballot Layout Manager	2.1.6	Election Management System					
	2.3.1.1 Import the election definition	x	x				The voting system SHALL:	2.1.6	An EMS shall generate and maintain a database, or one or more interactive databases, that election officials or their designees to perform the following functions:					
		x	x					2.1.6	Generate ballots and election-specific programs for voting equipment					
								2.1.6	Install ballots and election-specific programs					
				x	x	Agree with Requirement	a. Keep all data logically separated by, and accessible only to, the appropriate state and local jurisdictions;	2.1.6	Define political subdivision boundaries and multiple election districts as indicated in the system documentation	10, May, 2011 @ 0845 14, May, 2011 @ 0714 Documentation: Pass Functional: Insufficient Robustness data not separated	7, June, 2011 @ 1502 Documentation: Pass Functional: Insufficient Robustness data not separated	1		
								2.2.2	Election Programming					
								2.2.2 a	Logical definition of the ballot, including the definition of the number of allowable choices for each office and contest					
								2.2.2 b	Logical definition of political and administrative subdivisions, where the list of candidates or contests varies between polling places					
		x	x	x	x	Enumerate the activities	b. Provide the capability to import or manually enter ballot content, ballot instructions and election rules, including all required alternative language translations from each jurisdiction;	2.1.6	Identify contests, candidates, and issues; Define ballot formats and appropriate voting options	10, May, 2011 @ 0912 2, June, 2011 @ 0725 Documentation: Pass Functional: Pass	7, June, 2011 @ 1510 Documentation: Pass Functional: Pass	1		
								2.2.1.1 a	Enabling the automatic formatting of ballots in accordance with the requirements for offices, candidates, and measures qualified to be placed on the ballot for each political subdivision and election district					
								2.2.1.2	Ballot Formatting					
								2.2.1.3	Ballot Production					
		x	x	x	x	Agree with Requirement	c. Provide the capability for the each jurisdiction to verify that their election definition was imported accurately and completely;	2.1.6	Test that ballots and programs have been properly prepared and installed	2, June, 2011 @ 0749 Documentation: Pass Functional: Pass	7, June, 2011 @ 1520 Documentation: Pass Functional: Pass	1		
								2.2.3	Ballot and Program Installation and Control					

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
		x	x	x	x	Agree with Requirement	d. Support image files (e.g., jpg or gif) andor a handwritten signature image on the ballot so that state seals, official signatures and other graphical ballot elements may be properly displayed; and			2, June, 2011 @ 0749 Documentation: Pass Functional: Pass	7, June, 2011 @ 1525 Tested, graphical images not supported	1		
		x	x	x	x	Agree with Requirement	e. Support multiple ballot styles per each local jurisdiction.		Define ballot formats and appropriate voting options	14, May, 2011 @ 0755 Documentation: Pass Functional: Pass	7, June, 2011 @ 1540 Documentation: Pass Functional: Pass	1		
	2.3.1.2 Protect the election definition	x	x	x		Agree with Requirement	The voting system SHALL provide a method to protect the election definition from unauthorized modification.	2.2.1.2	Ballot Formatting; f. Prevention of unauthorized modification of any ballot formats	13, May, 2011 @ 1632 Documentation: Pass Functional: Pass	7, June, 2011 @ 1603 Documentation: Pass Functional: Pass	1		
	2.3.2 Readiness Testing							2.2.4	Readiness Testing					
								2.1.6	Test that ballots and programs have been properly prepared and installed					
	2.3.2.1 Voting system test mode	x		x		Agree with Requirement	The voting system SHALL provide a test mode to verify that the voting system is correctly installed, properly configured, and all functions are operating to support pre-election readiness testing for each jurisdiction.	2.2.4 a	Verify that voting equipment and precinct count equipment is properly prepared for an election, and collect data that verifies equipment readiness	13, May, 2011 @ 1657 Documentation: Insufficient Robustnes Functional: Insufficient Robustness data not separated No test mode provided	7, June, 2011 @ 1609 Documentation: Insufficient Robustnes Functional: Insufficient Robustness data not separated No test mode provided	1		
								2.2.4 b	Obtain status and data reports from each set of equipment					
								2.2.4 c	Verify the correct installation and interface of all voting equipment					
								2.2.4 d	Verify that hardware and software function correctly					
						This requirement would cover from the voting phase to the tallying and reporting, not necessarily including the election definition portion.	u. Provide the ability for election officials to submit test ballots for use in verifying the end-to-end integrity of the voting system	2.2.4 e	Generate consolidated data reports at the polling place and higher jurisdictional levels	12, May, 2011 @ 1505 6, June, 2011 @ 1210 Documentation: Pass Functional: Pass	Documentation: Pass Functional: Pass			
								2.2.4	Resident test software, external devices, and special purpose test software connected to or installed in voting equipment to simulate operator and voter functions may be used for these tests provided that the following standards are met:					
								2.2.4 g	These elements shall be capable of being tested separately, and shall be proven to be reliable verification tools prior to their use					
								2.2.4 h	These elements shall be incapable of altering or introducing any residual effect on the intended operation of the voting device during any succeeding test and operational phase					
									Paper-based systems shall:					
								2.2.4 i	i. Support conversion testing that uses all potential ballot positions as active positions					
								2.2.4 j	j. Support conversion testing of ballots with active position density for systems without pre-designated ballot positions					
	2.3.2.2 Test data segregation	x		x		Agree with Requirement	The voting system SHALL provide the capability to zero-out or otherwise segregate test data from actual voting data.	2.1.8	a. Can be set to zero before any ballots are submitted for tally	12, May, 2011 @ 0942 3, June, 2011 @ 0821 Documentation: Pass Functional: Pass	1, June, 2011 @ 1526 7, June, 2011 @ 1640 Documentation: Pass Functional: Pass	1		
								2.2.4 f	f. Segregate test data from actual voting data, either procedurally or by hardware/software features					
								2.3.3.3 v	Isolate test ballots such that they are accounted for accurately in vote counts and are not reflected in official vote counts for specific candidates or measures					
								2.2.5	Verification at the Polling Place					
									Election officials perform verification at the polling place to ensure that all voting systems and voting equipment function properly before and during an election. All voting systems shall provide a formal record of the following, in any media, upon verification of the authenticity of the command source:					
								2.2.5 a	The election's identification data					
								2.2.5 b	The identification of all equipment units					
								2.2.5 c	The identification of the polling place					
								2.2.5 d	The identification of all ballot formats					
								2.2.5 e	The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain only zeros)					

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
								2.2.5 f	A list of all ballot fields that can be used to invoke special voting options					
								2.2.5 g	Other information needed to confirm the readiness of the equipment, and to accommodate administrative reporting requirements					
								2.2.5	To prepare voting devices to accept voted ballots, all voting systems shall provide the capability to test each device prior to opening to verify that each is operating correctly. At a minimum, the tests shall include:					
								2.2.5 h	Confirmation that there are no hardware or software failures					
								2.2.5. i	Confirmation that the device is ready to be activated for accepting votes					
								2.2.5	If a precinct count system includes equipment for the consolidation of polling place data at one or more central counting locations, it shall have means to verify the correct extraction of voting data from transportable memory devices, or to verify the transmission of secure data over secure communication links.					
								2.2.6	Verification at the Central Location					
									Election officials perform verification at the central location to ensure that vote counting and vote consolidation equipment and software function properly before and after an election. Upon verification of the authenticity of the command source, any system used in a central count environment shall provide a printed record of the following:					
								2.2.6 a	a. The election's identification data					
								2.2.6 b	b. The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain all zeros)					
								2.2.6 c	c. Other information needed to ensure the readiness of the equipment and to accommodate administrative reporting requirements					
												8		
	2.4 Voting Capabilities													
	2.4.1 Opening the Voting Period	x												
	2.4.1.1 Accessing the ballot	x					The voting system SHALL:							
		x		x		Agree with Requirement	a. Present the correct ballot style to each voter;			2, June, 2011 @ 0915 Documentation: Pass Functional: Pass	2, June, 2011 @ 0935 7, June, 2011 @ 1658 Documentation: Pass Functional: Pass	1		
		x		x		Agree with Requirement	b. Allow the voting session to be canceled; and			2, June, 2011 @ 0915 Documentation: Pass Functional: Pass	2, June, 2011 @ 1233 7, June, 2011 @ 1700 Documentation: Pass Functional: Pass	1		
		x		x		Agree with Requirement	c. Prevent a voter from casting more than one ballot in the same election.			2, June, 2011 @ 0915 Documentation: Pass Functional: Pass	2, June, 2011 @ 0950 7, June, 2011 @ 1703 Documentation: Pass Functional: Pass	1		
								2.3	Voting Capabilities					
								2.3.1	Opening the Polls					
								2.3.1.1	Precinct Count Systems					
								2.3.1.2	Paper-based System Requirements					
								2.3.1.3	DRE System Requirements					
								2.3.1.2	Paper-based System Requirements					
								2.3.1.3	DRE System Requirements					
								2.3.2	Activating the Ballot (DRE Systems)					
	2.4.2 Casting a Ballot	x				There should be a sub-requirement that deals with the system allowing the voter to change their selection within a contest prior to casting their ballot (similar to (g) for undervotes)	The voting system SHALL:	2.3.3	Casting a Ballot				1	
	2.4.2.1 Record voter selections	x		x		Agree with Requirement	a. Record the selection and non-selection of individual vote choices;	2.3.3.1 c	Record the selection and non-selection of individual vote choices for each contest and ballot measure	11, May, 2011 @ 0847 24, May, 2011 @ 0932 Documentation: Pass Functional: Pass	7, June, 2011 @ 1705 Documentation: Pass Functional: Pass	1		
								2.3.3.2 b	b. Allow the voter to mark the ballot to register a vote					

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
		x		x		Recommend splitting sub-requirement so that one validates the ability to enter a write in, and the other verifies that the correct number of write-ins is allowed	b. Record the voter's selection of candidates whose names do not appear on the ballot, if permitted under state law, and record as many write-ins as the number of candidates the voter is allowed to select;	2.3.3.1 d	Record the voter's selection of candidates whose names do not appear on the ballot, if permitted under state law, and record as many write-in votes as the number of candidates the voter is allowed to select	11, May, 2011 @ 0847 24, May, 2011 @ 0932 Documentation: Pass Functional: Pass	7, June, 2011 @ 1722 Documentation: Pass Functional: Pass	1		
		x		x		Agree with Requirement	c. Prohibit the voter from accessing or viewing any information on the display screen that has not been authorized and preprogrammed into the voting system (i.e., no potential for display of external information or linking to other information sources);	2.3.3.3 a	(DRE) Prohibit the voter from accessing or viewing any information on the display screen that has not been authorized by election officials and preprogrammed into the voting system (i.e., no potential for display of external information or linking to other information sources)	11, May, 2011 @ 0847 24, May, 2011 @ 0932 Documentation: Pass Functional: Pass	7, June, 2011 @ 1727 Documentation: Pass Functional: Pass	1		
		x		x		Agree with Requirement	d. Allow the voter to change a vote within a contest before advancing to the next contest;			11, May, 2011 @ 0847 24, May, 2011 @ 0932 Documentation: Pass Functional: Pass	7, June, 2011 @ 1731 Documentation: Pass Functional: Pass	1		
		x		x		Agree with Requirement	e. Provide unambiguous feedback regarding the voter's selection, such as displaying a checkmark beside the selected option or conspicuously changing its appearance;	2.3.3.3 d	(DRE) Indicate that a selection has been made or canceled	11, May, 2011 @ 0847 24, May, 2011 @ 0932 Documentation: Pass Functional: Pass	7, June, 2011 @ 1733 Documentation: Pass Functional: Pass	1		
		x		x		Recommend that this requirement is made more specific as to notifying voter of potential undervote prior to casting of ballot (as opposed to when going from one contest (or screen) to another).	f. Indicate to the voter when no selection, or an insufficient number of selections, has been made for a contest (e.g., undervotes);	2.3.3.2 e; 2.3.3.3 e	Provide feedback to the voter that identifies specific contests for which he or she has made no selection or fewer than the allowable number of selections (e.g., undervotes)	11, May, 2011 @ 0847 24, May, 2011 @ 0932 Documentation: Pass Functional: Pass	7, June, 2011 @ 1735 Documentation: Pass Functional: Pass	1		
		x		x		Agree with Requirement	g. Provide the voter the opportunity to correct the ballot for an undervote before the ballot is cast;	2.3.3.2 h	Provide the voter opportunity to correct the ballot for either an undervote or overvote before the ballot is cast and counted	11, May, 2011 @ 0847 24, May, 2011 @ 0932 Documentation: Pass Functional: Pass	7, June, 2011 @ 1738 Documentation: Pass Functional: Pass	1		
		x		x		Agree with Requirement	h. Allow the voter, at the voter's choice, to submit an undervoted ballot without correction.			11, May, 2011 @ 0847 24, May, 2011 @ 0932 Documentation: Pass Functional: Pass	7, June, 2011 @ 1739 Documentation: Pass Functional: Pass	1		
		x		x		Agree with Requirement	i. Prevent the voter from making more than the allowable number of selections for any contest (e.g., overvotes); and	2.3.3.2 f; 2.3.3.3 f	Notify the voter if he or she has made more than the allowable number of selections for any contest (e.g., overvotes)	11, May, 2011 @ 0847 24, May, 2011 @ 0932 Documentation: Pass Functional: Pass	7, June, 2011 @ 1741 Documentation: Pass Functional: Pass	1		
		x		x		This may not be feasible in a remote session environment. Depending on where the power failure occurs, as well as the duration, will dictate if a ballot can be recorded within the voting system without loss or degradation of voting/audit data. The "… allow voters to resume voting…" clause would inherently cause some kind of voter data to be resident on the vote capture device, which would potentially violate other Security requirements (5.4.1.3)	j. In the event of a failure of the main power supply external to the voting system, provide the capability for any voter who is voting at the time to complete casting a ballot, allow for the successful shutdown of the voting system without loss or degradation of the voting and audit data, and allow voters to resume voting once the voting system has reverted to back-up power.	2.3.3.1 e	In the event of a failure of the main power supply external to the voting system, provide the capability for any voter who is voting at the time to complete casting a ballot, allow for the successful shutdown of the voting system without loss or degradation of the voting and audit data, and allow voters to resume voting once the voting system has reverted to back-up power.	14, May, 2011 @ 1403 Documentation: Pass Functional: NT All main power failure tests. Steps developed but not testable with the current configuration" for Manufacturer.	7, June, 2011 @ 1743 Documentation: Pass Functional: Insufficient Robustness Tested, power loss results in need to redo ballots if not cast.		1	
								2.3.3.1 f	Provide the capability for voters to continue casting ballots in the event of a failure of a telecommunications connection within the polling place or between the polling place and any other location		7, June, 2011 @ 1744 Documentation: Pass Functional: Pass			
	2.4.2.2 Verify voter selections	x					The voting system SHALL:	2.3.3.3 k	For electronic image displays, prompt the voter to confirm the voter's choices before casting his or her ballot, signifying to the voter that casting the ballot is irrevocable and directing the voter to confirm the voter's intention to cast the ballot					

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
		x		x		Would recommend that a paper record is generated only when the ballot is cast and not each time the confirmation screen is accessed.	a. Produce a paper record each time the confirmation screen is displayed;		Provide a capability to retrieve ballot images in a form readable by humans [in accordance with the requirements of Subsections 2.1.2 (f) and 2.1.4 (k) and (l)]	14, May, 2011 @ 1403 24, May, 2011 @ 1256 Documentation: Insufficient Robustness Functional: Insufficient Robustness No paper record made available	7, June, 2011 @ 1746 Documentation: Insufficient Robustness Functional: Insufficient Robustness No paper record made available	1		
		x		x		Agree with Requirement	b. Generate a paper record identifier. This SHALL be a random identifier that uniquely links the paper record with the cast vote record;			14, May, 2011 @ 1403 24, May, 2011 @ 0932 Documentation: Insufficient Robustness	7, June, 2011 @ 1749 Documentation: Insufficient Robustness Functional: Insufficient Robustness	1		
		x		x		Recommend removing "... and paper record", see comment to "a" above.	c. Allow the voter to either cast the ballot or return to the vote selection process to make changes after reviewing the confirmation screen and paper record; and	2.3.3.3 j	Allow the voter, before the ballot is cast, to review his or her choices and, if the voter desires, to delete or change his or her choices before the ballot is cast	11, May, 2011 @ 0847 24, May, 2011 @ 0932 Documentation: Pass Functional: Pass, though no paper record	7, June, 2011 @ 1751 Documentation: Pass Functional: Pass, though no paper record	1		
		x		x		Agree with Requirement	d. Prompt the voter to confirm his choices before casting the ballot, signifying to the voter that casting the ballot is irrevocable and directing the voter to confirm his intention to cast the ballot.	2.3.3.3 k	For electronic image displays, prompt the voter to confirm the voter's choices before casting his or her ballot, signifying to the voter that casting the ballot is irrevocable and directing the voter to confirm the voter's intention to cast the ballot	24, May, 2011 @ 0932 Documentation: Pass Functional: Pass	7, June, 2011 @ 1752 Documentation: Pass Functional: Pass	1		
	2.4.2.3 Cast ballot	x				Recommend renaming requirement to "Post Cast Ballot Process"	The voting system SHALL:							
		x		x		Agree with Requirement	a. Store all cast ballots in a random order; logically separated by, and only accessible to, the appropriate state local jurisdictions;			14, May, 2011 @ 1403 24, May, 2011 @ 1332 3, June, 2011 @ 0846 Documentation: Pass Functional: Pass	7, June, 2011 @ 1754 Documentation: Pass Functional: Pass	1		
		x		x		Recommend defining "persistently" to more detail. In a full electronic system, "persistently" would indicate that the central server has received the vote record and stored it. In a ballot delivery system, "persistently" would indicate the printing of a physical ballot, or creation of a pdf.	b. Notify the voter after the vote has been stored persistently that the ballot has been cast;	2.3.3.3 l	(DRE) Notify the voter after the vote has been stored successfully that the ballot has been cast	11, May, 2011 @ 1030 3, June, 2011 @ 0836 Documentation: Pass Functional: Pass	7, June, 2011 @ 1757 Documentation: Pass Functional: Pass	1		
		x		x		Recommend enumerating this requirement to c.i and c.ii	c. Notify the voter that the ballot has not been cast successfully if it is not stored successfully, and provide clear instruction as to steps the voter should take to cast his ballot should this event occur; and	2.3.3.3 m	(DRE) Notify the voter that the ballot has not been cast successfully if it is not stored successfully, including storage of the ballot image, and provide clear instruction as to the steps the voter should take to cast his or her ballot should this event occur	24, May, 2011 @ 0747 Documentation: Pass Functional: Pass	7, June, 2011 @ 1800 Documentation: Pass Functional: Pass	1		
		x		x		Agree with Requirement	d. Prohibit access to voted ballots until such time as state law allows for processing of absentee ballots.	2.3.3.3 t	Prohibit access to voted ballots until after the close of polls	24, May, 2011 @ 0747 Documentation: Pass Functional: Pass	7, June, 2011 @ 1807 Documentation: Pass Functional: Pass	1		
	2.4.2.4 Ballot linking to voter identification	x	x					2.3.3.3 p	Prevent modification of the voter's vote after the ballot is cast					
	2.4.2.4.1 Absentee model	x		x		Agree with Requirement	The cast ballot SHALL be linked to the voter's identity without violating the privacy of the voter.	2.3.3.3 s	Protect the secrecy of the vote throughout the voting process	24, May, 2011 @ 0747 Documentation: Pass Functional: Pass	7, June, 2011 @ 1811 Documentation: Pass Functional: Pass	1		
	2.4.2.4.2 Early voting model		x		x	Agree with Requirement	The cast ballot SHALL NOT be linked to the voter's identity.	2.3.3.3 s	Protect the secrecy of the vote throughout the voting process	24, May, 2011 @ 0747 Not tested, beyond scope	7, June, 2011 @ 1812 Not tested, beyond scope	1		
	2.4.3 Vote Secrecy													

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
	2.4.3.1 Link to voter	x		x		In the Glossary, cast vote record needs a better definition, such that it is differentiated from the cast ballot more explicitly. Should indicate that it is the record stored in the voting system, as opposed to the cast ballot that is produced by the vote capture device. In the Absentee model the cast ballot contains links to the voters identity, where the cast vote record should not	The voting system SHALL be capable of producing a cast vote record that does not contain any information that would link the record to the voter.	2.3.3.1 b	Protect the secrecy of the vote such that the system cannot reveal any information about how a particular voter voted, except as otherwise required by individual state law	2, June, 2011 @ 0948 Documentation: Pass Functional: Pass	7, June, 2011 @ 1813 Documentation: Pass Functional: Pass		1	
	2.4.3.2 Voting session records	x		x		Audit logs would record when the voter accessed ballot, as well as when they cast the ballot, but no information that would link stored information to individual voter	The voting system SHALL NOT store any information related to the actions performed by the voter during the voting session.			24, May, 2011 @ 0747 Documentation: Pass Functional: Pass	7, June, 2011 @ 1815 Documentation: Pass Functional: Pass	1		
												23	3	
	2.5 Post Voting Capabilities							2.4	Post-Voting Capabilities					
									All voting systems shall provide capabilities to accumulate and report results for the jurisdiction and to generate audit trails. In addition, precinct count voting systems must provide a means to close the polls including generating appropriate reports. If the system provides the capability to broadcast results, additional standards apply					
	2.5.1 Ballot Box Retrieval and Tabulation	x				An additional requirement is recommended that explicitly deals with encryption of electornic ballot box upon closure of the voting period, in order to prevent voter data (private information and vote data) from being exposed in even a read only manner. "Seal" in 2.5.1.1 may be used to cover this concept. But then should be broken out to a seperate requirement from the "sign" portion.							1	
	2.5.1.1 Seal and sign the electronic ballot box	x		x		Would recommend that the term "seal" be more explicitly defined. "Seal" is historically more of a physical concept, whereas in this instance it is a logical concept. May want to define as making the electronic ballot box "read only", with corresponding time stamp or something similar.	The voting system SHALL seal and sign each jurisdiction's electronic ballot box, by means of a digital signature, to protect the integrity of its contents.	2.3.3.3 t	Prohibit access to voted ballots until after the close of polls	13, May, 2011 @ 1250 25, May, 2011 @ 0905 Documentation: Pass Functional: Pass	7, June, 2011 @ 1824 Documentation: Pass Functional: Pass		1	
	2.5.1.2 Electronic ballot box retrieval	x		x		Agree with Requirement	The voting system SHALL allow each jurisdiction to retrieve its electronic ballot box.			13, May, 2011 @ 1250 25, May, 2011 @ 0905 Documentation: Pass Functional: Pass	3, June, 2011 @ 1435 7, June, 2011 @ 1825 Documentation: Pass Functional: Pass	1		
	2.5.1.3 Electronic ballot box integrity check	x		x		See comments in 2.5.1 and 2.5.1.1, as would pertain to this requirement	The voting system SHALL perform an integrity check on the electronic ballot box verifying that it has not been tampered with or modified before opening.			13, May, 2011 @ 1250 25, May, 2011 @ 0905 Documentation: Pass Functional: Pass	7, June, 2011 @ 1825 Documentation: Pass Functional: Pass		1	
	2.5.2 Tabulation	x	x					2.1.7	Vote Tabulating Program					
								2.1.7.1	Functions					
									a. Monitor system status and generate machine-level audit reports					
									b. Accommodate device control functions performed by polling place officials and maintenance personnel					
									c. Register and accumulate votes					
									d.Accommodate variations in ballot counting logic					
	2.5.2.1 Tabulation device connectivity		x		x	Enumerate the activities	The tabulation device SHALL be physically, electrically, and electromagnetically isolated from any other computer network.			25, May, 2011 @ 1253 Documentation: Pass Functional: Pass	7, June, 2011 @ 1827 Documentation: Pass Functional: Pass	1		
	2.5.2.2 Open ballot box	x		x		Recommend adding "voting system" in front of "authorized entity"	The tabulation device SHALL allow only an authorized entity to open the ballot box.			25, May, 2011 @ 1253 Documentation: Pass Functional: Pass	7, June, 2011 @ 1828 Documentation: Pass Functional: Pass	1		
	2.5.2.3 Absentee model	x												

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
	2.5.2.3.1 Adjudication	x		x		1) See comment in 2.5.2.2 2) "electronic ballots" is not a defined term. Recommend using the term "Cast Ballot"	The tabulation device SHALL allow the designation of electronic ballots as "accepted" or "not accepted" by an authorized entity.			11, May, 2011 @ 1337 25, May, 2011 @ 1320 2, June, 2011 @ 0725 Documentation: Pass Functional: Pass	7, June, 2011 @ 1830 Documentation: Pass Functional: Pass		1	
	2.5.2.4 Ballot decryption	x		x		Decryption process may be different that what is used to break all correlations between voter and ballot. This requirement should be broken out. The breaking of the correlation should only be done after the adjudication is completed. The decryption process may be involved at multiple points of this overall process.	The tabulation device decryption process SHALL remove all layers of encryption and breaking all correlation between the voter and the ballot, producing a record that is in clear text.			25, May, 2011 @ 1253 Documentation: Pass Functional: Pass	7, June, 2011 @ 1833 Documentation: Pass Functional: Pass	1		
	2.5.2.5 Tabulation report format	x		x		Agree with Requirement	The tabulation device SHALL have the capability to generate a tabulation report of voting results in an open and non-proprietary format.			11, May, 2011 @ 1405 Documentation: Pass Functional: Pass	7, June, 2011 @ 1835 Documentation: Pass Functional: Pass	1		
								2.1.7.2	Voting Variations					
									There are significant variations among state election laws with respect to permissible ballot contents, voting options, and the associated ballot counting logic. The Technical Data Package accompanying the system shall specifically identify which of the following items can and cannot be supported by the voting system, as well as how the voting system can implement the items supported:					
									Closed primaries					
									• Open primaries					
									• Partisan offices					
									• Non-partisan offices					
									• Write-in voting					
									• Primary presidential delegation nominations					
									• Ballot rotation					
									• Straight party voting					
									• Cross-party endorsement					
									• Split precincts					
									• Vote for N of M					
									• Recall issues, with options					
									• Cumulative voting					
									• Ranked order voting					
									• Provisional or challenged ballots					
								2.1.8	Ballot Counter					
									For all voting systems, each piece of voting equipment that tabulates ballots shall provide a counter that:					
									a. Can be set to zero before any ballots are submitted for tally					
									b. Records the number of ballots cast during a particular test cycle or election					
									c. Increases the count only by the input of a ballot					
									d. Prevents or disables the resetting of the counter by any person other than authorized persons at authorized points					
									e. Is visible to designated election officials					
												5	4	
	2.6 Audit and Accountability	x				Assumption is that 2.6.1 and 2.6.2 are "header" sections that should not have any actionable events. The "Shall" in 2.6.2 should be removed.								
	2.6.1 Scope						The intention is to provide for independent verification of the agreement of the paper record and electronic tabulation results. These audits could be conducted on the entire set of records or on a sampling basis, depending on the preferences of state/local jurisdictions:	2.1.5	Election audit trails provide the supporting documentation for verifying the accuracy of reported election results. They present a concrete, indestructible archival record of all system activity related to the vote tally, and are essential for public confidence in the accuracy of the tally, for recounts, and for evidence in the event of criminal or civil litigation.					
				x			a. Hand audit – Validation of electronic tabulation results via comparison with results of a hand tally of paper records; and			25, May, 2011 @ 1320 Documentation: Pass Functional: Pass	Documentation: Pass Functional: Pass	1		
				x			b. Comparison of ballot images and the corresponding paper records.			25, May, 2011 @ 1320 Documentation: Pass Functional: Pass	Documentation: Pass Functional: Pass	1		

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
									The requirements for all system types, both precinct and central count, are described in generic language. Because the actual implementation of specific characteristics may vary from system to system, it is the responsibility of the vendor to describe each system's characteristics in sufficient detail so that test labs and system users can evaluate the adequacy of the system's audit trail. This description shall be incorporated in the System Operating Manual, which is part of the Technical Data Package.					
								2.1.5.1	Operational Requirements. Audit records shall be prepared for all phases of election operations performed using devices controlled by the jurisdiction or its contractors.					
									These records shall address the ballot preparation and election definition phase, system readiness tests, and voting and ballot-counting operations. The software shall activate the logging and reporting of audit data as described below.					
								2.1.5.1 a	a. The timing and sequence of audit record entries is as important as the data contained in the record. All voting systems shall meet the requirements for time, sequence and preservation of audit records outlined below.					
								2.1.5.1 a	i. Except where noted, systems shall provide the capability to create and maintain a real-time audit record. This capability records and provides the operator or precinct official with continuous updates on machine status. This information allows effective operator identification of an error condition requiring intervention, and contributes to the reconstruction of election-related events necessary for recounts or litigation.					
								2.1.5.1 a	ii. All systems shall include a real-time clock as part of the system's hardware. The system shall maintain an absolute record of the time and date or a record relative to some event whose time and data are known and recorded.					
								2.1.5.1 a	iii.All audit record entries shall include the time-and-date stamp.					
								2.1.5.1 a	iv. The audit record shall be active whenever the system is in an operating mode. This record shall be available at all times, though it need not be continually visible.					
								2.1.5.1 a	v. The generation of audit record entries shall not be terminated or altered by program control, or by the intervention of any person. The physical security and integrity of the record shall be maintained at all times.					
								2.1.5.1 a	vi. Once the system has been activated for any function, the system shall preserve the contents of the audit record during any interruption of power to the system until processing and data reporting have been completed.					
								2.1.5.2	Use of Shared Computing Platforms					
								2.1.5.2	Further requirements must be applied to Commercial-off-the-Shelf operating systems to ensure completeness and integrity of audit data for election software.					
								2.1.5.2	"Simultaneous processes" of concern include: unauthorized network connections, unplanned user logins, and unintended execution or termination of operating system processes.					
								2.1.5.2	Operating system audit shall be enabled for all session openings and closings, for all connection openings and closings, for all process executions and terminations, and for the alteration or deletion of any memory or file object.					
								2.1.5.2	The system shall be configured to execute only intended and necessary processes during the execution of election software. The system shall also be configured to halt election software processes upon the termination of any critical system process (such as system audit) during the execution of election software.					
	2.6.2 Electronic Records	x		x		1) Recommend using appropriate NIST standard, and/or VVSG section 2.1.5, in place of "secure and usable manner". 2) Recommend removing "Typically", and rephrasing to something like, "this includes, but is not limited to:" 3) Enumerate bullets such that they are referenceable. 4) Remove "Shall" as it causes need for actionable event	In order to support independent auditing, a voting system SHALL be able to produce electronic records that contain the necessary information in a secure and usable manner. Typically, this includes records such as:			26, May, 2011 @ 1215 Documentation: Pass Functional: Pass	7, June, 2011 @ 1838 Documentation: Pass Functional: Pass		1	
		x		x			. Vote counts;			26, May, 2011 @ 1230 Documentation: Pass Functional: Pass	7, June, 2011 @ 1839 Documentation: Pass Functional: Pass	1		
		x		x			. Counts of ballots recorded;			26, May, 2011 @ 1440 Documentation: Pass Functional: Pass	7, June, 2011 @ 1841 Documentation: Pass Functional: Pass	1		

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
		x		x			. Paper record identifier;			27, May, 2011 @ 0915 Documentation: Pass Functional: Pass	7, June, 2011 @ 1842 Documentation: Pass Functional: Pass	1		
		x		x		Recommend more explicity defining "important events"	. Event logs and other records of important events; and			31, May, 2011 @ 0842 Documentation: Pass Functional: Pass	7, June, 2011 @ 1842 Documentation: Pass Functional: Pass		1	
		x		x			. Election archive information.			31, May, 2011 @ 0842 Documentation: Pass Functional: Pass	7, June, 2011 @ 1842 Documentation: Pass Functional: Pass	1		
		x				Enumerate in relation to above subsection	The following requirements apply to records produced by the voting system for any exchange of information between devices, support of auditing procedures, or reporting of final results:							
		x		x		The pertinent requirements associated to this sub requirement should be explicitly called out. A vague reference will only create gaps in coverage.	a. Requirements for electronic records to be produced by tabulation devices; and			31, May, 2011 @ 0842 Documentation: Pass Functional: Pass	7, June, 2011 @ 1845 Documentation: Pass Functional: Pass		1	
		x		x		The pertinent requirements associated to this sub requirement should be explicitly called out. A vague reference will only create gaps in coverage.	b. Requirements for printed reports to support auditing steps.		vii. The system shall be capable of printing a copy of the audit record. A separate printer is not required for the audit record, and the record may be produced on the standard system printer if all the following conditions are met:	31, May, 2011 @ 0842 Documentation: Pass Functional: Pass	7, June, 2011 @ 1848 Documentation: Pass Functional: Pass		1	
								2.4.3	Producing Reports					
									All systems shall be able to create reports summarizing the vote data on multiple level					
	2.6.2.1 All records capable of being exported	x		x		Agree with Requirement	The voting system SHALL provide the capability to export its electronic records in an open format, such as XML, or include a utility to export log data into a publicly documented format.			31, May, 2011 @ 0920 Documentation: Pass Functional: Pass	7, June, 2011 @ 1838 Documentation: Pass Functional: Pass	1		
								4.1.4.3	DRE System Recording Requirements					
	2.6.2.2 Ballot images	x		x		Agree with Requirement	The voting system SHALL have the capability to generate ballot images in a human readable format.	4.1.4.3 v	Provide a capability to retrieve ballot images in a form readable by humans	31, May, 2011 @ 0951 Documentation: Pass Functional: Pass	7, June, 2011 @ 1839 Documentation: Pass Functional: Pass	1		
	2.6.2.3 Ballot image content	x		x		Does this requirement need a complementary requirement, similar to how 2.6.3.2 has 2.6.3.3 Privacy?	The voting system SHALL be capable of producing a ballot image that includes:			31, May, 2011 @ 1458 Documentation: Pass Functional: Pass	7, June, 2011 @ 1841 Documentation: Pass Functional: Pass	1		
		x		x			a. Election title and date of election;			31, May, 2011 @ 1458 Documentation: Pass Functional: Pass	7, June, 2011 @ 1841 Documentation: Pass Functional: Pass	1		
		x		x			b. Jurisdiction identifier;			31, May, 2011 @ 1458 Documentation: Pass Functional: Pass	7, June, 2011 @ 1841 Documentation: Pass Functional: Pass	1		
		x		x			c. Ballot style;			31, May, 2011 @ 1458 Documentation: Pass Functional: Pass	7, June, 2011 @ 1841 Documentation: Pass Functional: Pass	1		
		x		x			d. Paper record identifier; and			31, May, 2011 @ 1458 Documentation: Pass Functional: Pass	7, June, 2011 @ 1841 Documentation: Pass Functional: Pass	1		
		x		x			e. For each contest and ballot question:			31, May, 2011 @ 1458 Documentation: Pass Functional: Pass	7, June, 2011 @ 1841 Documentation: Pass Functional: Pass	1		
		x		x			i. The choice recorded, including write-ins; and			31, May, 2011 @ 1458 Documentation: Pass Functional: Pass	7, June, 2011 @ 1841 Documentation: Pass Functional: Pass	1		

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
		x		x			ii. Information about each write-in.			31, May, 2011 @ 1458 Documentation: Pass Functional: Pass	7, June, 2011 @ 1841 Documentation: Pass Functional: Pass	1		
	2.6.2.4 All records capable of being printed	x		x		Should be enumerated or split out	The tabulation device SHALL provide the ability to produce printed forms of its electronic records. The printed forms SHALL retain all required information as specified for each record type other than digital signatures.			31, May, 2011 @ 0930 Documentation: Pass Functional: Pass	7, June, 2011 @ 1842 Documentation: Pass Functional: Pass	1		
	2.6.2.5 Summary count record	x		x		Agree with Requirement	The voting system SHALL produce a summary count record including the following:					1		
		x		x			a. Time and date of summary record; and			1, June, 2011 @ 0851 Documentation: Pass Functional: Pass	7, June, 2011 @ 1845 Documentation: Pass Functional: Pass	1		
		x		x			b. The following, both in total and broken down by ballot style and voting location:			1, June, 2011 @ 0851 Documentation: Pass Functional: Pass	7, June, 2011 @ 1848 Documentation: Pass Functional: Pass	1		
		x		x			i. Number of received ballots			1, June, 2011 @ 0851 Documentation: Pass Functional: Pass	7, June, 2011 @ 1851 Documentation: Pass Functional: Pass	1		
		x		x			ii. Number of counted ballots			1, June, 2011 @ 0851 Documentation: Pass Functional: Pass	7, June, 2011 @ 1852 Documentation: Pass Functional: Pass	1		
		x		x			iii. Number of rejected electronic CVRs			1, June, 2011 @ 0851 Documentation: Pass Functional: Pass	7, June, 2011 @ 1853 Documentation: Pass Functional: Pass	1		
		x		x			iv. Number of write-in votes			1, June, 2011 @ 0851 Documentation: Pass Functional: Pass	7, June, 2011 @ 1856 Documentation: Pass Functional: Pass	1		
		x		x			v. Number of undervotes.			1, June, 2011 @ 0851 Documentation: Pass Functional: Pass	7, June, 2011 @ 1857 Documentation: Pass Functional: Pass	1		
	2.6.3 Paper Records	x	x	x	x	Need to remove "Shall" from header	The vote capture device is required to produce a paper record for each ballot cast. This record SHALL be available to the voter to review and verify, and SHALL be retained for later auditing or recounts, as specified by state law. Paper records provide an independent record of the voter's choices that can be used to verify the correctness of the electronic record created by the vote capture device.							
	2.6.3.1 Paper record creation	x		x		Agree with Requirement	Each vote capture device SHALL print a human readable paper record.			31, May, 2011 @ 1419 Not tested, paper record not available	7, June, 2011 @ 1858 Documentation: Pass Functional: Pass	1		
	2.6.3.2 Paper record contents		x			2.6.2.3 and 2.6.3.2 test for the same thing, but one if Test Method Inspection and the other is Functional. Should be consistent. Recommend making both Inspection.	Each paper record SHALL contain at least:							
			x		x		a. Election title and date of election;			31, May, 2011 @ 1423 Not tested, paper record not available	7, June, 2011 @ 1859 Documentation: Pass Functional: Pass	1		
			x		x		b. Voting location;			31, May, 2011 @ 1423 Documentation: Insufficient Robustness Functional: Insufficient Robustness Not tested, paper record not available	7, June, 2011 @ 1859 Documentation: Pass Functional: Pass	1		

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
			x		x		c. Jurisdiction identifier;			31, May, 2011 @ 1423 Documentation: Insufficient Robustness Functional: Insufficient Robustness Not tested, paper record not available	7, June, 2011 @ 1859 Documentation: Pass Functional: Pass	1		
			x		x		d. Ballot style;			31, May, 2011 @ 1423 Documentation: Insufficient Robustness Functional: Insufficient Robustness Not tested, paper record not available	7, June, 2011 @ 1859 Documentation: Pass Functional: Pass	1		
			x		x		e. Paper record identifier; and			31, May, 2011 @ 1423 Documentation: Insufficient Robustness Functional: Insufficient Robustness Not tested, paper record not available	7, June, 2011 @ 1859 Documentation: Pass Functional: Pass	1		
			x		x		f. For each contest and ballot question:			31, May, 2011 @ 1423 Documentation: Insufficient Robustness Functional: Insufficient Robustness Not tested, paper record not available	7, June, 2011 @ 1859 Documentation: Pass Functional: Pass	1		
			x		x		i. The recorded choice, including write-ins; and			31, May, 2011 @ 1423 Documentation: Insufficient Robustness Functional: Insufficient Robustness Not tested, paper record not available	7, June, 2011 @ 1859 Documentation: Pass Functional: Pass	1		
			x		x		ii. Information about each write-in.			31, May, 2011 @ 1423 Documentation: Insufficient Robustness	7, June, 2011 @ 1859 Documentation: Pass Functional: Pass	1		
	2.6.3.3 Privacy		x		x	Agree with Requirement	The vote capture device SHALL be capable of producing a paper record that does not contain any information that could link the record to the voter.			31, May, 2011 @ 1423 Documentation: Insufficient Robustness Functional: Insufficient Robustness Not tested, paper record not available	7, June, 2011 @ 1859 Documentation: Pass Functional: Pass	1		

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
	2.6.3.4 Multiple pages	x		x		Enumerate the activities	When a single paper record spans multiple pages, each page SHALL include the voting location, ballot style, date of election, and page number and total number of the pages (e.g., page 1 of 4).			31, May, 2011 @ 1423 Documentation: Insufficient Robustness Functional: Insufficient Robustness Not tested, paper record not available	7, June, 2011 @ 1901 No tested, ballot did not span pages.	1		
	2.6.3.5 Machine-readable part contains same information as human-readable part		x		x	Agree with Requirement	If a non-human-readable encoding is used on the paper record, it SHALL contain the entirety of the human-readable information on the record			31, May, 2011 @ 1423 Documentation: Insufficient Robustness Functional: Insufficient Robustness Not tested, paper record not available	7, June, 2011 @ 1903 Not tested, paper record not available	1		
	2.6.3.6 Format for paper record non-human-readable data		x		x	Agree with Requirement	Any non-human-readable information on the paper record SHALL be presented in a non-proprietary format.			31, May, 2011 @ 1423 Documentation: Insufficient Robustness Functional: Insufficient Robustness Not tested, paper record not available	7, June, 2011 @ 1904 Not tested, paper record not available	1		
	2.6.3.7 Linking the electronic CVR to the paper record		x				The paper record SHALL:							
			x		x		a. Contain the paper record identifier; and			1, June, 2011 @ 0931 Documentation: Insufficient Robustness Functional: Insufficient Robustness	7, June, 2011 @ 1905 Documentation: Pass Functional: Pass	1		
			x		x	Recommend replacing "Identify" with "Validates"	b. Identify whether the paper record represents the ballot that was cast.			1, June, 2011 @ 0931 Documentation: Insufficient Robustness Functional: Insufficient Robustness Not tested, paper record not available	7, June, 2011 @ 1905 Documentation: Pass Functional: Pass		1	
												39	5	
	2.7 Performance Monitoring													
	2.7.1 Voting system and Network Status	x		x										
	2.7.1.1 Network monitoring	x		x		More detail should be added as to what level of monitoring should be taking place. This could be as minimal as, "the light is green, the system is up".	The system server SHALL provide for system and network monitoring during the voting period.			2, June, 2011 @ 0915 Documentation: Insufficient Robustness Functional: Insufficient Robustness Explicit tools not provided, only os tools	8, June, 2011 @ 1247 Documentation: Insufficient Robustness Functional: Insufficient Robustness Explicit tools not provided, only os tools		1	
	2.7.1.2 Tool access	x		x		Agree with Requirement	The system and network monitoring functionality SHALL only be accessible to authorized personnel from restricted consoles.			2, June, 2011 @ 0915 Documentation: Pass Functional: Pass	8, June, 2011 @ 1259 Documentation: Pass	1		
	2.7.1.3 Tool privacy	x		x		Agree with Requirement	System and network monitoring functionality SHALL NOT have the capability to compromise voter privacy or election integrity.			2, June, 2011 @ 0915 Documentation: Pass Functional: Pass	8, June, 2011 @ 1320 Documentation: Pass Functional: Pass	1		
												2	1	
Section 3: Usability, Accessibility, and Privacy Requirements												190	49	4
		NA		NA			Not included as part of vendor/ VSTL testing in 5.1.1							

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
	3.2 General Usability	NA		NA			Not included as part of vendor/ VSTL testing in 5.1.1							
	3.2.1 Privacy						The voting process must preclude anyone else from determining the content of a voter's ballot without the voter's cooperation.	3.1.7	The voting process shall preclude anyone else from determining the content of a voter's ballot, without the voter's cooperation.					
	3.2.1.1 Privacy at the kiosk locations							3.1.7.1	Privacy at the Polls					
					x	Agree with Requirement	a. The vote capture device SHALL prevent others from determining the contents of a ballot.		When deployed according to the installation instructions provided by the vendor, the voting station shall prevent others from observing the contents of a voter's ballot.	16, May, 2011 @ 0755 VCD does not prevent others from determining the contents of a ballot.	2, June, 2011 @ 0730 Documentation: Pass Functional: Pass			
					x	Agree with Requirement	b. The vote capture device SHALL support ballot privacy during the voting session and ballot submission		a. The ballot and any input controls shall be visible only to the voter during the voting session and ballot submission.	16, May, 2011 @ 0755 No guidelines found within the manufacturer's documentation to ensure ballot privacy during the voting session and ballot submission.	2, June, 2011 @ 0730 Documentation: Pass Functional: Pass			
					x	Agree with Requirement	c. During the voting session, if an audio interface to the vote capture device is provided, it SHALL be audible only to the voter.		b. The audio interface shall be audible only to the voter.	16, May, 2011 @ 0755 The manufacturer's documentation provided no recommendation related to how to set up a kiosk to ensure voter privacy when the eLect Access voting style is in use.	2, June, 2011 @ 0730 Not Applicable			
					x	Agree with Requirement	d. The vote capture device SHALL issue all warnings in a way that preserves the privacy of the voter and the confidentiality of the ballot.		c. As mandated by HAVA 301 (a)(1)(C), the voting system shall notify the voter of an attempted overvote in a way that preserves the privacy of the voter and the confidentiality of the ballot.	16, May, 2011 @0755 The manufacturer's warnings are not issued in a way that preserves the privacy of the voter and the confidentiality of the ballot.	2, June, 2011 @ 0730 Documentation: Pass Functional: Pass			
					x	Agree with Requirement	e. The vote capture device SHALL not issue a receipt to the voter that would provide proof to another of how the voter voted.			16, May, 2011 @0755 Documentation: Pass Functional: Pass	2, June, 2011 @ 0730 Documentation: Pass Functional: Pass			
	3.2.1.2 No recording of alternative format usage							3.1.7.2	No Recording of Alternate Format Usage					
									Voter anonymity shall be maintained for alternative format ballot presentation					
					x	Agree with Requirement	a. No information SHALL be kept within an electronic cast voter record that identifies any alternative language feature(s) used by a voter.		a. No information shall be kept within an electronic cast vote record that identifies any alternative language feature(s) used by a voter.	16, May, 2011 @ 0755 Upon completing a ballot, the voter may save or print the ballot for later mailing, emailing, or faxing. The ballot is saved in the selected language.	2, June, 2011 @ 0730 Documentation: Pass Functional: Pass			
					x	Agree with Requirement	b. No information SHALL be kept within an electronic cast voter record that identifies any accessibility feature(s) used by a voter.		b. No information shall be kept within an electronic cast vote record that identifies any accessibility feature(s) used by a voter.	16, May, 2011 @ 0755 No documentation found specifically stating that the method by which the voter accesses the voting system is not preserved with the voter data.	2, June, 2011 @ 0730 Documentation: Pass Functional: Pass			

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
	3.2.2 Cognitive issues						The features specified in this section are intended to minimize cognitive difficulties for voters. They should always be able to operate the vote capture device and understand the effect of their actions.	3.1.4	The voting process shall be designed to minimize cognitive difficulties for the voter.					
					x	Agree with Requirement	a. The vote capture device SHALL provide instructions for all its valid operations.		b. The voting machine or related materials shall provide clear instructions and assistance to allow voters to successfully execute and cast their ballots independently.	16, May, 2011 @ 0755 Documentation: Pass Functional: Pass	2, June, 2011 @ 0730 Documentation: Pass Functional: Pass			
					x	Agree with Requirement	b. The vote capture device SHALL provide a means for the voter to get help directly from the system at any time during the voting session. Need to verify		i. Voting machines or related materials shall provide a means for the voter to get help at any time during the voting session.	16, May, 2011 @ 0830 Help option was not available for the two authentication screens. The Ballot screen had a help option, but errors occured when it is selected.	2, June, 2011 @ 0730 Documentation: Pass Functional: Pass			
									ii. The voting machine shall provide instructions for all its valid operations.					
					x	More explicit standards should be referenced to create a consistency as to norms and best practices.	c. Instructional material for the voter SHALL conform to norms and best practices for plain language.							
					x	Agree with Requirement	i. Warnings and alerts issued by the vote capture device SHALL be distinguishable from other information and should clearly state:		d. Warnings and alerts issued by the voting system should clearly state the nature of the problem and the set of responses available to the voter. The warning should clearly state whether the voter has performed or attempted an invalid operation or whether the voting equipment itself has malfunctioned in some way.	16, May, 2011 @ 0830 Documentation: Pass Functional: Pass	2, June, 2011 @ 0730 Documentation: Pass Functional: Pass			
					x	Agree with Requirement	The nature of the problem;							
					x	Agree with Requirement	Whether the voter has performed or attempted an invalid operation or whether the vote capture device itself has malfunctioned in some way; and							
					x	Agree with Requirement	The set of responses available to the voter.							
					x	Agree with Requirement	ii. When an instruction is based on a condition, the condition should be stated first, and then the action to be performed.			16, May, 2011 @ 0830 Documentation: Pass Functional: Pass	2, June, 2011 @ 0730 Documentation: Pass Functional: Pass			
					x	Agree with Requirement	iii. The vote capture device should use familiar, common words and avoid technical or specialized words that voters are not likely to understand.			16, May, 2011 @ 0830 Documentation: Pass Functional: Pass	2, June, 2011 @ 0730 Various instances where spaces are needed between words displayed on the screen. The vote capture device makes use of the word 'Disabled' rather than 'Not Selected' on the Selection button next to candidates who were not selected by the voter. While 'disabled' is used in computer sciences to imply 'non-available', its more common meaning is 'impaired, as in physical functioning'.			

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
					x	Agree with Requirement, Enumerate the activities	iv. Each distinct instruction should be separated spatially from other instructions for visual or tactile interfaces, and temporally for auditory interfaces.			16, May, 2011 @ 0830 Documentation: Pass Functional: Pass	2, June, 2011 @ 0730 The 'BallotStyle' selection screen two choice buttons ('Aceptar' and 'Cancelar') are placed too close together. Also, touching 'Cancelar' doesn't result in any action. The voting system does not offer an audio interface.			
					x	Agree with Requirement	v. The vote capture device should issue instructions on the correct way to perform actions, rather than telling voters what not to do.			16, May, 2011 @ 0830 Documentation: Pass Functional: Pass	2, June, 2011 @ 0730 Documentation: Pass Functional: Pass			
					x	Agree with Requirement	vi. The instructions should address the voter directly rather than use passive voice constructions.			16, May, 2011 @ 0830 Documentation: Pass Functional: Pass	2, June, 2011 @ 0730 In the 'Instructions to Kiosk Voters' screen, there is a statement: 'If you desire to change your vote, you must touch....'. 'Must touch' is more passive than 'Touch'. Also, 'If you desire to change your vote' could be said more effectively: 'To Change your vote...'			
					x	Agree with Requirement	vii. The vote capture device should avoid the use of gender-based pronouns.			16, May, 2011 @ 0830 Documentation: Pass Functional: Pass	2, June, 2011 @ 0730 The 'Counted As Cast Receipt' instructions, Step 4, contains the word 'him': 'Deliver all you foldedVoter Choice Records to the kiosk worker, and show him the visible part...'			
					x	Agree with Requirement, Enumerate the activities	d. Consistent with election law, the voting application SHALL support a process that does not introduce bias for or against any of the contest choices to be presented to the voter. In both visual and aural formats, the choices SHALL be presented in an equivalent manner.. Need to verify		a. Consistent with election law, the voting system should support a process that does not introduce any bias for or against any of the selections to be made by the voter. In both visual and aural formats, contest choices shall be presented in an equivalent manner.	16, May, 2011 @ 0850 Documentation: Pass Functional: Pass	2, June, 2011 @ 0730 Write-in candidates are the only candidates that appear with both first name and last name entirely in upper case.			
					x	Definition of clarity and comprehensibility is needed to make this less ambiguous	e. The voting system SHALL provide the capability to design a ballot with a high level of clarity and comprehensibility. Contained or referenced in test plans; however, the current specifications needs to be verified against this standard.		c. The voting system shall provide the capability to design a ballot for maximum clarity and comprehension.	16, May, 2011 @ 0850 Documentation: Pass Functional: Pass	2, June, 2011 @ 0730 Documentation: Pass Functional: Pass			
					x	Agree with Requirement	i The vote capture device should not visually present a single contest spread over two pages or two columns.		i. The voting equipment should not visually present a single contest spread over two pages or two columns.	16, May, 2011 @ 0850 Documentation: Pass Functional: Pass	2, June, 2011 @ 0730 Documentation: Pass Functional: Pass			
					x	Agree with Requirement	ii. The ballot SHALL clearly indicate the maximum number of candidates for which one can vote within a single contest.		ii. The ballot shall clearly indicate the maximum number of candidates for which one can vote within a single contest.	16, May, 2011 @ 0850 Documentation: Pass Functional: Pass	2, June, 2011 @ 0730 Documentation: Pass Functional: Pass			

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
					x	Agree with Requirement	iii. The relationship between the name of a candidate and the mechanism used to vote for that candidate SHALL be consistent throughout the ballot.		iii.There shall be a consistent relationship between the name of a candidate and the mechanism used to vote for that candidate.	16, May, 2011 @ 0850 Documentation: Pass Functional: Pass	2, June, 2011 @ 0730 Documentation: Pass Functional: Pass			
					x	Agree with Requirement	iv. The vote capture device should present instructions near to where they are needed.			16, May, 2011 @ 0850 Documentation: Pass Functional: Pass	2, June, 2011 @ 0730 Documentation: Pass Functional: Pass			
					x	Agree with Requirement	f. The use of color SHALL agree with common conventions: (a) green, blue or white is used for general information or as a normal status indicator; (b) amber or yellow is used to indicate warnings or a marginal status; (c) red is used to indicate error conditions or a problem requiring immediate attention.. Contained in		e. The use of color by the voting system should agree with common conventions: (a) green, blue or white is used for general information or as a normal status indicator; (b) amber or yellow is used to indicate warnings or a marginal status; (c) red is used to indicate error conditions or a problem requiring immediate attention.	16, May, 2011 @ 0850 Documentation: Pass Functional: Pass	2, June, 2011 @ 0730 Instructions are in red text			
					x	Agree with Requirement	g. When an icon is used to convey information, indicate an action, or prompt a response, it SHALL be accompanied by a corresponding linguistic label.. Need to verify			16, May, 2011 @ 0850 Selecting a candidate resulted in a green checkmark icon appearing in the selection box. No linguistic label was available to identify the checkmark.	2, June, 2011 @ 0730 The 'Ballot Style Selection' screen has a box containing a green questionmark. The purpose of the questionmark isn't clear.			
	3.2.3 Perceptual issues						Some of these requirements are designed to assist voters with poor reading vision. These are voters who might have some difficulty in reading normal text, but are not typically classified as having a visual disability.	3.1.5	The voting process shall be designed to minimize perceptual difficulties for the voter					
	a. The electronic display screen characteristics					Agree with Requirement, Enumerate the activities (not bullets)	a. The electronic display screen of the vote capture device SHALL have the following characteristics: Contained or referenced in test plans; however, the current specifications needs to be verified against this standard.							
					x	Agree with Requirement	Flicker frequency NOT between 2 Hz and 55 Hz.	3.1.5	a. No voting machine display screen shall flicker with a frequency between 2 Hz and 55 Hz. Aside from usability concerns, this requirement protects voters with epilepsy.	16, May, 2011 @ 0850 Not Applicable	2, June, 2011 @ 0730 SLI could not find details on the vote capture device related to display flicker frequency, display brightness, pixel pitch, display area size, antiglare screen surface, or ambient contrast.			
					x	Agree with Requirement	Minimum display brightness: 130 cd/m2							
					x	Agree with Requirement	Minimum display darkroom 7×7 checkerboard contrast: 150:1							
					x	Agree with Requirement	Minimum display pixel pitch: 85 pixels/inch (0.3 mm/pixel)							
					x	Agree with Requirement	Minimum display area 700 cm2							
					x	Agree with Requirement	Antiglare screen surface that shows no distinct virtual image of a light source							
					x	Agree with Requirement	Minimum uniform diffuse ambient contrast for 500 1× illuminance: 10:1							
	b. Automatically reset of adjustments to default settings after voter's session.			x		Agree with Requirement, Enumerate the activities	b. Any aspect of the vote capture device that is adjustable by either the voter or kiosk worker, including font size, color, contrast, audio volume, or rate of speech, SHALL automatically reset to a standard default value upon completion of that voter's session.	3.1.5	b. Any aspect of the voting machine that is adjustable by the voter or poll worker, including font size, color, contrast, and audio volume, shall automatically reset to a standard default value upon completion of that voter's session.	16, May, 2011 @ 0850 Not Applicable	2, June, 2011 @ 0730 Not Applicable			
	c. Voter reset of adjustments to default settings, while preserving current votes.			x			c. If any aspect of a vote capture device is adjustable by either the voter or kiosk worker, there SHALL be a mechanism to allow the voter to reset all such aspects to their default values while preserving the current votes.	3.1.5	c. If any aspect of a voting machine is adjustable by the voter or poll worker, there shall be a mechanism to reset all such aspects to their default values.	16, May, 2011 @ 0850 Not Applicable	2, June, 2011 @ 0730 Not Applicable			

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
	d. Text font characteristics				x	Agree with Requirement, Enumerate the activities (not bullets)	d. For all text the vote capture device SHALL provide a font with the following characteristics. Contained or referenced in test plans; however, the current specifications needs to be verified against this standard.			16, May, 2011 @ 0850 Not Applicable	2, June, 2011 @ 0730 The ballot for Presidential / Vice Presential candidates presented the candidate names in approximately 1/8 of an inch in both height and width, which translates to approximately 2 millimeters.			
					x	Agree with Requirement	Height of capital letters at least: 3.0 mm	3.1.5	d. All electronic voting machines shall provide a minimum font size of 3.0 mm (measured as the height of a capital letter) for all text.					
					x	Agree with Requirement	x-height of a least: 70% of cap height	2.3.3.1 a.	a. Provide text that is at least 3 millimeters high and provide the capability to adjust or magnify the text to an apparent size of 6.3 millimeters					
					x	Agree with Requirement	Stroke width at least: 0.35 mm.							
	e. Font Sizes					Agree with Requirement	e. The vote capture device electronic image display SHALL be capable of showing all information in at least two font sizes:	3.1.5	e. All voting machines using paper ballots should make provisions for voters with poor reading vision. Discussion: Possible solutions include: (a) providing paper ballots in at least two font sizes, 3.0-4.0mm and 6.3-9.0mm and (b) providing a magnifying device.					
								3.2.2.1	b. The accessible voting station with an electronic image display shall be capable of showing all information in at least two font sizes, (a) 3.0-4.0 mm and (b) 6.3-9.0 mm, under control of the voter.					
					x	Agree with Requirement	3.0-4.0 mm cap height, with a corresponding x-height at least 70% of the cap height and a minimum stroke width of 0.35 mm;			16, May, 2011 @ 0850 Not Applicable	2, June, 2011 @ 0730 The voter is not able to make font adjustments to the VCD image display.			
					x	Agree with Requirement, Enumerate the activities	6.3-9.0 mm cap height, with a corresponding x-height at least 70% of the cap height and a minimum stroke width of 0.7 mm; under control of the voter. The device SHALL allow the voter to adjust font size throughout the voting session while preserving the current votes.			16, May, 2011 @ 0850 Not Applicable	2, June, 2011 @ 0730 The voter is not able to make font adjustments to the VCD image display.			
	f. Sans Serif font				x	Agree with Requirement	f. Text should be presented in a sans serif font.		h. All text intended for the voter should be presented in a sans serif font.	16, May, 2011 @ 0915 Documentation: Pass Functional: Pass	2, June, 2011 @ 0730 In the Review Instruction screen, a serif font is used in all of the contest boxes. The printed 'Voter's Choice Record' 'Instructions' and 'Selected Options' sections are in a serif font.			
	g. paper verification records.					Agree with Requirement	g. Vote capture devices providing paper verification records SHALL provide features that assist in the reading of such records by voters with poor reading vision.			16, May, 2011 @ 0930 Not Applicable	2, June, 2011 @ 0730 The VCD did not support the printing of records in at least two font sizes nor was a magnifier provided or recommended.			
					x	Agree with Requirement, enumerate the activities	i. The vote capture device may achieve legibility of paper records by supporting the printing of those records in at least two font sizes, 3.0-4.0mm and 6.3-9.0mm.			16, May, 2011 @ 0930 Not Applicable	31, May, 2011 @ 1300 Not Applicable			

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
					x		ii. The vote capture device may achieve legibility of paper records by supporting magnification of those records. This magnification may be done by optical or electronic devices. The manufacturer may either: 1) provide the magnifier itself as part of the system, or 2) provide the make and model number of readily available magnifiers that are compatible with the system.			16, May, 2011 @ 0930 Not Applicable	31, May, 2011 @ 1300 Not Applicable			
	h. Figure to ground Contrast ratio				x	Agree with Requirement	h. The minimum figure-to-ground ambient contrast ratio for all text and informational graphics (including icons) SHALL be 10:1		i. The minimum figure-to-ground ambient contrast ratio for all text and informational graphics (including icons) intended for the voter shall be 3:1.	16, May, 2011 @ 0930 Not Applicable	2, June, 2011 @ 0730 No documentation found on ambient contrast ratios. The VCD did not appear to have any anti-glare coating.			
	i. showing all information in high contrast.				x	Agree with Requirement	i. The electronic display screen of the vote capture device SHALL be capable of showing all information in high contrast either by default or under the control of the voter.Need to verify			16, May, 2011 @ 0930 Not Applicable	2, June, 2011 @ 0730 The voter is not able to alter contrast.			
	j. Default color coding				x	Agree with Requirement	j. The default color coding SHALL support correct perception by voters with color blindness. Need to verify		f. The default color coding shall maximize correct perception by voters with color blindness. Discussion: There are many types of color blindness and no color coding can, by itself, guarantee correct perception for everyone. However, designers should take into account such factors as: red-green color blindness is the most common form; high luminosity contrast will help colorblind voters to recognize visual features; and color-coded graphics can also use shape to improve the ability to distinguish certain features.					
					x	Agree with Requirement	i. Ordinary information presented to the voter should be in the form of black text on a white background. The use of color should be reserved for special cases, such as warnings or alerts.			16, May, 2011 @ 0930 Documentation: Pass Functional: Pass	2, June, 2011 @ 0730 Documentation: Pass Functional: Pass			
					x	Agree with Requirement	ii. No information presented to the voter SHALL be in the form of colored text on a colored background. Either the text or background SHALL be black or white.			16, May, 2011 @ 0930 The voter was presented with information in the form of colored text on a colored background (red lettering on a pink background) when returning to the site after previously being authenticated but not completing the ballot	2, June, 2011 @ 0730 Found: Red text, white text on a bright blue background, light green box containing a dark green questionmark, bold blue text on a yellow background, bold red text, black text on light blue background, black text on a grey background, Yellow is used as a background, bold black on a light blue background.			
						Agree with Requirement	iii. If text is colored other than black or white:							
					x	Agree with Requirement	1. The background SHALL be black or white.			16, May, 2011 @ 1220 The text displayed with red lettering on a pink background	2, June, 2011 @ 0730 The Voter Instruction screen has bold blue text on a yellow background stating 'Use buttons UP and DOWN to see all text.'			

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
					x	Agree with Requirement	2. The text SHALL be presented in a bold font (minimum 0.6 mm stroke width).			16, May, 2011 @ 1220 The colored text was not presented in a bold font	2, June, 2011 @ 0730 The colored text was not presented in a bold font			
					x	Agree with Requirement	3. If the background is black, the text color SHALL be yellow or light cyan.			16, May, 2011 @ 1220 Not Applicable	2, June, 2011 @ 0730 Documentation: Pass Functional: Pass			
					x	Agree with Requirement	4. If the background is white, the text color SHALL be dark enough to maintain a 10:1 contrast ratio.			16, May, 2011 @ 1220 Not Applicable	2, June, 2011 @ 0730 Not Testable			
						Agree with Requirement	iv. If the background is colored other than black or white, the presentation SHALL follow these guidelines:							
					x	Agree with Requirement	1. The text color SHALL be black.			16, May, 2011 @ 1240 Authentication failures were presented in white lettering on a red background.	2, June, 2011 @ 0730 Found: White text on a bright blue background, bold blue text on a yellow background			
					x	Agree with Requirement	2. The background color SHALL be yellow or light cyan.			16, May, 2011 @ 1240 Authentication failures were presented in white lettering on a red background.	2, June, 2011 @ 0730 Found: White text on a bright blue background, black text on a light grey background, black text on bright red background.			
	k. Color coding SHALL not be used as the sole means of conveying information				x	Agree with Requirement	k. Color coding SHALL not be used as the sole means of conveying information, indicating an action, prompting a response, or distinguishing a visual element. Need to verify		g. Color coding shall not be used as the sole means of conveying information, indicating an action, prompting a response, or distinguishing a visual element	16, May, 2011 @ 1240 Documentation: Pass Functional: Pass	2, June, 2011 @ 0730 Within the Review Instructions screen, the use of red background is the method for distinguishing contests in which the voter either undervoted or didn't vote at all.			
	3.2.4 Interaction issues					Do not put actionable activities in header, need to create sub-requirement to put these into	The requirements of this section are designed to minimize interaction difficulties for the voter.		The voting process shall be designed to minimize interaction difficulties for the voter.					
					x	Agree with Requirement	a. The vote capture device SHALL not require page scrolling by the voter.		a. Voting machines with electronic image displays shall not require page scrolling by the voter.	16, May, 2011 @ 1240 The entire ballot is on one screen and accessible only via using the scroll bar.	2, June, 2011 @ 0730 Documentation: Pass Functional: Pass			
					x	Agree with Requirement	b. The vote capture device SHALL provide unambiguous feedback regarding the voter's selection, such as displaying a checkmark beside the selected option or conspicuously changing its appearance.		b. The voting machine shall provide unambiguous feedback regarding the voter's selection, such as displaying a checkmark beside the selected option or conspicuously changing its appearance.	16, May, 2011 @ 1240 Documentation: Pass Functional: Pass	2, June, 2011 @ 0730 Documentation: Pass Functional: Pass			
					x	Agree with Requirement	c. Vote capture device input mechanisms SHALL be designed to prevent accidental activation.		d. Input mechanisms shall be designed to minimize accidental activation.	16, May, 2011 @ 1240 Documentation: Pass Functional: Pass	2, June, 2011 @ 0730 This requirement is dependent upon all sub-requirements passing.			

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
					x	Agree with Requirement, enumerate activities	i. On touch screens, the sensitive touch areas SHALL have a minimum height of 0.5 inches and minimum width of 0.7 inches. The vertical distance between the centers of adjacent areas SHALL be at least 0.6 inches, and the horizontal distance at least 0.8 inches. Touch areas SHALL not overlap.		i. On touch screens, the sensitive touch areas shall have a minimum height of 0.5 inches and minimum width of 0.7 inches. The vertical distance between the centers of adjacent areas shall be at least 0.6 inches, and the horizontal distance at least 0.8 inches.	16, May, 2011 @ 1300 Not Applicable	2, June, 2011 @ 0730 The distance between the SELECT button on one row and the SELECT button on a subsequent row was only 1/4".			
									ii. No key or control on a voting machine shall have a repetitive effect as a result of being held in its active position. Discussion: This is to preclude accidental activation. For instance, if a voter is typing in the name of a write-in candidate, depressing and holding the "e" key results in only a single "e" added to the name.					
	3.2.4.1 Timing issues						These requirements address how long the system and voter wait for each other to interact.							
					x	Agree with Requirement	a. The initial system response time of the vote capture device SHALL be no greater than 0.5 seconds.			16, May, 2011 @ 1300 Documentation: Pass Functional: Pass	2, June, 2011 @ 0730 Documentation: Pass Functional: Pass			
					x	Agree with Requirement, enumerate the activities	b. When the voter performs an action to record a single vote, the completed system response time of the vote capture device SHALL be no greater than one second in the case of a visual response, and no greater than five seconds in the case of an audio response			16, May, 2011 @ 1300 Documentation: Pass Functional: Pass	2, June, 2011 @ 0730 Documentation: Pass Functional: Pass			
					x	Agree with Requirement	c. The completed system response time of the vote capture device SHALL be no greater than 10 seconds.			16, May, 2011 @ 1300 Documentation: Pass Functional: Pass	2, June, 2011 @ 0730 Documentation: Pass Functional: Pass			
					x	Agree with Requirement	d. If the vote capture device has not completed its visual response within one second, it SHALL present to the voter, within 0.5 seconds of the voter's action, some indication that it is preparing its response			16, May, 2011 @ 1300 Not Testable	2, June, 2011 @ 0730 Not Testable			
					x	Agree with Requirement, enumerate the activities	e. If the vote capture device requires a response by a voter within a specific period of time, it SHALL issue an alert at least 20 seconds before this time period has expired and provide a means by which the voter may receive additional time		c. If the voting machine requires a response by a voter within a specific period of time, it shall issue an alert at least 20 seconds before this time period has expired and provide a means by which the voter may receive additional time.	16, May, 2011 @ 1300 Documentation: Pass Functional: Pass	2, June, 2011 @ 0730 No warning message was issued.			
	3.2.5 Alternative languages					Do not put actionable activities in header, need to create sub-requirement to put these into	a. The voting system SHALL be capable of presenting the ballot, contest choices, review screens, paper verification records, and voting instructions in any language declared by the manufacturer to be supported by the system.	3.1.5	The voting equipment shall be capable of presenting the ballot, ballot selections, review screens and instructions in any language required by state or federal law.	16, May, 2011 @ 1300 Not Testable	2, June, 2011 @ 0730 Not Testable			
						Agree with Requirement, enumerate the activities								
	3.2.6 Usability for kiosk workers					Do not put actionable activities in header, need to create sub-requirement to put these into. Agree with Requirement, enumerate the activities				16, May, 2011 @ 1300 Not Applicable				
	3.2.6.1 Operation					"Reasonably easy" needs to be better defined. The ambiguity created by this phrase can be too easily manipulated.				16, May, 2011 @ 1300 Not Applicable	2, June, 2011 @ 0800 The instructions failed to advise the kiosk worker to insert a card into the SmartCard reader.			
	3.2.6.2 Safety					"Presented at a level appropriate for kiosk workers who are not experts ...", needs to be better defined. The ambiguity created by this phrase can be too easily manipulated.				16, May, 2011 @ 1300 Not Applicable	2, June, 2011 @ 0800 There was no documentation related to the design of the voting system as to eliminate hazards.			

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
	3.3 Accessibility requirements	NA		NA		Note that last sentence of this header refers reader to section 3.1.3. There is not any such section.	Not included as part of vendor/ VSTL testing in 5.1.1	3.2	The voting process shall be accessible to voters with disabilities. As a minimum, every polling place shall have at least one voting station equipped for individuals with disabilities, as provided in HAVA 301 (a)(3)(B). A machine so equipped is referred to herein as an accessible voting station.					
	3.3.1 General						Contained or referenced in test plans; however, the current specifications needs to be verified against this standard.	3.2.1	General.					
									The voting process shall incorporate the following features that are applicable to all types of disabilities:					
						Agree with Requirement	a. The Acc-VS SHALL be integrated into the manufacturer's complete voting system so as to support accessibility for disabled voters throughout the voting session.							
					x	Agree with Requirement	i. The manufacturer SHALL supply documentation describing 1) recommended procedures that fully implement accessibility for voters with disabilities and 2) how the Acc-VS supports those procedures.			16, May, 2011 @ 1345 The manufacturer's documentation does not address kiosk sites and accessibility to the voting system for voters in wheel chairs, or voters with mobility or dexterity impairment.	31, May, 2011 @ 1300 The manufacturer's documentation does not detail any particular support for disabled voters. There is no provisioning for blind voters or those with impaired motor skills.			
					x	Agree with Requirement, enumerate the activities	b. When the provision of accessibility for Acc-VS involves an alternative format for ballot presentation, then all information presented to non-disabled voters, including instructions, warnings, error and other messages, and contest choices, SHALL be presented in that alternative format.		a. When the provision of accessibility involves an alternative format for ballot presentation, then all information presented to voters including instructions, warnings, error and other messages, and ballot choices shall be presented in that alternative format.	16, May, 2011 @ 1345 No documentation found of a single voting system that supports both audio and visual interfaces.	31, May, 2011 @ 1300 The manufacturer does not provide for an alternative format for ballot presentation.			
					x	Agree with Requirement, enumerate the activities	c. The support provided to voters with disabilities SHALL be intrinsic to the accessible voting station. It SHALL not be necessary for the accessible voting station to be connected to any personal assistive device of the voter in order for the voter to operate it correctly.		b. The support provided to voters with disabilities shall be intrinsic to the accessible voting station. It shall not be necessary for the accessible voting station to be connected to any personal assistive device of the voter in order for the voter to operate it correctly.	16, May, 2011 @ 1345 Not Applicable	31, May, 2011 @ 1300 Documentation: Pass Functional: Pass			
					x	Agree with Requirement	d. If a voting system provides for voter identification or authentication by using biometric measures that require a voter to possess particular biological characteristics, then Acc-VS SHALL provide a secondary means that does not depend on those characteristics.		c. When the primary means of voter identification or authentication uses biometric measures that require a voter to possess particular biological characteristics, the voting process shall provide a secondary means that does not depend on those characteristics	16, May, 2011 @ 1345 Not Applicable	31, May, 2011 @ 1300 Not Applicable			
					x	Agree with Requirement, remove self referencing aspect of text.	e. If the Acc-VS generates a paper record (or some other durable, human-readable record) for the purpose of allowing voters to verify their votes, then the system SHALL provide a means to ensure that the verification record is accessible to all voters with disabilities, as identified in 3.3 "Accessibility requirements".			16, May, 2011 @ 1345 Not Applicable	31, May, 2011 @ 1300 The voting system generates a Voter's Choice Record which prints on the printer attached to the Voting Laptop. No other means of providing this information is documented.			
					x	Agree with Requirement	i. If the Acc-VS generates a paper record (or some other durable, human-readable record) for the purpose of allowing voters to verify their votes, then the system SHALL provide a mechanism that can read that record and generate an audio representation of its contents.			16, May, 2011 @ 1345 Not Applicable	31, May, 2011 @ 1300 The voting system does generate a paper record (Voter's Choice Record), however, there is no provisioning of a mechanism that can read that record and generate an audio representation of its contents.			

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
	3.3.2 Low vision					Agree with Requirement. Reference to section 3.2.5 is incorrect, should be 3.2.3 for Perceptual Issues	Contained or referenced in test plans; however, the current specifications needs to be verified against this standard.	3.2.2	Vision					
							These requirements specify the features of the accessible voting station designed to assist voters with low vision.		The voting process shall be accessible to voters with visual disabilities.					
								3.2.2.1	Partial Vision					
									The accessible voting station shall be accessible to voters with partial vision.					
									a. The vendor shall conduct summative usability tests on the voting system using partially sighted individuals. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification.					
								3.2.2.1	b. The accessible voting station with an electronic image display shall be capable of showing all information in at least two font sizes, (a) 3.0-4.0 mm and (b) 6.3-9.0 mm, under control of the voter.					
									c. An accessible voting station with a monochrome-only electronic image display shall be capable of showing all information in high contrast either by default or under the control of the voter or poll worker. High contrast is a figure-to-ground ambient contrast ratio for text and informational graphics of at least 6:1.					
					x	Agree with Requirement, enumerate the activities	a. An accessible voting station with a color electronic image display SHALL allow the voter to adjust the color saturation throughout the voting session while preserving the current votes. Two options SHALL be available: 1) black text on white background and 2) white text on black background.		d. An accessible voting station with a color electronic image display shall allow the voter to adjust the color or the figure-to-ground ambient contrast ratio.	16, May, 2011 @ 1430 The voter is not provided with the option to select black text on white background vs. white text on black background.	2, June, 2011 @ 0730 The voter can not adjust the color saturation on the touchscreen monitor.			
					x	Agree with Requirement	b. Buttons and controls on accessible voting stations SHALL be distinguishable by both shape and color. This applies to buttons and controls implemented either "on-screen" or in hardware. This requirement does not apply to sizeable groups of keys, such as a conventional 4x3 telephone keypad or a full alphabetic keyboard.		e. Buttons and controls on accessible voting stations shall be distinguishable by both shape and color.	16, May, 2011 @ 1430 Documentation: Pass Functional: Pass	2, June, 2011 @ 0730 Documentation: Pass Functional: Pass			
					x	Agree with Requirement, enumerate the activities	c. The Acc-VS SHALL provide synchronized audio output to convey the same information as that which is displayed on the screen. There SHALL be a means by which the voter can disable either the audio or the video output, resulting in a video-only or audio-only presentation, respectively. The system SHALL allow the voter to switch among the three modes (synchronized audio/video, video-only, or audio-only) throughout the voting session while preserving the current votes.		f. An accessible voting station using an electronic image display shall provide synchronized audio output to convey the same information as that which is displayed on the screen.	16, May, 2011 @ 1430 The voting station does not provide synchronized audio output to convey the same information as that which is on the screen.	2, June, 2011 @ 0730 The VCD does not provide audio output.			
	3.3.3. Blindness						These requirements specify the features of the accessible voting station designed to assist voters who are blind.	3.2.2.2	Blindness. The accessible voting station shall be accessible to voters who are blind.					
									a. The vendor shall conduct summative usability tests on the voting system using who are blind. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification.					
					x	Agree with Requirement	a. The accessible voting station SHALL provide an audio-tactile interface (ATI) that supports the full functionality of the visual ballot interface.		b. The accessible voting station shall provide an audio-tactile interface (ATI) that supports the full functionality of the visual ballot interface, as specified in Subsection 2.3.3.	16, May, 2011 @ 1430 Not Testable	31, May, 2011 @ 1300 The manufacturer's documentation does not detail any audio-tactile interface to its voting system.			

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
					x	Agree with Requirement	i. The ATI of VEBD-A of the accessible voting station SHALL provide the same capabilities to vote and cast a ballot as are provided by its visual interface.		i. The ATI of the accessible voting station shall provide the same capabilities tovote and cast a ballot as are provided by other voting machines or by the visual interface of the standard voting machine.	16, May, 2011 @ 1430 Not Testable	31, May, 2011 @ 1300 The manufacturer does not support an audio interface to its voting system.			
					x	Agree with Requirement	ii. The ATI SHALL allow the voter to have any information provided by the voting system repeated.		ii. The ATI shall allow the voter to have any information provided by the voting system repeated.	16, May, 2011 @ 1430 Not Testable	31, May, 2011 @ 1300 Not Applicable			
					x	Agree with Requirement	iii. The ATI SHALL allow the voter to pause and resume the audio presentation.		iii. The ATI shall allow the voter to pause and resume the audio presentation	16, May, 2011 @ 1430 Not Testable	31, May, 2011 @ 1300 Not Applicable			
					x	Agree with Requirement	iv. The ATI SHALL allow the voter to skip to the next contest or return to previous contests.		iv. The ATI shall allow the voter to skip to the next contest or return to previous contests.	16, May, 2011 @ 1430 Not Testable	31, May, 2011 @ 1300 Not Applicable			
					x	Agree with Requirement	v. The ATI SHALL allow the voter to skip over the reading of a referendum so as to be able to vote on it immediately.		v. The ATI shall allow the voter to skip over the reading of a referendum so as to be able to vote on it immediately.	16, May, 2011 @ 1430 Not Testable	31, May, 2011 @ 1300 Not Applicable			
						Agree with Requirement	b. Voting stations that provide audio presentation of the ballot SHALL do so in a usable way, as detailed in the following sub-requirements.		c. All voting stations that provide audio presentation of the ballot shall conform to the following requirements:	16, May, 2011 @ 1430 Not Testable	31, May, 2011 @ 1300 Not Applicable			
					x	Agree with Requirement	i. The ATI SHALL provide its audio signal through an industry standard connector for private listening using a 3.5mm stereo headphone jack to allow voters to use their own audio assistive devices.		i. The ATI shall provide its audio signal through an industry standard connector for private listening using a 3.5mm stereo headphone jack to allow voters to use their own audio assistive devices.	16, May, 2011 @ 1430 The manufacturer's documentation on it's telephone voting system did not specify whether or not an industry standard connector for private listening would be recommended or provided.	31, May, 2011 @ 1300 Not Applicable			
					x	Agree with Requirement, enumerate the activities	ii. When VEBD-A utilizes a telephone style handset or headphone to provide audio information, it SHALL provide a wireless T-Coil coupling for assistive hearing devices so as to provide access to that information for voters with partial hearing. That coupling SHALL achieve at least a category T4 rating as defined by [ANSI01] American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19.		ii. When a voting machine utilizes a telephone style handset or headphone to provide audio information, it shall provide a wireless T-Coil coupling for assistive hearing devices so as to provide access to that information for voters with partial hearing. That coupling shall achieve at least a category T4 rating as defined by American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19.	16, May, 2011 @ 1430 The manufacturer's documentation does not provide details related to its telephone voting system such that SLI can determine if a wireless T-Coil coupling is recommended or provided for voters with partial hearing.	31, May, 2011 @ 1300 Not Applicable			
									iii. No voting equipment shall cause electromagnetic interference with assistive hearing devices that would substantially degrade the performance of those devices. The voting equipment, considered as a wireless device, shall achieve at least a category T4 rating as defined by American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19.					
					x	Agree with Requirement, though this is more procedural at the jurisdictional level.	iii. A sanitized headphone or handset SHALL be made available to each voter.		iv. A sanitized headphone or handset shall be made available to each voter.	17, May, 2011 @ 0720 There is no documentation related to headphones or handsets.	31, May, 2011 @ 1300 Not Applicable			
					x	Agree with Requirement	iv. VEBD-A SHALL set the initial volume for each voting session between 40 and 50 dB SPL.		v. The voting machine shall set the initial volume for each voter between 40 and 50 dB SPL.	17, May, 2011 @ 0720 There is no documentation related to audio volume.	31, May, 2011 @ 1300 Not Applicable			

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
					x	Agree with Requirement, enumerate the activities	v. The audio system SHALL allow the voter to control the volume throughout the voting session while preserving the current votes. The volume SHALL be adjustable from a minimum of 20dB SPL up to a maximum of 100 dB SPL, in increments no greater than 10 dB.		vi. The voting machine shall provide a volume control with an adjustable volume from a minimum of 20dB SPL up to a maximum of 100 dB SPL, in increments no greater than 10 dB.	17, May, 2011 @ 0720 The documentation provided by the manufacturer did not provide any details related to volume control.	31, May, 2011 @ 1300 Not Applicable			
					x	Agree with Requirement	vi. The audio system SHALL be able to reproduce frequencies over the audible speech range of 315 Hz to 10 KHz.		vii. The audio system shall be able to reproduce frequencies over the audible speech range of 315 Hz to 10 KHz.	17, May, 2011 @ 0720 The documentation provided by the manufacturer did not reveal any detail on audio frequencies.	31, May, 2011 @ 1300 Not Applicable			
					x	Agree with Requirement, enumerate the activities. Also "readily comprehensible" should be more definitively defined. In part, this requirement will be procedural at the jurisdictional level. Primarily the "included characteristics" portion of the requirement	vii. The audio presentation for VEBD-A of verbal information should be readily comprehensible by voters who have normal hearing and are proficient in the language. This includes such characteristics as proper enunciation, normal intonation, appropriate rate of speech, and low background noise. Candidate names should be pronounced as the candidate intends.		viii. The audio presentation of verbal information should be readily comprehensible by voters who have normal hearing and are proficient in the language. This includes such characteristics as proper enunciation, normal intonation, appropriate rate of speech, and low background noise. Candidate names should be pronounced as the candidate intends.	17, May, 2011 @ 0720 Not Testable	31, May, 2011 @ 1300 Not Applicable			
					x	Agree with Requirement, enumerate the activities	viii. The audio system SHALL allow the voter to control the rate of speech throughout the voting session while preserving the current votes. The range of speeds supported SHALL include 75% to 200% of the nominal rate. Adjusting the rate of speech SHALL not affect the pitch of the voice.		ix. The audio system shall allow voters to control the rate of speech. The range of speeds supported should be at least 75% to 200% of the nominal rate.	17, May, 2011 @ 0720 Not Testable	31, May, 2011 @ 1300 Not Applicable			
					x	Agree with Requirement	c. If Acc-VS supports ballot activation for non-blind voters, then it SHALL also provide features that enable voters who are blind to perform this activation.		d. If the normal procedure is to have voters initialize the activation of the ballot, the accessible voting station shall provide features that enable voters who are blind to perform this activation.	17, May, 2011 @ 0720 Documentation: Pass Functional: Pass	31, May, 2011 @ 1300 Not Applicable			
					x	Agree with Requirement	d. If Acc-VS supports ballot submission or vote verification for non-blind voters, then it SHALL also provide features that enable voters who are blind to perform these actions.		e. If the normal procedure is for voters to submit their own ballots, then the accessible voting station shall provide features that enable voters who are blind to perform this submission.	17, May, 2011 @ 0720 Documentation: Pass Functional: Pass	31, May, 2011 @ 1300 Not Applicable			
					x	Agree with Requirement, would be helpful to more definitively define "tactilely discernible"	e. Mechanically operated controls or keys, or any other hardware interface on Acc-VS available to the voter SHALL be tactilely discernible without activating those controls or keys.		f. All mechanically operated controls or keys on an accessible voting station shall be tactilely discernible without activating those controls or keys.	17, May, 2011 @ 0720 Documentation: Pass Functional: Pass	31, May, 2011 @ 1300 Not Applicable			
					x	Agree with Requirement, enumerate the activities	f. The status of all locking or toggle controls or keys (such as the "shift" key) for Acc-VS SHALL be visually discernible, and also discernible through either touch or sound.		g. On an accessible voting station, the status of all locking or toggle controls or keys (such as the "shift" key) shall be visually discernible, and discernible either through touch or sound.	17, May, 2011 @ 0720 The documentation provided by the manufacturer did not detail locking or toggle controls or keys.	31, May, 2011 @ 1300 Not Applicable			
	3.3.4 Dexterity						Contained or referenced in test plans; however, the current specifications needs to be verified against this standard.	3.2.3	Dexterity					
							These requirements specify the features of the accessible voting station designed to assist voters who lack fine motor control or use of their hands.		The voting process shall be accessible to voters who lack fine motor control or use of their hands.					
									a. The vendor shall conduct summative usability tests on the voting system using individuals lacking fine motor control. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification.					
									Discussion: Voting system developers are required to conduct realistic usability tests on the final product. For the present, vendors can define their own testing protocols. Future revisions to the Guidelines will include requirements for usability testing that will provide specific performance benchmarks.					

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
					x	Agree with Requirement, enumerate the activities	a. The accessible voting station SHALL provide a mechanism to enable non-manual input that is functionally equivalent to tactile input. All the functionality of the accessible voting station (e.g., straight party voting, write-in candidates) that is available through the conventional forms of input, such as tactile, SHALL also be available through the non-manual input mechanism.		d. The accessible voting station shall provide a mechanism to enable non-manual input that is functionally equivalent to tactile input. Discussion: This requirement ensures that the accessible voting station is operable by individuals who do not have the use of their hands. All the functionality of the accessible voting station (e.g., straight party voting, write-in candidates)that is available through the other forms of input, such as tactile, must also be available through a non-manual input mechanism if it is provided by the accessible voting station.	17, May, 2011 @ 0720 The internet voting system offers no alternate mechanism for input other that tactile. SLI could not determine if the telephone voting system allows for verbal input as opposed to tactile input.	31, May, 2011 @ 1300 The documentation provided by the manufacturer does not detail any auditory interface to the voting system.			
					x	Agree with Requirement	b. If Acc-VS supports ballot submission or vote verification for non-disabled voters, then it SHALL also provide features that enable voters who lack fine motor control or the use of their hands to perform these actions.		d. If the normal procedure is for voters to submit their own ballots, then the accessible voting station shall provide features that enable voters who lack fine motor control or the use of their hands to perform this submission.	17, May, 2011 @ 0720 The internet voting system offers no alternate mechanism for input other that tactile. SLI could not determine if the telephone voting system allows for verbal input as opposed to tactile input.	31, May, 2011 @ 1300 The manufacturer does not provide for any other interface to its voting system other than tactile.			
					x	Agree with Requirement, enumerate the activities	c. Keys, controls, and other manual operations on the accessible voting station SHALL be operable with one hand and SHALL not require tight grasping, pinching, or twisting of the wrist. The force required to activate controls and keys SHALL be no greater 5 lbs. (22.2 N).		b. All keys and controls on the accessible voting station shall be operable with one hand and shall not require tight grasping, pinching, or twisting of the wrist. The force required to activate controls and keys shall be no greater 5 lbs. (22.2 N).	17, May, 2011 @ 0720 The internet voting system offers no alternate mechanism for input other that tactile.	2, June, 2011 @ 0730 Documentation: Pass Functional: Pass			
					x	Agree with Requirement, enumerate the activities	d. The accessible voting station controls SHALL not require direct bodily contact or for the body to be part of any electrical circuit.		c. The accessible voting station controls shall not require direct bodily contact or for the body to be part of any electrical circuit.	17, May, 2011 @ 0720 The documentation provided by the manufacturer did not address VCDs which do not require bodily contact.	2, June, 2011 @ 0730 Voting is accomplished by touching the touchscreen monitor. Bodily contact is required.			
	3.3.5 Mobility					This section appears to be more oriented to FVAP implementation at the kiosk site, rather than the manufacturer's in a certification.	These requirements specify the features of the accessible voting station designed to assist voters who use mobility aids, including wheelchairs. Many of the requirements of this section are based on the ADA Accessibility Guidelines for Buildings and Facilities (ADAAG).	3.2.4	Mobility. The voting process shall be accessible to voters who use mobility aids, including wheelchairs.					
					x	Agree with Requirement	a. The accessible voting station SHALL provide a clear floor space of 30 inches minimum by 48 inches minimum for a stationary mobility aid. The clear floor space SHALL be designed for a forward approach or a parallel approach.		a. The accessible voting station shall provide a clear floor space of 30 inches (760 mm) minimum by 48 inches (1220 mm) minimum for a stationary mobility aid. The clear floor space shall be level with no slope exceeding 1:48 and positioned for a forward approach or a parallel approach.	17, May, 2011 @ 0930 The documentation provided by the manufacturer did not recommend clear floor space specifications	31, May, 2011 @ 1300 The manufacturer provides no specification for floor space as related to its voting station.			

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
					x	Agree with Requirement	b. When deployed according to the installation instructions provided by the manufacturer, Acc-VS SHALL allow adequate room for an assistant to the voter. This includes clearance for entry to and exit from the area of the voting station.			17, May, 2011 @ 0930 The documentation provided by the manufacturer does not address VCD accessibility.	31, May, 2011 @ 1300 Not Applicable			
					x	Agree with Requirement	c. Labels, displays, controls, keys, audio jacks, and any other part of the accessible voting station necessary for the voter to operate the voting system SHALL be legible and visible to a voter in a wheelchair with normal eyesight (no worse than 20/40, corrected) who is in an appropriate position and orientation with respect to the accessible voting station.		c. All labels, displays, controls, keys, audio jacks, and any other part of the accessible voting station necessary for the voter to operate the voting machine shall be easily legible and visible to a voter in a wheelchair with normal eyesight (no worse than 20/40, corrected) who is in an appropriate position and orientation with respect to the accessible voting station	17, May, 2011 @ 0930 The documentation provided by the manufacturer does not address VCD accessibility.	31, May, 2011 @ 1300 Not Applicable			
	3.3.5.1 Controls within reach				x		The requirements of this section ensure that the controls, keys, audio jacks and any other part of the accessible voting station necessary for its operation are within easy reach. Note that these requirements have meaningful application mainly to controls in a fixed location. A hand-held tethered control panel is another acceptable way of providing reachable controls.		b. All controls, keys, audio jacks and any other part of the accessible voting station necessary for the voter to operate the voting machine shall be within reach as specified under the following sub-requirements: Discussion: Note that these requirements have meaningful application mainly to controls in a fixed location. A hand-held tethered control panel is another acceptable way of providing reachable controls.					
					x	Agree with Requirement	a. If the accessible voting station has a forward approach with no forward reach obstruction then the high reach SHALL be 48 inches maximum and the low reach SHALL be 15 inches minimum. See Part 1: Figure 3-1.		i. If the accessible voting station has a forward approach with no forward reach obstruction then the high reach shall be 48 inches maximum and the low reach shall be 15 inches minimum. See Figure 1.	17, May, 2011 @ 1000 The documentation provided by the manufacturer does not address VCD accessibility.	31, May, 2011 @ 1300 Not Applicable			
					x	Agree with Requirement	b. If the accessible voting station has a forward approach with a forward reach obstruction, the following sub-requirements SHALL apply. (See Part 1: Figure 3-2).		ii. If the accessible voting station has a forward approach with a forward reach obstruction, the following requirements apply (See Figure 2):					
					x	Agree with Requirement	i. The forward obstruction for Acc-VS SHALL be no greater than 25 inches in depth, its top no higher than 34 inches and its bottom surface no lower than 27 inches.		The forward obstruction shall be no greater than 25 inches in depth, its top no higher than 34 inches and its bottom surface no lower than 27 inches.	17, May, 2011 @ 1000 The documentation provided by the manufacturer does not address VCD accessibility.	31, May, 2011 @ 1300 Not Applicable			
					x	Agree with Requirement	ii. If the obstruction for Acc-VS is no more than 20 inches in depth, then the maximum high reach SHALL be 48 inches, otherwise it SHALL be 44 inches.		If the obstruction is no more than 20 inches in depth, then the maximum high reach shall be 48 inches, otherwise it shall be 44 inches.	17, May, 2011 @ 1000 The documentation provided by the manufacturer does not address VCD accessibility.	31, May, 2011 @ 1300 Not Applicable			
					x	Agree with Requirement	iii. Space under the obstruction between the finish floor or ground and 9 inches above the finish floor or ground SHALL be considered toe clearance and SHALL comply with the following provisions for Acc-VS:		iii.Space under the obstruction between the finish floor or ground and 9 inches (230 mm) above the finish floor or ground shall be considered toe clearance and shall comply with the following provisions:	17, May, 2011 @ 1000 The documentation provided by the manufacturer does not address VCD accessibility.	31, May, 2011 @ 1300 Not Applicable			
					x	Agree with Requirement	1. Toe clearance depth SHALL extend 25 inches maximum under the obstruction;		Toe clearance shall extend 25 inches (635 mm) maximum under the obstruction	17, May, 2011 @ 1000 The documentation provided by the manufacturer does not address VCD accessibility.	31, May, 2011 @ 1300 Not Applicable			
					x	Agree with Requirement	2. The minimum toe clearance depth under the obstruction SHALL be either 17 inches or the depth required to reach over the obstruction to operate the accessible voting station, whichever is greater; and		The minimum toe clearance under the obstruction shall be either 17 inches (430 mm) or the depth required to reach over the obstruction to operate the accessible voting station, whichever is greater	17, May, 2011 @ 1000 The documentation provided by the manufacturer does not address VCD accessibility.	31, May, 2011 @ 1300 Not Applicable			

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
					x	Agree with Requirement	3. Toe clearance width SHALL be 30 inches minimum.		Toe clearance shall be 30 inches (760 mm) wide minimum	17, May, 2011 @ 1000 The documentation provided by the manufacturer does not address VCD accessibility.	31, May, 2011 @ 1300 Not Applicable			
					x	Agree with Requirement	iv. Space under the obstruction between 9 inches and 27 inches above the finish floor or ground SHALL be considered knee clearance and SHALL comply with the following provisions:		iv. Space under the obstruction between 9 inches (230 mm) and 27 inches (685 mm) above the finish floor or ground shall be considered knee clearance and shall comply with the following provisions:	17, May, 2011 @ 1000 The documentation provided by the manufacturer does not address VCD accessibility.	31, May, 2011 @ 1300 Not Applicable			
					x	Agree with Requirement	1. Knee clearance depth SHALL extend 25 inches maximum under the obstruction at 9 inches above the finish floor or ground;		Knee clearance shall extend 25 inches (635 mm) maximum under the obstruction at 9 inches (230 mm) above the finish floor or ground.	17, May, 2011 @ 1000 The documentation provided by the manufacturer does not address VCD accessibility.	31, May, 2011 @ 1300 Not Applicable			
					x	Agree with Requirement	2. The minimum knee clearance depth at 9 inches above the finish floor or ground SHALL be either 11 inches or 6 inches less than the toe clearance, whichever is greater;		The minimum knee clearance at 9 inches (230 mm) above the finish floor or ground shall be either 11 inches (280 mm) or 6 inches less than the toe clearance, whichever is greater.	17, May, 2011 @ 1000 The documentation provided by the manufacturer does not address VCD accessibility.	31, May, 2011 @ 1300 Not Applicable			
					x	Agree with Requirement	3. Between 9 inches and 27 inches above the finish floor or ground, the knee clearance depth SHALL be permitted to reduce at a rate of 1 inch in depth for each 6 inches in height. (It follows that the minimum knee clearance at 27 inches above the finish floor or ground SHALL be 3 inches less than the minimum knee clearance at 9 inches above the floor.); and		Between 9 inches (230 mm) and 27 inches (685 mm) above the finish floor or ground, the knee clearance shall be permitted to reduce at a rate of 1 inch (25 mm) in depth for each 6 inches (150 mm) in height. Discussion: It follows that the minimum knee clearance at 27 inches above the finish floor or ground shall be 3 inches less than the minimum knee clearance at 9 inches above the floor.	17, May, 2011 @ 1000 The documentation provided by the manufacturer does not address VCD accessibility.	31, May, 2011 @ 1300 Not Applicable			
					x	Agree with Requirement	4. Knee clearance width SHALL be 30 inches minimum.		Knee clearance shall be 30 inches (760 mm) wide minimum.	17, May, 2011 @ 1000 The documentation provided by the manufacturer does not address VCD accessibility.	31, May, 2011 @ 1300 Not Applicable			
					x	Agree with Requirement	c. If the accessible voting station has a parallel approach with no side reach obstruction then the maximum high reach SHALL be 48 inches and the minimum low reach SHALL be 15 inches. See Part 1: Figure 3-3.		v. If the accessible voting station has a parallel approach with no side reach obstruction then the maximum high reach shall be 48 inches and the minimum low reach shall be 15 inches. See Figure 3.	17, May, 2011 @ 1000 The documentation provided by the manufacturer does not address VCD accessibility.	31, May, 2011 @ 1300 Not Applicable			
					x	Agree with Requirement	d. If the accessible voting station has a parallel approach with a side reach obstruction, the following sub-requirements SHALL apply. See Figure 3-1.		vi. If the accessible voting station has a parallel approach with a side reach obstruction, the following sub-requirements apply. See Figure 4.	17, May, 2011 @ 1000 The documentation provided by the manufacturer does not address VCD accessibility.	31, May, 2011 @ 1300 Not Applicable			
					x	Agree with Requirement	i. The side obstruction for Acc-VS SHALL be no greater than 24 inches in depth and its top no higher than 34 inches.		The side obstruction shall be no greater than 24 inches in depth and its top no higher than 34 inches.	17, May, 2011 @ 1000 The documentation provided by the manufacturer does not address VCD accessibility.	31, May, 2011 @ 1300 Not Applicable			

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Can be met today?	Need Modification	Delete
					x	Agree with Requirement	ii. If the obstruction is no more than 10 inches in depth, then the maximum high reach SHALL be 48 inches, otherwise it SHALL be 46 inches.		If the obstruction is no more than 10 inches in depth, then the maximum high reach shall be 48 inches, otherwise it shall be 46 inches.	17, May, 2011 @ 1000 The documentation provided by the manufacturer does not address VCD accessibility.	31, May, 2011 @ 1300 Not Applicable			
	3.3.6 Hearing						These requirements specify the features of the accessible voting station designed to assist voters with hearing disabilities.	3.2.5	Hearing. The voting process shall be accessible to voters with hearing disabilities.					
					x	Is this meant to only include 3.3.3-c?	a. The accessible voting station SHALL incorporate the features listed under Requirement 3.3.3-C for voting systems that provide audio presentation of the ballot.		a. The accessible voting station shall incorporate the features listed under requirement 3.2.2.2 (c) for voting equipment that provides audio presentation of the ballot to provide accessibility to voters with hearing disabilities. Discussion: Note especially the requirements for volume initialization and control.	17, May, 2011 @ 1200 Documentation: Pass Functional: Pass	31, May, 2011 @ 1300 The voting system does not provide ballot activation for blind voters.			
					x	Agree with Requirement	b. If the accessible voting system provides sound cues as a method to alert the voter, the tone SHALL be accompanied by a visual cue, unless the station is in audio-only mode.		b. If voting equipment provides sound cues as a method to alert the voter, the tone shall be accompanied by a visual cue, unless the station is in audio-only mode.	17, May, 2011 @ 1200 Not Applicable	31, May, 2011 @ 1300 Not Applicable			
					x	Agree with Requirement	c. No voting device SHALL cause electromagnetic interference with assistive hearing devices that would substantially degrade the performance of those devices. The voting device, measured as if it were a wireless device, SHALL achieve at least a category T4 rating as defined by [ANSI01] American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19.	3.2.2.2.c	iii. No voting equipment shall cause electromagnetic interference with assistive hearing devices that would substantially degrade the performance of those devices. The voting equipment, considered as a wireless device, shall achieve at least a category T4 rating as defined by American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19.	17, May, 2011 @ 1200 The documentation provided by the manufacturer does not detail any design in place to prevent electromagnetic interference with assistive hearing devices.	31, May, 2011 @ 1300 Not Applicable			
	3.3.7 Cognition						These requirements specify the features of the accessible voting station designed to assist voters with cognitive disabilities.	3.2.8	Cognition, The voting process should be accessible to voters with cognitive disabilities.					
					x	More detail is needed for this requirement. Is this supposed to be a "should" instead of a "shall"?	a. The accessible voting station should provide support to voters with cognitive disabilities.		Discussion: At present there are no design features specifically aimed at helping those with cognitive disabilities. Requirements 3.2.2.1 (f), the synchronization of audio with the screen in a DRE, is helpful for some cognitive disabilities such as dyslexia. Requirements in Subsection 3.1.4 also address cognitive issues relative to voting system usability.	17, May, 2011 @ 1200 Not Testable	31, May, 2011 @ 1300 Not Testable			
								3.2.6	Speech. The voting process shall be accessible to voters with speech disabilities.					
									a. No voting equipment shall require voter speech for its operation.					
									Discussion: This does not preclude voting equipment from offering speech input as an option, but speech must not be the only means of input.					
	3.3.8 English proficiency						These requirements specify the features of the accessible voting station designed to assist voters who lack proficiency in reading English.	3.2.7	English proficiency					
					x	Agree with Requirement	a. For voters who lack proficiency in reading English, Acc-VS SHALL provide an audio interface for instructions and ballots as described in 3.3.3 b.		For voters who lack proficiency in reading English, or whose primary language is unwritten, the voting equipment shall provide spoken instructions and ballots in the preferred language of the voter, consistent with state and federal law. The requirements of 3.2.2.2 (c) shall apply to this mode of interaction.	17, May, 2011 @ 1200 No single voting system comes with both audio and visual support.	31, May, 2011 @ 1300 The voting system does not provide for an audio interface in any language.			

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Manufacturer 3	Manufacturer 4	Manufacturer 5	Manufacturer 6	Manufacturer 7	Can be met today?	Need Modification	Delete
Section 5: Security																			
	5.1 Access Control	x	x	x		Manufacturer shall clearly define what level users, roles and groups are defined on, whether that be at the operating system or the voting system level	This section states requirements for the identification of authorized system users, processes and devices and the authentication or verification of those identities as a prerequisite to granting access to system processes and data. It also includes requirements to limit and control access to critical system components to protect system and data integrity, availability, confidentiality, and accountability. This section applies to all entities attempting to physically enter voting system facilities or to request services or data from the voting system	2.1.1 a	To ensure security, all systems shall: Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			
				x				2.1.1. f	Incorporate a means of implementing a capability if access to a system function is to be restricted or controlled										
			x		x		Contained (or referenced) in test plans, and in the System Security Specification in the Technical Data Package. (see section 8.5 of UOCAVA guideline)												
	5.1.1 Separation of Duties	x		x			Contained (or referenced) in test plans	2.1.1 g	Provide documentation of mandatory administrative procedures for effective system security	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			
	5.1.1.1 Definition of roles	x		x		Agree with Requirement	The voting system SHALL allow the definition of personnel roles with segregated duties and responsibilities on critical processes to prevent a single person from compromising the integrity of the system.			16, May, 2011 @ 0930 Documentation: Insufficient Robustness Functional: Pass	25, May, 2011 @ 1400 Documentation: Pass Functional: Pass	16, May, 2011 @ 0930 Documentation: Insufficient Robustness Functional: Pass	12, May, 2011 @ 1036 Documentation: Pass Functional: NT - Kiosk worker & Administrator Pass: Election Official, Electioin Judge & Voter	9, May, 2011 @ 1420 Documentation: Insufficient Robustness Functional: NT	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: NT - Lack of access.	20, May, 2011 @ 1300 Documentation: Insufficient Robustness Functional: Pass - Election Official NA - Election Judge NT - Administrator, Kiosk worker, Voter	1		
	5.1.1.2 Access to election data	x		x		Agree with Requirement	The voting system SHALL ensure that only authorized roles, groups, or individuals have access to election data.			16, May, 2011 @ 0930 Documentation: Pass Functional: Pass	25, May, 2011 @ 1400 Documentation: Pass Functional: Pass	16, May, 2011 @ 0930 Documentation: Pass Functional: Pass	12, May, 2011 @ 1123 Documentation: Pass Functional: Pass: - Voter, Election Official, Election Judge NT - Administrator & Kiosk worker	9, May, 2011 @ 1420 Documentation: Insufficient Robustness Functional: Pass	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: NT - Election Official NA - Election Judge Pass - Voter	20, May, 2011 @ 1300 Documentation: Insufficient Robustness Functional: NT - election official, NA - Election Judge Pass - Voter NT - Administrator	1		
	5.1.1.3 Separation of duties	x		x		Enumerate the activities	The voting system SHALL require at least two persons from a predefined group for validating the election configuration information, accessing the cast vote records, and starting the tabulation process.			16, May, 2011 @ 0930 Documentation: Insufficient Robustness Functional: Insufficient Robustness The Manufacturers Administrative software did not prevent a single Election Official from changing the election configuration. The Manufacturer Administrative console did require a predefined	25, May, 2011 @ 1400 Manufacturer's provided documentation did not specify that two persons from a predefined group are required for validating the election configuration information, accessing the cast vote records, and starting the tabulation process.	16, May, 2011 @ 0930 Documentation: Insufficient Robustness Functional: Insufficient Robustness The Manufacturers Administrative software did not prevent a single Election Official from changing the election configuration. The Manufacturer Administrative console did require a predefined number of election judges before	12, May, 2011 @ 1123 Documentation: Insufficient Robustness Functional: Two people were not required to start the tabulation process.	9, May, 2011 @ 1420 Documentation: Insufficient Robustness Functional: NT	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: NT - Lack of access.	20, May, 2011 @ 1300 Documentation: Insufficient Robustness Functional: NT - Election Official NA - Election Judge NA - Voter Not Testable Manufacturer supplied documentation did not	1		
	5.1.2 Voting System Access	x		x		SHALL should be removed, as it designates an actionable item. The header of a section is validated when all of its sub requirements are validated	The voting system SHALL provide access control mechanisms designed to permit authorized access and to prevent unauthorized access to the system.			Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			
	5.1.2.1 Identity verification	x		x		This requirement should be split out. It covers both authentication and authorization.	The voting system SHALL identify and authenticate each person to whom access is granted, and the specific functions and data to which each person holds authorized access.			16, May, 2011 @ 1030 Documentation: Pass Functional: Pass	25, May, 2011 @ 1400 Documentation: Pass Functional: Pass	16, May, 2011 @ 1030 Documentation: Pass Functional: Pass	12, May, 2011 @ 1123 Documentation: Insufficient Robustness Functional: Pass	9, May, 2011 @ 1420 Documentation: Insufficient Robustness Functional: Pass	5, May 2011 @ 1425 Documentation: Pass Functional: NT SLI was not provided with administrative credentials.	20, May, 2011 @ 1300 Documentation: Pass Functional: Pass	1		
	5.1.2.2 Access control configuration	x		x		Enumerate the activities	The voting system SHALL allow the administrator group or role to configure permissions and functionality for each identity, group or role to include account and group/role creation, modification, and deletion.			16, May, 2011 @ 1145 Documentation: Insufficient Robustness Functional: Pass	14, June, 2011 @ 1312 Documentation: Pass Functional: Pass	16, May, 2011 @ 1145 Documentation: Insufficient Robustness Functional: Pass	12, May, 2011 @ 1223 Documentation: Insufficient Robustness Functional: Pass	9, May, 2011 @ 1420 Documentation: Insufficient Robustness Functional: NT	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: NT due to lack of access.	20, May, 2011 @ 1300 Documentation: Pass Functional: Pass	1		

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Manufacturer 3	Manufacturer 4	Manufacturer 5	Manufacturer 6	Manufacturer 7	Can be met today?	Need Modification	Delete
	5.1.2.3 Default access control configuration	x		x		Agree with Requirement	The voting system's default access control permissions SHALL implement the least privileged role or group needed.			16, May, 2011 @ 0930 1230 Documentation: Pass Functional: Pass	25, May, 2011 @ 1600 Documentation: Pass Functional: Insufficient Robustness inappropriate role allowed access	16, May, 2011 @ 0930 1230 Documentation: Pass Functional: Pass	12, May, 2011 @ 1223 Documentation: Pass Functional: Pass	9, May, 2011 @ 1420 Documentation: Insufficient Robustness Functional: Pass	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: NT - Administrator & Voter NA - Election Judge	20, May, 2011 @ 1300 Documentation: Insufficient Robustness Functional: NA - Election Judge Pass - Voter	1		
	5.1.2.4 Escalation prevention	x		x		Agree with Requirement	The voting system SHALL prevent a lower-privilege process from modifying a higher-privilege process.			16, May, 2011 @ 0930 1300 Documentation: Pass Functional: Pass	25, May, 2011 @ 1600 Documentation: Pass Functional: Pass	16, May, 2011 @ 0930 1300 Documentation: Pass Functional: Pass	12, May, 2011 @ 1239 Documentation: Insufficient Robustness Functional: NT - See Req. 5.9	9, May, 2011 @ 1420 Documentation: Insufficient Robustness Functional: NT - See Req. 5.9	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: NT - See Req. 5.9	20, May, 2011 @ 1300 Documentation: Insufficient Robustness Functional: NT - See Req. 5.9	1		
	5.1.2.5 Operating system privileged account restriction	x		x		Should enumerate the activities	The voting system SHALL NOT require its execution as an operating system privileged account and SHALL NOT require the use of an operating system privileged account for its operation.			16, May, 2011 @ 1705 Documentation: Insufficient Robustness Functional: Pass	14, June, 2011 @ 1312 Documentation: Insufficient Robustness Functional: Pass	16, May, 2011 @ 1705 Documentation: Insufficient Robustness Functional: Pass	12, May, 2011 @ 1239 Documentation: Insufficient Robustness Functional: NT - due to lack of remote access.	9, May, 2011 @ 1420 Documentation: Insufficient Robustness Functional: Pass	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: NT: SLI did not have access to the Manufacturer voting server.	20, May, 2011 @ 1300 Documentation: Insufficient Robustness Functional: NT - no access to the central server.	1		
	5.1.2.6 Logging of account	x		x		This is tested in 5.6.3.3	The voting system SHALL log the identification of all personnel accessing or attempting to access the voting system to the system event log.			Documentation: Insufficient Robustness Functional: Insufficient Robustness Logoffs in the Administrative application were logged, but not logins.	25, May, 2011 @ 1700 Documentation: Insufficient Robustness Functional: Pass	Documentation: Insufficient Robustness Functional: Insufficient Robustness Logoffs in the Administrative application were logged, but not logins.	12, May, 2011 @ 1239 Documentation: Insufficient Robustness Functional: NT - due to lack of information.	9, May, 2011 @ 1420 Documentation: Insufficient Robustness Functional: Pass	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: NT: SLI did not have access to the Manufacturer voting server.	20, May, 2011 @ 1300 Documentation: Insufficient Robustness Functional: NT - Adminstrator Pass: Voter	1		
	5.1.2.7 Monitoring voting system access	x		x		Should enumerate the activities Concern for this requirement is if it is realistically feasible to monitor a globally distributed system, with potentially a very large set of users	The{(voting system)}SHALL provide tools ((or shall be provided)) for monitoring access to the system. These tools SHALL provide specific users real time display of persons accessing the system as well as reports from logs.			17, May, 2011 @ 0930 Documentation: Insufficient Robustness Functional: Pass No real time display or via log reports.	25, May, 2011 @ 1700 Documentation: Insufficient Robustness Functional: Pass	17, May, 2011 @ 0930 Documentation: Insufficient Robustness Functional: Pass No real time display or via log reports.	12, May, 2011 @ 1457 Documentation: Insufficient Robustness Functional: NT - due to lack of information.	9, May, 2011 @ 1420 Documentation: Insufficient Robustness Functional: NT	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: NT: SLI did not have access to the Manufacturer voting server.	20, May, 2011 @ 1300 Documentation: Insufficient Robustness Functional: Lack of information	0	1	
	5.1.2.8 Login failures	x		x		1) SHALL should be removed, as it designates an actionable item. The header of a section is validated when all of its sub requirements are validated. 2) Enumerate activities 3) This requirement is too specific, should use the term "voting system" so that all areas are covered	The vote capture devices at the kiosk locations and the central server SHALL have the capability to restrict access to the voting system after a preset number of login failures.			Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	13, May, 2011 @ 1230 Documentation: Insufficient Robustness Functional: NT - due to lack of information.	9, May, 2011 @ 1420 Documentation: Insufficient Robustness Functional: NT	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: NT: SLI did not have access to the Manufacturer voting server.	20, May, 2011 @ 1700 Documentation: Insufficient Robustness Functional: NT - due to lack of information			
		x		x		Agree with Requirement	a. The lockout threshold SHALL be configurable by appropriate administrators/operators.			17, May, 2011 @ 1030 Documentation: Pass Functional: Insufficient Robustness Manufacturer's provided documentation did not detail restricting access to the voting system after a preset number of login failures.	25, May, 2011 @ 1700 Documentation: Insufficient Robustness Functional: Pass	17, May, 2011 @ 1030 Documentation: Pass Functional: Insufficient Robustness Manufacturer's provided documentation did not detail restricting access to the voting system after a preset number of login failures.	13, May, 2011 @ 1230 Documentation: Insufficient Robustness Functional: NT - due to lack of information.	9, May, 2011 @ 1420 Documentation: Insufficient Robustness Functional: NT	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: NT: SLI did not have access to the Manufacturer voting server.	20, May, 2011 @ 1700 Documentation: Insufficient Robustness Functional: NT - due to lack of information	1		

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Manufacturer 3	Manufacturer 4	Manufacturer 5	Manufacturer 6	Manufacturer 7	Can be met today?	Need Modification	Delete
		x		x		Covered in 5.6.3.3	b. The voting system SHALL log the event.			17, May, 2011 @ 1030 Documentation: Insufficient Robustness Functional: Insufficient Robustness No Logging	25, May, 2011 @ 1700 Documentation: Insufficient Robustness Functional: Pass	17, May, 2011 @ 1030 Documentation: Insufficient Robustness Functional: Insufficient Robustness No Logging	13, May, 2011 @ 1230 Documentation: Insufficient Robustness Functional: NT - due to lack of information.	9, May, 2011 @ 1420 Documentation: Insufficient Robustness Functional: NT	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: NT: SLI did not have access to the Manufacturer voting server.	20, May, 2011 @ 1700 Documentation: Insufficient Robustness Functional: NT - due to lack of information	1		
		x		x		Agree with Requirement	c. The voting system SHALL immediately send a notification to appropriate administrators/operators of the event.			17, May, 2011 @ 1150 Documentation: Insufficient Robustness Functional: Insufficient Robustness No notification	25, May, 2011 @ 1700 Documentation: Insufficient Robustness Functional: Pass	17, May, 2011 @ 1150 Documentation: Insufficient Robustness Functional: Insufficient Robustness No notification	13, May, 2011 @ 1230 Documentation: Insufficient Robustness Functional: NT - due to lack of information.	9, May, 2011 @ 1420 Documentation: Insufficient Robustness Functional: NT	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: NT: SLI did not have access to the Manufacturer voting server..	20, May, 2011 @ 1700 Documentation: Insufficient Robustness Functional: NT - due to lack of information	1		
		x		x		Agree with Requirement	d. The voting system SHALL provide a mechanism for the appropriate administrators/operators to reactivate the account after appropriate confirmation.			17, May, 2011 @ 1150 Documentation: Insufficient Robustness Functional: Insufficient Robustness Not all instances passed	25, May, 2011 @ 1700 Documentation: Insufficient Robustness Functional: Pass	17, May, 2011 @ 1150 Documentation: Insufficient Robustness Functional: Insufficient Robustness Not all instances passed	13, May, 2011 @ 1230 Documentation: Insufficient Robustness Functional: NT - due to lack of information.	9, May, 2011 @ 1420 Documentation: Insufficient Robustness Functional: NT	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: NT: SLI did not have access to the Manufacturer voting server.	20, May, 2011 @ 1700 Documentation: Insufficient Robustness Functional: NT - due to lack of information	1		
	5.1.2.9 Account lockout logging	x		x		Covered in 5.6.3.3	The voting system SHALL log a notification when any account has been locked out.			18, May, 2011 @ 0930 Documentation: Insufficient Robustness Functional: Insufficient Robustness No notification	14, June, 2011 @ 1312 Documentation: Insufficient Robustness Functional: Pass	18, May, 2011 @ 0930 Documentation: Insufficient Robustness Functional: Insufficient Robustness No notification	13, May, 2011 @ 1430 Documentation: Insufficient Robustness Functional: NT - due to lack of information.	9, May, 2011 @ 1420 Documentation: Insufficient Robustness Functional: NT	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: NT: SLI did not have access to the Manufacturer voting server.	20, May, 2011 @ 1700 Documentation: Insufficient Robustness Functional: NT - due to lack of information	1		
	5.1.2.10 Session time-out	x		x		Enumerate activities	Authenticated sessions on critical processes SHALL have an inactivity time-out control that will require personnel re-authentication when reached. This time-out SHALL be implemented for administration and monitor consoles on all voting system devices.			18, May, 2011 @ 0930 Documentation: Insufficient Robustness Functional: Insufficient Robustness The Manufacturer voting system did not time-out a voter following fifteen minutes of inactivity. Similarly, the system did	25, May, 2011 @ 1700 Documentation: Insufficient Robustness Functional: Pass	18, May, 2011 @ 0930 Documentation: Insufficient Robustness Functional: Insufficient Robustness The Manufacturer voting system did not time-out a voter following fifteen minutes of inactivity. Similarly, the system did not	13, May, 2011 @ 1430 Documentation: Insufficient Robustness Functional: Authenticated sessions on critical processes were enacted voters after five minutes of inactivity. There was no time-out enacted when users of the	9, May, 2011 @ 1510 @ 540 Documentation: NT Functional: Fail	6, May, 2011 @ 1000 Documentation: Insufficient Robustness Functional: NT - Administrator, due to lack of access Pass: Voter	20, May, 2011 @ 1700 Documentation: Insufficient Robustness Functional: No timeout set.	1		
	5.1.2.11 Screen lock	x		x		Should mention need for re-authentication in order to re-access	Authenticated sessions on critical processes SHALL have a screen-lock functionality that can be manually invoked			18, May, 2011 @ 1100 Documentation: Insufficient Robustness Functional: Insufficient Robustness The Manufacturer system allowed a voter to place a screen-lock on the computer.	14, June, 2011 @ 1312 Documentation: Insufficient Robustness Functional: Pass	18, May, 2011 @ 1100 Documentation: Insufficient Robustness Functional: Insufficient Robustness The Manufacturer system allowed a voter to place a screen-lock on the computer.	13, May, 2011 @ 1430 Documentation: Pass Functional: Pass: voter, application user NT - Kiosk worker	9, May, 2011 @ 1540 Documentation: NT Functional: Pass	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: NT due to lack of access - Adminstrator & Kiosk Pass: Voter	20, May, 2011 @ 1700 Documentation: Insufficient Robustness Functional: Pass	1		
							Section totals										16	1	
	5.2 Identification and Authentication	x							First, authentication shall be configured on the local terminal (display screen and keyboard) and on all external connection devices ("network cards" and "ports"). This ensures that only authorized and identified users affect the system while election software is running.	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			
	5.2.1 Authentication	x		x						Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			
	5.2.1.1 Strength of authentication	x		x		This should be referring to appropriate NIST SP, NIST 800-63 Electronic Authentication Guideline Standards.	Authentication mechanisms supported by the voting system SHALL support authentication strength of at least 1/1,000,000.			9, May, 2011 @ 1205 Documentation: Insufficient Robustness Functional: Pass	15, June, 2011 @ 0900 Documentation: Pass Functional: Pass	9, May, 2011 @ 1205 Documentation: Insufficient Robustness Functional: Pass	6, May, 2011 @ 1100 Documentation: Insufficient Robustness Functional: NT	12, May, 2011 @ 1100 Documentation: Insufficient Robustness Functional: NT	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: Pass	17, May, 2011 @ 1120 Documentation: Pass Functional: Pass	0	1	
	5.2.1.2 Minimum authentication methods	x		x			The voting system SHALL authenticate users per the minimum authentication methods outlined below. GROUP OR ROLE MINIMUM AUTHENTICATION STRENGTH			Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			
		x		x		Agree with Requirement	Election Judge Two factor			9, May, 2011 @ 1205 Documentation: Pass Functional: NT Not Testable: Election Judge credentials not provided	17, June, 2011 @ 0915 Documentation: Pass Functional: Pass	9, May, 2011 @ 1205 Documentation: Pass Functional: NT Not Testable: Election Judge credentials not provided	6, May, 2011 @ 1110 Documentation: Pass Functional: NT Not Testable: Election Judge credentials not provided	12, May, 2011 @ 1100 Documentation: Insufficient Robustness Functional: Insufficient Robustness	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: Insufficient Robustness	17, May, 2011 @ 1210 Documentation: Insufficient Robustness Functional: Insufficient Robustness Multifactor authentication not supported	1		

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Manufacturer 3	Manufacturer 4	Manufacturer 5	Manufacturer 6	Manufacturer 7	Can be met today?	Need Mod-ification	Delete
		x		x		Agree with Requirement	Kiosk Worker One factor			9, May, 2011 @ 1205 Documentation: Insufficient Robustness Functional: Insufficient Robustness Not Testable Role is not defined	17, June, 2011 @ 0915 Documentation: Pass Functional: Pass	9, May, 2011 @ 1205 Documentation: Insufficient Robustness Functional: Insufficient Robustness Not Testable Role is not defined	9, May, 2011 @ 1545 Documentation: Insufficient Robustness Functional: Insufficient Robustness Not Testable Role is not defined	12, May, 2011 @ 1100 Documentation: Insufficient Robustness Functional: Insufficient Robustness	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: Pass	17, May, 2011 @ 1400 Documentation: Insufficient Robustness Functional: NT - due to lack of information.	1		
		x		x		Assuming voter authentication is performed "outside" the scope of the voting system, by kiosk worker/Election Official	Voter Not required			9, May, 2011 @ 1245 Documentation: Insufficient Robustness Functional: Pass	17, June, 2011 @ 0915 Documentation: Insufficient Robustness Functional: Pass	9, May, 2011 @ 1245 Documentation: Insufficient Robustness Functional: Pass	6, May, 2011 @ 1110 Documentation: Insufficient Robustness Functional: Pass	12, May, 2011 @ 1100 19, May, 2011 @ 1600 Documentation: Insufficient Robustness Functional: Pass	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: Pass	17, May, 2011 @ 1400 18, May, 2011 @ 1200 Documentation: Pass Functional: Pass	1		
		x				Agree with Requirement	Election Official Two factor			9, May, 2011 @ 1405 Documentation: Pass Functional: Insufficient Robustness Not Testable: Election Official credentials not provided	17, June, 2011 @ 0915 Documentation: Pass Functional: Pass	9, May, 2011 @ 1405 Documentation: Pass Functional: Insufficient Robustness Not Testable: Election Official credentials not provided	6, May, 2011 @ 1110 Documentation: Pass Functional: Insufficient Robustness Not Testable: Election Official credentials not provided	12, May, 2011 @ 1200 Documentation: Insufficient Robustness Functional: Insufficient Robustness	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: Insufficient Robustness The Voting system doesn't have multi-factor authentication	17, May, 2011 @ 1210 Documentation: Insufficient Robustness Functional: Insufficient Robustness Multifactor authentication not supported	1		
		x		x		Agree with Requirement	Administrator Two factor			9, May, 2011 @ 14012 Documentation: Insufficient Robustness Functional: Pass	17, June, 2011 @ 0915 Documentation: Insufficient Robustness Functional: Pass	9, May, 2011 @ 14012 Documentation: Insufficient Robustness Functional: Pass	6, May, 2011 @ 1110 Documentation: Insufficient Robustness Functional: Pass	12, May, 2011 @ 1200 Documentation: Insufficient Robustness Functional: Insufficient Robustness	5, May 2011 @ 1425 5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: Insufficient Robustness The Voting system doesn't have multi-factor authentication	17, May, 2011 @ 1210 Documentation: Insufficient Robustness Functional: Insufficient Robustness Multifactor authentication not supported	1		
		x		x		Agree with Requirement	Application or Process Digital signature 112 bits of security1			9, May, 2011 @ 1245 Documentation: Insufficient Robustness Functional: Pass	17, June, 2011 @ 0915 Documentation: Insufficient Robustness Functional: Insufficient Robustness Use of 80 bit key in system under review	9, May, 2011 @ 1245 Documentation: Insufficient Robustness Functional: Pass	6, May, 2011 @ 1110 Documentation: Insufficient Robustness Functional: Insufficient Robustness	12, May, 2011 @ 1200 Documentation: Insufficient Robustness Functional: Insufficient Robustness	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional:Insufficient Robustness	17, May, 2011 @ 1400 Documentation: Pass Functional: Pass	1		
	5.2.1.3 Multiple authentication mechanisms	x		x		Agree with Requirement	The voting system SHALL provide multiple authentication methods to support multi-factor authentication.			9, May, 2011 @ 1245 Documentation: Insufficient Robustness Functional: Insufficient Robustness	20, June, 2011 @ 0900 Documentation: Pass Functional: Not Tested due to time constraints.	9, May, 2011 @ 1245 Documentation: Insufficient Robustness Functional: Insufficient Robustness	6, May, 2011 @ 1145 Documentation: Insufficient Robustness Functional: Insufficient Robustness The voting system does not provide authentication methods to support mult-factor authentication.	12, May, 2011 @ 1350 Documentation: Insufficient Robustness Functional: Insufficient Robustness Voting system did not provide the capability to support multi-factor authentication	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: Insufficient Robustness The Voting system doesn't have multi-factor authentication	17, May, 2011 @ 1210 Documentation: Insufficient Robustness Functional: Insufficient Robustness Multifactor authentication not supported	1		
	5.2.1.4 Secure storage of authentication data	x		x		Agree with Requirement	When private or secret authentication data is stored by the voting system, it SHALL be protected to ensure that the confidentiality and integrity of the data are not violated.			9, May, 2011 @ 1245 Documentation: Insufficient Robustness Functional: Insufficient Robustness	15, June, 2011 @ 0904 Documentation: Pass Functional: Pass Due to scope and time constraints only the backend/frontend were tested. The mixer would have the same results as it is running the same OS.	9, May, 2011 @ 1245 Documentation: Insufficient Robustness Functional: Insufficient Robustness	6, May, 2011 @ 1145 NT due to lack of information.NT due to lack of information.	12, May, 2011 @ 1200 Documentation: Insufficient Robustness Functional: NT due to lack of information.	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: NT - due to lack of information.	17, May, 2011 @ 1500 Documentation: Insufficient Robustness Functional: NT - due to lack of information.	1		
	5.2.1.5 Password reset	x		x		Covers passwords only. What if there are alternative methods of authentication?	The voting system SHALL provide a mechanism to reset a password if it is forgotten, in accordance with the system access/security policy.			9, May, 2011 @ 1245 Documentation: Insufficient Robustness Functional: Insufficient Robustness NT due to the lack of information on the authentication sysyem	15, June, 2011 @ 0908 Documentation: Insufficient Robustness Functional: Pass Due to scope and time constraints only the backend/frontend were tested. The mixer would have the same results as it is running the same OS.	9, May, 2011 @ 1245 Documentation: Insufficient Robustness Functional: Insufficient Robustness NT due to the lack of information on the authentication sysyem	6, May, 2011 @ 1300 11, May, 2011 @ 1630 19, May, 2011 @ 1300 Documentation: Insufficient Robustness Functional: Insufficient Robustness Unable to change	12, May, 2011 @ 1430 Documentation: Insufficient Robustness Functional: Pass	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: Insufficient Robustness NT - due to lack of information.	17, May, 2011 @ 1500 Documentation: Insufficient Robustness Functional: Pass	1		

GAP Analysis Matrix	Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Manufacturer 3	Manufacturer 4	Manufacturer 5	Manufacturer 6	Manufacturer 7	Can be met today?	Need Modification	Delete
5.2.1.6 Password strength configuration	x		x		Should specify the authentication level as defined in reference NIST SP	The voting system SHALL allow the administrator group or role to specify password strength for all accounts including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters per NIST 800-63 Electronic Authentication Guideline Standards.			9, May, 2011 @ 1430 Documentation: Insufficient Robustness Functional: Insufficient Robustness NT due to the lack of information on the procedure	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: Pass Due to scope and time constraints only the backend/frontend were tested. The mixer would have the same results as it is running the same OS.	9, May, 2011 @ 1430 Documentation: Insufficient Robustness Functional: Insufficient Robustness NT due to the lack of information on the procedure	6, May, 2011 @ 1340 10, May, 2011 @ 1600 19, May, 2011 @1045 24, May, 2011 @1115 Documentation: Pass Functional: Pass (confirmation message has incorrect spelling of a	12, May, 2011 @ 1545 Documentation: Insufficient Robustness Functional: Password length allowed = 1 character	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: Pass	17, May, 2011 @ 1500 Documentation: Insufficient Robustness Functional: Pass	1		
5.2.1.7 Password history configuration	x				Agree with Requirement	The voting system SHALL enforce password histories and allow the administrator to configure the history length when passwords are stored by the system. NIST Special Publication 800-57			9, May, 2011 @ 1430 10, May, 2011 @ 1700 Documentation: Insufficient Robustness Functional: Insufficient Robustness The system allows original password to be used too soon again as password therefore not allowing password history to be created successfully -	15, June, 2011 @ 0954 Documentation: Insufficient Robustness Functional: Pass Due to scope and time constraints only the backend/frontend were tested. The mixer would have the same results as it is running the same OS.	9, May, 2011 @ 1430 10, May, 2011 @ 1700 Documentation: Insufficient Robustness Functional: Insufficient Robustness The system allows original password to be used too soon again as password therefore not allowing password history to be created successfully -	6, May, 2011 @ 1300 24, May, 2011 @1200 Documentation: Insufficient Robustness Functional: The voting system allows original password to be re-used too soon	12, May, 2011 @ 1430 Documentation: Insufficient Robustness Functional: Old passwords not restricted.	Documentation: Insufficient Robustness Functional:Not Tested due to time constraints	17, May, 2011 @ 1615 Documentation: Pass Functional: User was allowed to enter a previous password.	1		
5.2.1.8 Account information password restriction	x				Agree with Requirement	The voting system SHALL ensure that the user name is not used in the password. Cannot be fully verified in lab; Testing at remote voting location(s) at operational level			9, May, 2011 @ 1430 10, May, 2011 @ 1400 Documentation: Insufficient Robustness Functional: Insufficient Robustness Enter username for password and it incorrectly saved -	15, June, 2011 @0956 Documentation: Insufficient Robustness Functional: Pass Due to scope and time constraints only the backend/frontend were tested. The mixer would have the same results as it is running the same OS.	9, May, 2011 @ 1430 10, May, 2011 @ 1400 Documentation: Insufficient Robustness Functional: Insufficient Robustness Enter username for password and it incorrectly saved -	6, May, 2011 @ 1300 10, May, 2011 @ 1400 Documentation: Insufficient Robustness Functional: password incorrectly saved.	12, May, 2011 @ 1430 Documentation: Insufficient Robustness Functional: Voting system allows for the username to be part of the password with no restrictions.	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: NT - due to lack of information.	17, May, 2011 @ 1615 Documentation: Pass Functional: Insufficient Robustness Account information used in password.	1		
5.2.1.9 Automated password expiration	x		x		Agree with Requirement	The voting system SHALL provide a means to automatically expire passwords.			9, May, 2011 @ 1430 10, May, 2011 @ 1515 Documentation: Insufficient Robustness Functional: Insufficient Robustness Currently Admin password does not expire in set period and is usable	15, June, 2011 @ 1019 Documentation: Insufficient Robustness Functional: Pass Due to scope and time constraints only the backend/frontend were tested. The mixer would have the same results as it is running the same OS.	9, May, 2011 @ 1430 10, May, 2011 @ 1515 Documentation: Insufficient Robustness Functional: Insufficient Robustness Currently Admin password does not expire in set period and is usable	6, May, 2011 @ 1300 10, May, 2011 @ 1730 Documentation: Insufficient Robustness Functional: Insufficient Robustness no procedure in place to set the automatic password expiration	12, May, 2011 @ 1650 Documentation: Insufficient Robustness Functional: NT due to lack of information.	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: NT - due to lack of information.	17, May, 2011 @ 1615 Documentation: Insufficient Robustness Functional: NT - due to lack of information.	1		
5.2.1.10 Device authentication	x		x		Tested in 5.3.1.2	The voting system servers and vote capture devices SHALL identify and authenticate one another using NIST - approved cryptographic authentication methods at the 112 bits of security.			9, May, 2011 @ 1445 Documentation: Insufficient Robustness Functional: Insufficient Robustness Not Testable - Lack of Specific Information See 5.3.1.3 form more Information.	15, June, 2011 @ 1029 Tested - Insufficient Robustness No certification for the Open VPN cryptographic module. See 5.3.1.3 for more Information.	9, May, 2011 @ 1445 Documentation: Insufficient Robustness Functional: Insufficient Robustness Not Testable - Lack of Specific Information See 5.3.1.3 form more Information.	6, May, 2011 @ 1445 Documentation: Insufficient Robustness Functional: NT - due to lack of procedure.	16, May, 2011 @ 1700 Documentation: Insufficient Robustness Functional: NT	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: NT - See Req. 5.3	18, May, 2011 @1050 Documentation: Pass Functional: Pass	1		
5.2.1.11 Network authentication	x		x		Tested in 5.3.1.2	Remote voting location site Virtual Private Network (VPN) connections (i.e., vote capture devices) to voting servers SHALL be authenticated using strong mutual cryptographic authentication at the 112 bits of security. Cannot be fully verified in lab; Testing at remote voting location(s) at operational level			9, May, 2011 @ 1445 Documentation: Not Applicable Functional: Not Applicable VPN is not utilized	15, June, 2011 @ 1029 Documentation: Insufficient Robustness Functional: Insufficient Robustness No certification for the Open VPN cryptographic module. See 5.3.1.3 for more Information.	9, May, 2011 @ 1445 Documentation: Not Applicable Functional: Not Applicable VPN is not utilized	6, May, 2011 @ 1445 Documentation: Not Applicable Functional: Not Applicable VPN is not utilized	16, May, 2011 @ 1700 Documentation: Not Applicable Functional: Not Applicable VPN is not utilized	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: Not Applicable VPN is not utilized	18, May, 2011 @1050 Documentation: Pass Functional:Not Applicable - no VPN	1		
5.2.1.12 Message authentication	x		x		1) need to define what is a "message" 2) Tested in 5.3.1.2	Message authentication SHALL be used for applications to protect the integrity of the message content using a schema with 112 bits of security.			9, May, 2011 @ 1445 Documentation: Insufficient Robustness Functional: Insufficient Robustness Not Testable - Lack of Specific Information See 5.3.1.3	15, June, 2011 @ 1029 Documentation: Insufficient Robustness Functional: Insufficient Robustness No certification for the Open VPN cryptographic module. See 5.3.1.3 for more Information.	9, May, 2011 @ 1445 Documentation: Insufficient Robustness Functional: Insufficient Robustness Not Testable - Lack of Specific Information See 5.3.1.3	6, May, 2011 @ 1445 Documentation: Insufficient Robustness Functional: NT - due to lack of information.	16, May, 2011 @ 1725 Documentation: Insufficient Robustness Functional: NT Not Testable - Lack of Information See 5.3.1.3 form more Information.	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: NT - due to lack of information.	17, May, 2011 @ 1615 Documentation: Insufficient Robustness Functional: NT - due to lack of information.	1		

GAP Analysis Matrix	Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Manufacturer 3	Manufacturer 4	Manufacturer 5	Manufacturer 6	Manufacturer 7	Can be met today?	Need Modification	Delete
5.2.1.13 Message authentication mechanisms	x		x		1) Is the intent here to use current certified communication methodologies? If so, would be better suited as an Inspection test method 2) Tested in 5.3.1.1 and 5.3.1.3 and 5.3.2.4	IPsec, SSL, or TLS and MAC mechanisms SHALL all be configured to be compliant with FIPS 140-2 using approved algorithm suites and protocols.			9, May, 2011 @ 1500 Documentation: Insufficient Robustness Functional: Insufficient Robustness Not Testable - Lack of Specific Information See 5.3.1.3 form more Information.	15, June, 2011 @ 1029 Documentation: Insufficient Robustness Functional: Insufficient Robustness No certification for the Open VPN cryptographic module. See 5.3.1.3 for more Information.	9, May, 2011 @ 1500 Documentation: Insufficient Robustness Functional: Insufficient Robustness Not Testable - Lack of Specific Information See 5.3.1.3 form more Information.	6, May, 2011 @ 1445 Documentation: Insufficient Robustness Functional: NT - due to lack of information.	16, May, 2011 @ 1725 Documentation: Insufficient Robustness Functional: NT Not Testable - Lack of Information See 5.3.1.3 form more Information.	5, May 2011 @ 1425 Documentation: Insufficient Robustness Functional: NT - due to lack of information.	18, May, 2011 @1050 Documentation: Pass Functional: Pass	1		
						Section totals										17	1	
5.3 Cryptography					1) SHALL should be removed, as it designates an actionable item. The header of a section is validated when all of its sub requirements are validated. 2) Note quantify "Strong Authentication", this term is too vague, should reference a standard				Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			
5.3.1 General Cryptography Requirements		x			This section needs additional requirements that handle the situation of keys purchase from a Certificate Authority				Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			
5.3.1.1 Cryptographic functionality		x		x	"… or use published and credible cryptographic algorithms/schemas/protocols" is something that should be qualified by FVAP/NIST. Perference is to not leave it to a VSTL to determine, or leave as a loophole for a manufacturer to argue.	All cryptographic functionality SHALL be implemented using NIST-approved cryptographic algorithms/schemas, or use published and credible cryptographic algorithms/schemas/protocols			14, June, 2011 @ 0900 Documentation: Insufficient Robustness Functional: Insufficient Robustness Fail for Bouncy Castle NT for OpenSSL due to lack of information	17, June, 2011 @ 0820 Documentation: Insufficient Robustness Functional: Insufficient Robustness	14, June, 2011 @ 0900 Documentation: Insufficient Robustness Functional: Insufficient Robustness Fail for Bouncy Castle NT for OpenSSL due to lack of information	13, June, 2011 @ 0815 Documentation: Insufficient Robustness Functional: NT Not Testable - Lack of Information See 5.3.1.3 form more Information.	15, June, 2011 @ 0815 Documentation: Insufficient Robustness Functional: NT Not Testable - Lack of Information See 5.3.1.3 form more Information.	16, June, 2011 @ 0920 Documentation: Insufficient Robustness Functional: NT - due to lack of information Without additional information about the environment and the cryptographic module used the requirements in section 5.3 cannot be adequately assessed to be compliant.	16,June, 2011 @ 0830 Documentation: Insufficient Robustness Functional: Pass		1	
5.3.1.2 Required security strength		x		x	Agree with Requirement	Cryptographic algorithms and schemas SHALL be implemented with a security strength equivalent to at least 112 bits of security to protect sensitive voting information and election records.			14, June, 2011 @ 0940 Documentation: Insufficient Robustness Functional: Insufficient Robustness Fail for Bouncy Castle NT for OpenSSL due to lack of information	17, June, 2011 @ 0900 Documentation: Insufficient Robustness Functional: Insufficient Robustness 80 bit key used	14, June, 2011 @ 0940 Documentation: Insufficient Robustness Functional: Insufficient Robustness Fail for Bouncy Castle NT for OpenSSL due to lack of information	13, June, 2011 @ 0940 Documentation: Insufficient Robustness Functional: Pass	15, June, 2011 @ 0830 Documentation: Insufficient Robustness Functional: NT Not Testable - Lack of Information See 5.3.1.3 form more Information.	16, June, 2011 @ 0920 Documentation: Insufficient Robustness Functional: NT - due to lack of information Without additional information about the environment and the cryptographic module used the requirements in section 5.3 cannot be adequately assessed to be compliant.	16,June, 2011 @ 0830 Documentation: Insufficient Robustness Functional: Pass	1		
5.3.1.3 Use NIST-approved cryptography for communications	x		x		These requirements should be split out to discrete items	Cryptography used to protect information in-transit over public telecommunication networks SHALL use NIST-approved algorithms and cipher suites. In addition the implementations of these algorithms SHALL be NIST-approved (Cryptographic Algorithm Validation Program).			14, June, 2011 @ 0900 Documentation: Insufficient Robustness Functional: Insufficient Robustness Fail for Bouncy Castle NT for OpenSSL due to lack of information	17, June, 2011 @ 0950 Documentation: Insufficient Robustness Functional: Insufficient Robustness NT Due to lack of access	14, June, 2011 @ 0900 Documentation: Insufficient Robustness Functional: Insufficient Robustness Fail for Bouncy Castle NT for OpenSSL due to lack of information	13, June, 2011 @ 1000 Documentation: Insufficient Robustness Functional: NT Not Testable - Lack of Information See 5.3.1.3 form more Information.	15, June, 2011 @ 0840 Documentation: Insufficient Robustness Functional: NT Not Testable - Lack of Information See 5.3.1.3 form more Information.	16, June, 2011 @ 0920 Documentation: Insufficient Robustness Functional: NT - due to lack of information Without additional information about the environment and the cryptographic module used the requirements in section 5.3 cannot be adequately assessed to be	16,June, 2011 @ 0850 Documentation: Insufficient Robustness Functional: Pass	1		
5.3.2 Key Management		x				The following requirements apply to voting systems that generate cryptographic keys internally.			Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			
5.3.2.1 Key generation methods		x		x	See comment on 5.3.1.1, as it is applicable here as well	Cryptographic keys generated by the voting system SHALL use a NIST-approved key generation method, or a published and credible key generation method.			14, June, 2011 @ 1000 Documentation: Insufficient Robustness Functional: Insufficient Robustness NT due to lack of information	17, June, 2011 @ 1000 Documentation: Insufficient Robustness Functional: Insufficient Robustness NT due to lack of information	14, June, 2011 @ 1000 Documentation: Insufficient Robustness Functional: Insufficient Robustness NT due to lack of information	13, June, 2011 @ 1020 Documentation: Insufficient Robustness Functional: Pass	15, June, 2011 @ 0905 Documentation: Insufficient Robustness Functional: NT Not Testable - Lack of Information See 5.3.1.3 form more Information.	16, June, 2011 @ 0920 Documentation: Insufficient Robustness Functional: NT - due to lack of information Without additional information about the environment and the cryptographic module used the requirements in section 5.3 cannot be adequately assessed to be	16,June, 2011 @ 0900 Documentation: Insufficient Robustness Functional: Pass		1	

GAP Analysis Matrix	Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Manufacturer 3	Manufacturer 4	Manufacturer 5	Manufacturer 6	Manufacturer 7	Can be met today?	Need Modification	Delete
5.3.2.2 Security of key generation methods		x		x	Agree with Requirement	Compromising the security of the key generation method (e.g., guessing the sapplication value to initialize the deterministic random number generator (RNG)) SHALL require as least as many operations as determining the value of the generated key.			14, June, 2011 @ 1330 Documentation: Insufficient Robustness Functional: Insufficient Robustness Nt due to lack of information	17, June, 2011 @ 1030 Documentation: Insufficient Robustness Functional: Insufficient Robustness NT due to lack of information	14, June, 2011 @ 1330 Documentation: Insufficient Robustness Functional: Insufficient Robustness Nt due to lack of information	13, June, 2011 @ 1105 Documentation: Insufficient Robustness Functional: Pass	15, June, 2011 @ 0950 Documentation: Insufficient Robustness Functional: NT Not Testable - Lack of Information See 5.3.1.3 form more Information.	16, June, 2011 @ 0920 Documentation: Insufficient Robustness Functional: NT - due to lack of information Without additional information about the environment and the cryptographic module used the requirements in section 5.3 cannot be adequately assessed to be	16,June, 2011 @ 0910 Documentation: Insufficient Robustness Functional: Pass	1		
5.3.2.3 Sapplication values		x		x	These requirements should be split out to discrete items	If a sapplication key is entered during the key generation process, entry of the key SHALL meet the key entry requirements in 5.3.3.1. If intermediate key generation values are output from the cryptographic module, the values SHALL be output either in encrypted form or under split knowledge procedures.			14, June, 2011 @ 1400 Documentation: Insufficient Robustness Functional: Insufficient Robustness NT due to lack of information	17, June, 2011 @ 1045 Documentation: Insufficient Robustness Functional: Insufficient Robustness NT due to lack of information	14, June, 2011 @ 1400 Documentation: Insufficient Robustness Functional: Insufficient Robustness NT due to lack of information	13, June, 2011 @ 1215 Documentation: Insufficient Robustness Functional: Pass	15, June, 2011 @ 1110 Documentation: Insufficient Robustness Functional: NT Not Testable - Lack of Information See 5.3.1.3 form more Information.	16, June, 2011 @ 0920 Documentation: Insufficient Robustness Functional: NT - due to lack of information Without additional information about the environment and the cryptographic module used the requirements in section 5.3 cannot be adequately assessed to be	16,June, 2011 @ 0930 Documentation: Insufficient Robustness Functional: Pass	1		
5.3.2.4 Use NIST-approved key generation methods for communications		x		x	1) These requirements should be split out to discrete items 2) Unless key is purchased from a Certificate Authority	Cryptographic keys used to protect information in-transit over public telecommunication networks SHALL use NIST-approved key generation methods. If the approved key generation method requires input from a random number generator, then an approved (FIPS 140-2) random number generator SHALL be used.			14, June, 2011 @ 1430 Documentation: Insufficient Robustness Functional: Insufficient Robustness NT due to lack of information	17, June, 2011 @ 1105 Documentation: Insufficient Robustness Functional: Insufficient Robustness NT due to lack of information	14, June, 2011 @ 1430 Documentation: Insufficient Robustness Functional: Insufficient Robustness NT due to lack of information	13, June, 2011 @ 1410 Documentation: Insufficient Robustness Functional: Pass	15, June, 2011 @ 1205 Documentation: Insufficient Robustness Functional: NT Not Testable - Lack of Information See 5.3.1.3 form more Information.	16, June, 2011 @ 0920 Documentation: Insufficient Robustness Functional: NT - due to lack of information Without additional information about the environment and the cryptographic module used the requirements in section 5.3 cannot be adequately assessed to be compliant.	16,June, 2011 @ 1020 Documentation: Pass Functional: Pass	1		
5.3.2.5 Random number generator health tests		x		x	Agree with Requirement	Random number generators used to generate cryptographic keys SHALL implement one or more health tests that provide assurance that the random number generator continues to operate as intended (e.g., the entropy source is not stuck).			14, June, 2011 @ 1500 Documentation: Insufficient Robustness Functional: Insufficient Robustness NT due to lack of information	17, June, 2011 @ 1430 Documentation: Insufficient Robustness Functional: Insufficient Robustness NT due to lack of information	14, June, 2011 @ 1500 Documentation: Insufficient Robustness Functional: Insufficient Robustness NT due to lack of information	13, June, 2011 @ 1435 Documentation: Insufficient Robustness Functional: Pass	15, June, 2011 @ 1415 Documentation: Insufficient Robustness Functional: NT Not Testable - Lack of Information See 5.3.1.3 form more Information.	16, June, 2011 @ 0920 Documentation: Insufficient Robustness Functional: NT - due to lack of information Without additional information about the environment and the cryptographic module used the requirements in section 5.3 cannot be adequately assessed to be	16,June, 2011 @ 1130 Documentation: Insufficient Robustness Functional: Pass	1		
5.3.3 Key Establishment		x			Agree with Requirement	Key establishment may be performed by automated methods (e.g., use of a public key algorithm), manual methods (use of a manually transported key loading device), or a combination of automated and manual			Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	1		
5.3.3.1 Key entry and output		x	x	x	Agree with Requirement	Secret and private keys established using automated methods SHALL be entered into and output from a voting system in encrypted form. Secret and private keys established using manual methods may be entered into or output from a system in plaintext form.			14, June, 2011 @ 1530 Documentation: Insufficient Robustness Functional: Insufficient Robustness NT due to lack of information	17, June, 2011 @ 1515 Documentation: Insufficient Robustness Functional: Insufficient Robustness NT due to lack of information	14, June, 2011 @ 1530 Documentation: Insufficient Robustness Functional: Insufficient Robustness NT due to lack of information	13, June, 2011 @ 1505 Documentation: Insufficient Robustness Functional: NT Not Testable - Lack of Information See 5.3.1.3 form more Information.	15, June, 2011 @ 1545 Documentation: Insufficient Robustness Functional: NT Not Testable - Lack of Information See 5.3.1.3 form more Information.	16, June, 2011 @ 0920 Documentation: Insufficient Robustness Functional: NT - due to lack of information Without additional information about the environment and the cryptographic module used the requirements in section 5.3 cannot be adequately assessed to be	16,June, 2011 @ 1420 Documentation: Insufficient Robustness Functional: NT	1		
5.3.4 Key handling		x	x						Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			
5.3.4.1 Key storage		x			These requirements should be split out to discrete items	Cryptographic keys stored within the voting system SHALL NOT be stored in plaintext. Keys stored outside the voting system SHALL be protected from disclosure or modification.			14, June, 2011 @ 1600 Documentation: Insufficient Robustness Functional: Insufficient Robustness NT due to lack of information	17, June, 2011 @ 1620 Documentation: Insufficient Robustness Functional: Insufficient Robustness NT due to lack of information	14, June, 2011 @ 1600 Documentation: Insufficient Robustness Functional: Insufficient Robustness NT due to lack of information	13, June, 2011 @ 1540 Documentation: Insufficient Robustness Functional: NT Not Testable - Lack of Information See 5.3.1.3 form more Information.	15, June, 2011 @ 1625 Documentation: Insufficient Robustness Functional: NT Not Testable - Lack of Information See 5.3.1.3 form more Information.	16, June, 2011 @ 0920 Documentation: Insufficient Robustness Functional: NT - due to lack of information Without additional information about the environment and the cryptographic module used the requirements in section 5.3 cannot be adequately assessed to be	16,June, 2011 @ 1510 Documentation: Insufficient Robustness Functional: NT - due to lack of access.	1		
5.3.4.2 Key zeroization	NA		x		Agree with Requirement	The voting system SHALL provide methods to zeroize all plaintext secret and private cryptographic keys within the system.			14, June, 2011 @ 1630 Documentation: Insufficient Robustness Functional: NT Due to lack of access	17, June, 2011 @ 1640 Documentation: Insufficient Robustness Functional: NT Due to lack of access	14, June, 2011 @ 1630 Documentation: Insufficient Robustness Functional: NT Due to lack of access	13, June, 2011 @ 1620 Documentation: Insufficient Robustness Functional: NT Not Testable - Lack of Information See 5.3.1.3 form more Information.	15, June, 2011 @ 1700 Documentation: Insufficient Robustness Functional: NT Not Testable - Lack of Information See 5.3.1.3 form more Information.	16, June, 2011 @ 0920 Documentation: Insufficient Robustness Functional: NT - due to lack of information Without additional information about the environment and the cryptographic module used the requirements in section 5.3 cannot be adequately assessed to be	16,June, 2011 @ 1725 Documentation: Insufficient Robustness Functional: NT - No procedure.	1		

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Manufacturer 3	Manufacturer 4	Manufacturer 5	Manufacturer 6	Manufacturer 7	Can be met today?	Need Modification	Delete
	5.3.4.3 Support for rekeying	x		x		What is the acceptable level of effort to reset the cryptographic keys to new values? Is it aceptable to have to redefine the election? Or should the jurisdiction be able to just replace the keys?	The voting system SHALL support the capability to reset cryptographic keys to new values.			14, June, 2011 @ 1700 Documentation: Insufficient Robustness Functional: NT Due to lack of access	17, June, 2011 @ 1700 Documentation: Insufficient Robustness Functional: NT Due to lack of access	14, June, 2011 @ 1700 Documentation: Insufficient Robustness Functional: NT Due to lack of access	13, June, 2011 @ 1730 Documentation: Insufficient Robustness Functional: NT	15, June, 2011 @ 1735 Documentation: Insufficient Robustness Functional: NT Not Testable - Lack of Information See 5.3.1.3 form more Information.	16, June, 2011 @ 0920 Documentation: Insufficient Robustness Functional: NT - due to lack of information Without additional information about the environment and the cryptographic module used the requirements in section 5.3 cannot be adequately assessed to be	16,June, 2011 @ 1750 Documentation: Insufficient Robustness Functional: NT - No procedure.		1	
							Section totals										10	3	
	5.4 Voting System Integrity Management	x				This section has difficulty when applied to "ballot delivery" systems. Would work better to have 5.4.1 be specific to vote capture devices, then have a section 5.4.2 that pertains to vote capture devices and ballot delivery systems	Under 5.4.2, items like ballot integrity, Personally Identifiable Information (PII)			Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met		1	
	5.4.1 Protecting the Integrity of the Voting System					May need an additional requirement for nonrepudiation issues				Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			
	5.4.1.1 Cast vote integrity; transmission	x		x		Agree with Requirement	The integrity and authenticity of each individual cast vote SHALL be protected from any tampering or modification during transmission.			5, May, 2011 @ 0945 Documentation: Insufficient Robustness Functional: Insufficient Robustness. There was no alert	20, June, 2011 @ 0905 Documentation: Pass Functional: NT Because of the VPN encryption we can't see if the system is encrypting data using SSL or TLS.	5, May, 2011 @ 0945 Documentation: Insufficient Robustness Functional: Insufficient Robustness. There was no alert	9, May, 2011 @ 1443 Documentation: Insufficient Robustness Functional: Insufficient Robustness. PII was not protected	13, May, 2011 @ 0748 Documentation: Insufficient Robustness Functional: Insufficient Robustness. Ballot delivery system	17, June, 2011 @ 1020 Documentation: Insufficient Robustness Functional: Insufficient Robustness. Ballot delivery system	6, May, 2011 @ 0903 Documentation: Insufficient Robustness Functional: Insufficient Robustness. Ballot delivery system	1		
	5.4.1.2 Cast vote integrity; storage	x		x		Agree with Requirement	The integrity and authenticity of each individual cast vote SHALL be preserved by means of a digital signature during storage.			5, May, 2011 @ 1130 Documentation: Pass Functional: NT Needed access to the database on the remote system.	20, June, 2011 @ 0940 Documentation: Pass Functional: Not Tested Not Tested due to time constraints.	5, May, 2011 @ 1130 Documentation: Pass Functional: NT Needed access to the database on the remote system.	10, May, 2011 @ 1122 Documentation: Insufficient Robustness Functional: NT - due to lack of remote access.	13, May, 2011 @ 0749 Documentation: Not Applicable, Functional: Not Applicatble Ballot delivery system	17, June, 2011 @ 1038 Documentation: Not Applicable, Functional: Not Applicatble	6, May, 2011 @ 1020 Documentation: Not Applicable, Functional: Not Applicatble Ballot delivery system	1		
	5.4.1.3 Cast vote storage	x		x		For the kiosk environment this works fine. If this is ever applied beyond section 1.1.3, to personal computers being used as the vote capture device, then there will be issues with regards to how the configuration is regulated	Cast vote data SHALL NOT be permanently stored on the vote capture device			5, May, 2011 @ 1140 Documentation: Insufficient Robustness Functional: Insufficient Robustness There were cookies remaining after the voting system was closed.	15, June, 2011 @ 1517 Documentation: Pass Functional: NA There is no hard drive on the vote capture device.	5, May, 2011 @ 1140 Documentation: Insufficient Robustness Functional: Insufficient Robustness There were cookies remaining after the voting system was closed.	10, May, 2011 @ 1126 Documentation: Insufficient Robustness Functional: There were cookies remaining after the voting system was closed.	13, May, 2011 @ 0750 Documentation: Not Applicable, Functional: Not Applicatble Ballot delivery system	17, June, 2011 @ 1054 Documentation: Insufficient Robustness Functional: Insufficient robustness Ballot data resides on VCD after a session completes.	6, May, 2011 @ 1026 Documentation: Not Applicable, Functional: Not Applicatble Ballot delivery system	1		
	5.4.1.4 Electronic ballot box integrity	x		x		Additional detailed definition of "electronic ballot box" is needed.	The integrity and authenticity of the electronic ballot box SHALL be protected by means of a digital signature.			5, May, 2011 @ 1214 Documentation: Pass Functional: NT Needed access to the database on the remote	20, June, 2011 @ 1010 Documentation: Pass Functional: NT due to time constraints.	5, May, 2011 @ 1214 Documentation: Pass Functional: NT Needed access to the database on the remote	10, May, 2011 @ 0815 Documentation: Pass Functional: Not Tested Needed access to the database on the remote	16, May, 2011 @ 0950 Documentation: Not Applicable, Functional: Not Applicatble	17, June, 2011 @ 1110 Documentation: Not Applicable, Functional: Not Applicatble Ballot Delivery System	6, May, 2011 @1536 Documentation: Not Applicable, Functional: Not Applicatble		1	
	5.4.1.5 Malware detection		x		x	More definition is needed to quantify the level of protection needed. Potentially a hardware/software malware detection solution, instead of just software.	The voting system SHALL use malware detection software to protect against known malware that targets the operating system, services, and applications			15, June, 2011 @ 0856 Documentation: Insufficient Robustness Functional: Insufficient Robustness Vendor stated they were not meeting this requirement	20, June, 2011 @ 1500 Documentation: Insufficient Robustness Functional: Insufficient Robustness There is no documentation or program listed on the Servers for Malware.	15, June, 2011 @ 0856 Documentation: Insufficient Robustness Functional: Insufficient Robustness Vendor stated they were not meeting this requirement	10, May, 2011 @ 1154 Documentation: Insufficient Robustness Functional: Not Tested Needed access to the database on the remote system.	16, May, 2011 @ 0952 Documentation: Insufficient Robustness Functional: There is no documentation or program listed on the Servers for Malware.	Documentation: Insufficient Robustness Functional: No Malware proctection	6, May, 2011 @1125 Documentation: Insufficient Robustness Functional: Not Tested - No access to remote server		1	
	5.4.1.6 Updating malware detection		x		x	A follow on requirement to this one would be to have the manufacturer specify in their documentation (i.e. an Inspection test method) the recommend interval for requiring updated signatures	The voting system SHALL provide a mechanism for updating malware detection signatures.			15, June, 2011 @ 0858 Documentation: Insufficient Robustness Functional: Insufficient Robustness Vendor stated they were not meeting this requirement	20, June, 2011 @ 1410 Documentation: Insufficient Robustness Functional: Insufficient Robustness There is no documentation or program listed on the Servers for Malware.	15, June, 2011 @ 0858 Documentation: Insufficient Robustness Functional: Insufficient Robustness Vendor stated they were not meeting this requirement	10, May, 2011 @ 1154 Documentation: Insufficient Robustness Functional: Not Tested Needed access to the database on the remote system.	16, May, 2011 @ 0952 Documentation: Insufficient Robustness Functional: There are no procedures documented or program listed on the Servers for Malware.	Documentation: Insufficient Robustness Functional: No documented procedure.	6, May, 2011 @ 1125 Documentation: Insufficient Robustness Functional: Not Tested No access to remote server	1		

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Manufacturer 3	Manufacturer 4	Manufacturer 5	Manufacturer 6	Manufacturer 7	Can be met today?	Need Modification	Delete
	5.4.1.7 Validating software on kiosk voting devices		x		x	This requirement needs to be expanded to cover all associated devices at the kiosk location. Some systems contain additional devices.	The voting system SHALL provide the capability for kiosk workers to validate the software used on the vote capture devices as part of the daily initiation of kiosk operations.			5, May, 2011 @ 1221 Documentation: Insufficient Robustness Functional: Insufficient Robustness No method documented or applicable	15, June, 2011 @ 1440 Documentation: Insufficient Robustness Functional: Insufficient Robustness The documentation was not updated for the new method of validating software on the kiosk	5, May, 2011 @ 1221 Documentation: Insufficient Robustness Functional: Insufficient Robustness No method documented or applicable	10, May, 2011 @ 1203 Documentation: Insufficient Robustness Functional: Insufficient Robustness	16, May, 2011 @ 0952 Documentation: Insufficient Robustness Functional: There are no procedures documented or program listed on the Servers for Malware.	Documentation: Insufficient Robustness Functional: No documented procedure.	6, May, 2011 @ 1309 Documentation: Insufficient Robustness Functional: Not Tested No access to remote server	1		
							Section totals										5	3	
	5.5 Communications Security	x				Some of the requirements in this section appear to explicitly call out specific communication protocols, which could be interpreted to exclude all other like communication protocols.	This section provides requirements for communications security. These requirements address ensuring the integrity of transmitted information and protecting the voting system from external communications-based threats.			Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			
	5.5.1 Data Transmission Integrity	x								Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			
	5.5.1.1 Data integrity protection	x		x		Recommend that this requirement be broken out to handle outbound versus inbound seperately	Voting systems that transmit data over communications links SHALL provide integrity protection for data in transit through the generation of integrity data (digital signatures and/or message authentication codes) for outbound traffic and verification of the integrity data for inbound traffic.			5, May, 2011 @ 1318 Documentation: Insufficient Robustness Functional: Insufficient Robustness Modified packet not detected	15, June, 2011 @ 0840 Documentation: Pass Functional: NT because of the VPN encryption	5, May, 2011 @ 1318 Documentation: Insufficient Robustness Functional: Insufficient Robustness Modified packet not detected	10, May, 2011 2011 @ 1223 Documentation: Insufficient Robustness Functional: Pass	16, May, 2011 @ 0953 Documentation: Insufficient Robustness Functional: Intercepted and changed information without notification from the voting system	16, June, 2011 @ 0815 Documentation: Insufficient Robustness Functional: NT due to lack of access	6, May, 2011 @ 1416 Documentation: Insufficient Robustness Functional: Pass	1		
	5.5.1.2 TLS/SSL	x		x		Agree with Requirement	Voting systems SHALL use at a minimum TLS 1.0, SSL 3.1 or equivalent protocols, including all updates to both protocols and implementations as of the date of the submission (e.g., RFC 5746 for TLS 1.0). verify all updates to both protocols and implementations as of the date of the submission (e.g., RFC 5746 for TLS 1.0).			5, May, 2011 @ 1351 Documentation: Insufficient Robustness Functional: Pass	15, June, 2011 @ 0842 Documentation: Pass Functional: NT because of the VPN encryption	5, May, 2011 @ 1351 Documentation: Insufficient Robustness Functional: Pass	10, May, 2011 @ 1240 Documentation: Pass Functional: Pass	16, May, 2011 @ 0945 Documentation: Insufficient Robustness Functional: Pass	16, June, 2011 @ 0815 Documentation: Insufficient Robustness Functional: NT due to lack of access	6, May, 2011 @ 1437 Documentation: Insufficient Robustness Functional: Pass	1		
	5.5.1.3 Virtual private networks (VPN)	x		x		Tested in 5.3.1.1 and 5.3.1.3. As this appears to be a specific instance of the above mentioned requirements, would recommend removal in order to reduce redundancy.	Voting systems deploying VPNs SHALL configure them to only allow FIPS-compliant cryptographic algorithms and cipher suites.			5, May, 2011 @ 1351 Documentation: NA Functional: NA Not Applicable There is no VPN for the Voting System.	15, June, 2011 @ 0844 Documentation: Pass Functional: Insufficient Robustness There was no certification for the Open VPN cryptographic module.	5, May, 2011 @ 1351 Documentation: NA Functional: NA Not Applicable There is no VPN for the Voting System.	10, May, 2011 @ 1250 Documentation: NA Functional: NA Not Applicable. There is no VPN for the Voting System.	16, May, 2011 @ 1001 Documentation: NA Functional: NA Not Applicable. There is no VPN for the Voting System.	16, June, 2011 @ 0815 Documentation: Insufficient Robustness Functional: NT due to lack of access	6, May, 2011 @ 1437 Documentation: Not Applicable Functional: Not Applicable There is no VPN for the Voting System.	1		
	5.5.1.4 Unique system identifier		x		x	Agree with Requirement	Each communicating device SHALL have a unique system identifier			5, May, 2011 @ 1412 Documentation: Insufficient Robustness Functional: NT Not Tested. It could not be tested for a unique system identifier on the destination side as here was no access to the remote system. The source side, the vote capture system, was tested successfully.	15, June, 2011 @ 0846 Documentation: Pass Functional: NT because of the VPN encryption	5, May, 2011 @ 1412 Documentation: Insufficient Robustness Functional: NT Not Tested. It could not be tested for a unique system identifier on the destination side as here was no access to the remote system. The source side, the vote capture system, was tested successfully.	10, May, 2011 @ 1259 Documentation: NA Functional: NT - due to lack of access.	16, May, 2011 @ 1002 Documentation: NA Functional: NA Not Applicable. There is no VPN for the Voting System.	16, June, 2011 @ 0815 Documentation: Insufficient Robustness Functional: NT due to lack of access	6, May, 2011 @ 1452 Documentation: Insufficient Robustness Functional: NT - lack of access	1		
	5.5.1.5 Mutual authentication required	x		x		Recommend referencing appropriate NIST publication (SP 800-63) to more clearly define "mutually strongly authenticate"	Each device SHALL mutually strongly authenticate using the system identifier before additional network data packets are processed.			5, May, 2011 @ 1430 Documentation: Insufficient Robustness Functional: Pass	15, June, 2011 @ 0848 Documentation: Pass Functional: NT because of the VPN	5, May, 2011 @ 1430 Documentation: Insufficient Robustness Functional: Pass	10, May, 2011 @ 1301 Documentation: Pass Functional: Pass	16, May, 2011 @ 1007 Documentation: Insufficient Robustness Functional: Pass	16, June, 2011 @ 0815 Documentation: Insufficient Robustness Functional: NT due to lack of access	6, May, 2011 @ 1459 Documentation: Insufficient Robustness Functional: Pass		1	
	5.5.1.6 Secrecy of ballot data	x		x		1) This requirement should be split out 2) Recommend more clearly state that voter data is to be encrypted. "Preserve the secrecy ..." creates ambiguity.	Data transmission SHALL preserve the secrecy of voters' ballot selections and SHALL prevent the violation of ballot secrecy and integrity.		Documentation: Insufficient Robustness Functional: Insufficient Robustness	5, May, 2011 @ 1438 Documentation: Insufficient Robustness Functional: Pass	15, June, 2011 @ 0850 Documentation: Pass Functional: NT because of the VPN encryption	5, May, 2011 @ 1438 Documentation: Insufficient Robustness Functional: Pass	10, May, 2011 @ 1303 Documentation: Insufficient Robustness Functional: Both PIN & Elector ID are displayed in clear text under the URL	16, May, 2011 @ 1027 Documentation: Insufficient Robustness Functional: Pass	16, June, 2011 @ 0815 Documentation: Insufficient Robustness Functional: NT due to lack of access	6, May, 2011 @ 1510 Documentation: Insufficient Robustness Functional: Pass		1	
	5.5.2 External Threats	x				"SHALL" should be removed from header	Voting systems SHALL implement protections against external threats to which the system may be susceptible.			Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Manufacturer 3	Manufacturer 4	Manufacturer 5	Manufacturer 6	Manufacturer 7	Can be met today?	Need Modification	Delete
	5.5.2.1 Disabling network interfaces	x		x		Agree with Requirement	Voting system components SHALL have the ability to enable or disable physical network interfaces.			9, May, 2011 @ 1115 Documentation: Pass Functional: Pass	15, June, 2011 @ 1000 Documentation: Pass Functional: NT due to time constraints	9, May, 2011 @ 1115 Documentation: Pass Functional: Pass	9, May, 2011 @ 1255 Documentation: NA Functional: NA Manufacturer's voting system is accessed via non-secure computers. No kiosk equipment is	11, May, 2011 @ 0745 Documentation: Insufficient Robustness Functional: Pass	10, May, 2011 @ 0825 Documentation: Insufficient Robustness Functional: NT due to lack of access	11, May, 2011 @ 1415 Documentation: Insufficient Robustness Functional: NT - due to lack of access.	1		
	5.5.2.2 Minimizing interfaces		x		x	Need to define test method "Inspection/Vulnerability"	The number of active ports and associated network services and protocols SHALL be restricted to the minimum required for the voting system to function.			9, May, 2011 @ 1125 Documentation: Insufficient Robustness Functional: Pass Manufacturer's provided documentation does not detail which ports are required by the voting system and their associated network services and protocols.	15, June, 2011 @ 1020 Documentation: Pass Functional: Pass	9, May, 2011 @ 1125 Documentation: Insufficient Robustness Functional: Pass Manufacturer's provided documentation does not detail which ports are required by the voting system and their associated network services and protocols.	9, May, 2011 @ 1300 Documentation: Insufficient Robustness Functional: NT - due to lack of information.	11, May, 2011 @ 0745 Documentation: Insufficient Robustness Functional: There are no guidelines found for inactivating unnecessary ports on the voting hardware.	10, May, 2011 @ 0825 Documentation: Insufficient Robustness Functional: NT due to lack of access	11, May, 2011 @ 1420 Documentation: Insufficient Robustness Functional: NT - due to lack of information.	1		
	5.5.2.3 Prevention of attacks and security non-compliance	x		x		Make this 5.5.2.4 need to define test method "Functional/Vulnerability"	The voting system SHALL block all network connections that are not over a mutually authenticated channel.			9, May, 2011 @ 1130 Documentation: Pass Functional: Pass Manufacturer's 'System Security Specification' section 'Server Side Security details' confirms that the voting system was designed to authenticate transmissions although there is no explicit statement regarding blocking all network connections that are not over a mutually authenticated channel.	15, June, 2011 @ 1100 Documentation: Pass Functional: Pass Vendor defines the network authentication processes.	9, May, 2011 @ 1130 Documentation: Pass Functional: Pass Manufacturer's 'System Security Specification' section 'Server Side Security details' confirms that the voting system was designed to authenticate transmissions although there is no explicit statement regarding blocking all network connections that are not over a mutually authenticated channel.	9, May, 2011 @ 1305 Documentation: NA Functional: NA Manufacturer's voting system is accessed via non-secure computers. No kiosk equipment is provided.	11, May, 2011 @ 0745 Documentation: Insufficient Robustness Functional: NT - See Req. 5.3 for attacks and security non-compliance	10, May, 2011 @ 0825 Documentation: Insufficient Robustness Functional: NT - Manufacturer's provided documentation did not describe channel authentication nor the blocking of network connections.	11, May, 2011 @ 1440 Documentation: Insufficient Robustness Functional: NT - See Req. 5.9	1		
							Section totals										7	2	
	5.6 Logging									Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			
	5.6.1 Log Management									Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			
	5.6.1.1 Default settings		x		x	1) This should be split to more discrete sub requirements 2) term "default settings" is ambiguous, should require "minimal settings" as per NIST SP 800-92	The voting system SHALL implement default settings for secure log management activities, including log generation, transmission, storage, analysis, and disposal.			10, May, 2011 @ 0808 Documentation: Insufficient Robustness Functional: Insufficient Robustness Unable to determine if the internet voting system implements default settings for secure log management activities	2, June, 2011 @ 0904 Documentation: Insufficient Robustness Functional: Insufficient Robustness Unable to determine if the voting system implements default settings for secure log management activities	10, May, 2011 @ 0808 Documentation: Insufficient Robustness Functional: Insufficient Robustness Unable to determine if the Internet voting system implements default settings for secure log management activities	20, April, 2011 @ 1015 Documentation: Insufficient Robustness Functional: Unable to determine if the Internet voting system implements default settings for secure log management activities	9, May, 2011 @ 1001 Documentation: Insufficient Robustness Functional: The voting system does not generate time and date values	20, May, 2011 @ 1022 17, June, 2011 @ 0750 Documentation: Insufficient Robustness Functional: Unable to determine if the Internet voting system implements default settings for secure log management activities	13, May, 2011 @ 0917 Documentation: Insufficient Robustness Functional: Unable to determine if the Internet voting system implements default settings for secure log management activities	1		
	5.6.1.2 Log access	x		x		Term "authorized roles" is undefined within the requirements. This should be more clearly defined	Logs SHALL only be accessible to authorized roles			10, May, 2011 @ 1015 Documentation: Insufficient Robustness Functional: Insufficient Robustness Unable to locate documentation on log in roles and the log files they have access to.	16, June, 2011 @ 0916 Documentation: Pass Functional: Pass Logs are accessible to authorized roles. Roles authorized to access each log file within the system, are able to do so Roles not authorized to access each log file within the system, are not able to do so	10, May, 2011 @ 1015 Documentation: Insufficient Robustness Functional: Insufficient Robustness Unable to locate documentation on log in roles and the log files they have access to.	13, May, 2011 @ 1549 Passed: No information available in the documentation, but determined via logging on to IVAdministration that all Users with a role of Operator are restricted from accessing the administrative user management function	6, May, 2011 @ 0913 Failed: Unable to log on to the Administration system as a Superuser	20, May, 2011 @ 1422 17, June, 2011 @ 0750 Failed: Unable to determine authorized log in roles and the log files they have access to	13, May, 2011 @ 0917 Passed: The preferred test method here would be to change the User Group from Admin to a lower privilege of access level, but the only option available at this time for User Group is Admin. Using the Status option - Inactive as a workaround	1		

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Manufacturer 3	Manufacturer 4	Manufacturer 5	Manufacturer 6	Manufacturer 7	Can be met today?	Need Modification	Delete
	5.6.1.3 Log access	x		x		Term "privileged logging processes" is undefined within the requirements. This should be more clearly defined	The voting system SHALL restrict log access to append-only for privileged logging processes and read-only for authorized roles.			10, May, 2011 @ 1252 Documentation: Insufficient Robustness Functional: Insufficient Robustness The voting system allows privileged logging processes to only append to any/all log files The log in remains as the last entry on the audit log. The log in remains as the last entry on the audit log. The voting system does not allow an authorized role to modify or delete a portion of a file or in its entirety	16, June, 2011 @ 1252 Documentation: Pass Functional: Pass The voting system allows privileged logging processes to only append to any/all log files The log in remains as the last entry on the audit log. The log in remains as the last entry on the audit log. The voting system does not allow an authorized role to modify or delete a portion of a file or in its entirety	10, May, 2011 @ 1252 Documentation: Insufficient Robustness Functional: Insufficient Robustness The voting system allows privileged logging processes to only append to any/all log files The log in remains as the last entry on the audit log. The log in remains as the last entry on the audit log. The voting system does not allow an authorized role to modify or delete a portion of a file or in its entirety	13, May, 2011 @ 1411 Documentation: Insufficient Robustness Functional Pass except for: The EED Audit Report will not print in the PDF format.	6, May, 2011 @ 0913 Documentation: Insufficient Robustness Functional: Unable to locate any documentation on a priveleged logging processes role.	20, May, 2011 @ 1422 17, June, 2011 @ 1020 Documentation: Insufficient Robustness Functional: Unable to determine authorized log in roles and the log files they have access to	13, May, 2011 @ 0917 Documentation: Insufficient Robustness Functional: Pass	1		
	5.6.1.4 Logging events	x		x		This should be split out to discrete 3 sub-requirements	The voting system SHALL log logging failures, log clearing, and log rotation.			10, May, 2011 @ 1252 Documentation: Insufficient Robustness Functional: Insufficient Robustness Not all logging correct	16, June, 2011 @ 1311 Documentation: Insufficient Robustness Functional: Insufficient Robustness The voting system does not log all log logging failures, log clearing, and log rotation.	10, May, 2011 @ 1252 Documentation: Insufficient Robustness Functional: Insufficient Robustness Not all logging correct	3, June, 2011 @ 1345 Documentation: Insufficient Robustness Functional: NT - due to lack of information.	9, May, 2011 @ 1035 Documentation: Insufficient Robustness Functional: NT - due to lack of information.	23, May, 2011 @ 1022 17, June, 2011 @ 1102 Documentation: Insufficient Robustness Functional: NT - due to lack of information.	13, May, 2011 @ 1306 Documentation: Insufficient Robustness Functional: NT - due to lack of information.	1		
	5.6.1.5 Log format		x		x	Agree with Requirement	The voting system SHALL store log data in a publicly documented format, such as XML, or include a utility to export log data into a publicly documented format.			10, May, 2011 @ 1252 Documentation: Insufficient Robustness Functional: Pass The format available for reading the stored log data is CSV which is considered a publicly documented format.	16, June, 2011 @ 1311 Documentation: Pass Functional: Pass The document/s are reviewed, the stored log data can be read in a publicly documented format	10, May, 2011 @ 1252 Documentation: Insufficient Robustness Functional: Pass The format available for reading the stored log data is CSV which is considered a publicly documented format.	17, May, 2011 @ 1430 Documentation: Insufficient Robustness Functional: Pass	9, May, 2011 @ 1001 Documentation: Insufficient Robustness Functional: The voting system does not generate time and date valuesat.	20, May, 2011 @ 1022 17, June, 2011 @ 1140 Documentation: Insufficient Robustness Functional: NT due to lack of information	16, May, 2011 @ 0844 Documentation: Insufficient Robustness Functional: NT - due to lack of information.	1		
	5.6.1.6 Log separation	x		x		This should be split out to discrete 2 sub-requirements	The voting system SHALL ensure that each jurisdiction's event logs and each component's logs are separable from each other.			10, May, 2011 @ 1252 Documentation: Insufficient Robustness Functional: Insufficient Robustness Unable to locate documentation on jurisdictions of the voting system and the procedures to generate logs by jurisdiction	16, June, 2011 @ 1311 Documentation: Insufficient Robustness Functional: Insufficient Robustness There are no entries in the log viewer application regarding jurisdiction	10, May, 2011 @ 1252 Documentation: Insufficient Robustness Functional: Insufficient Robustness Unable to locate documentation on jurisdictions of the voting system and the procedures to generate logs by jurisdiction	17, May, 2011 @ 1458 Documentation: Insufficient Robustness Functional: Unable to separate event logs by jurisdiction	9, May, 2011 @ 1035 Documentation: Insufficient Robustness Functional: Unable to separate event logs by jurisdiction	23, May, 2011 @ 1056 17, June, 2011 @ 1140 Documentation: Insufficient Robustness Functional: Unable to separate event logs by jurisdiction	16, May, 2011 @ 0844 Documentation: Insufficient Robustness Functional: Unable to separate event logs by jurisdiction	1		
	5.6.1.7 Log review	x		x		This should be split out to 3 discrete sub-requirements	The voting system SHALL include an application or program to view, analyze, and search event logs.			11, May, 2011 @ 0915 Documentation: Insufficient Robustness Functional: Insufficient Robustness The voting system provides a method for searching event logs The voting system provides a method for analyzing event logs The voting system provides a method for analyzing event logs	16, June, 2011 @ 1311 Documentation: Insufficient Robustness Functional: Insufficient Robustness Unable to perform calculations and comparisons on the event logs Unable to perform a search/query of the event logs	11, May, 2011 @ 0915 Documentation: Insufficient Robustness Functional: Insufficient Robustness The voting system provides a method for searching event logs The voting system provides a method for analyzing event logs The voting system provides a method for analyzing event logs	17, May, 2011 @ 1353 Documentation: Insufficient Robustness Functional: NT - due to lack of information	9, May, 2011 @ 1001 Documentation: Insufficient Robustness Functional: NT - due to lack of information	23, May, 2011 @ 1143 17, June, 2011 @ 1250 Documentation: Insufficient Robustness Functional: NT - due to lack of information	16, May, 2011 @ 0844 Documentation: Insufficient Robustness Functional: Pass	1		
	5.6.1.8 Log preservation		x		x	Term "prior to voting system decommissioning" is ambiguous. We believe the intent is that the log data remains intact for the life cycle of the given election data for a particular election. This may be defined at the jurisdictional level.	All logs SHALL be preserved in a useable manner prior to voting system decommissioning.	2.1.5.1.a	v. The generation of audit record entries shall not be terminated or altered by program control, or by the intervention of any person. The physical security and integrity of the record shall be maintained at all times.	11, May, 2011 @ 0915 Failed: Unable to determine how the logs are to be preserved prior to the voting system decommissioning.	16, June, 2011 @ 1402 Documentation: Pass Functional: Pass All log files are preserved such that they are accessible even after the voting system has been decommissioned	11, May, 2011 @ 0915 Failed: Unable to determine how the logs are to be preserved prior to the voting system decommissioning.	21, April, 2011 @ 0915 Documentation: Insufficient Robustness	9, May, 2011 @ 1001 Documentation: Insufficient Robustness	20, May, 2011 @ 1022 17, June, 2011 @ 1250 Documentation: Insufficient Robustness	16, May, 2011 @ 1007 Documentation: Insufficient Robustness	1		
	5.6.1.9 Voter privacy	x		x		Agree with Requirement	Logs SHALL NOT contain any data that could violate the privacy of the voter's identity.			11, May, 2011 @ 1007 Documentation: Insufficient Robustness Functional: Insufficient Robustness There are unidentified fields in the voting system log files. No voting system log file contains any data that could violate the privacy of the voter's identity	16, June, 2011 @ 1402 Documentation: Pass Functional: Pass There are no unidentified fields in the voting system log files. No voting system log file contains any data that could violate the privacy of the voter's identity	11, May, 2011 @ 1007 Documentation: Insufficient Robustness Functional: Insufficient Robustness There are unidentified fields in the voting system log files. No voting system log file contains any data that could violate the privacy of the voter's identity	16, May, 2011 @ 1324 Documentation: Pass Functional: Pass	9, May, 2011 @ 1035 Documentation: Pass Functional: Pass	23, May, 2011 @ 1143 17, June, 2011 @ 1328 Documentation: Pass Functional: Pass	16, May, 2011 @ 1007 Documentation: insufficient Robustness Functional: The audit logs contain voter identity information	1		

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Manufacturer 3	Manufacturer 4	Manufacturer 5	Manufacturer 6	Manufacturer 7	Can be met today?	Need Modification	Delete
	5.6.1.10 Timekeeping format	x		x		Agree with Requirement	Timekeeping mechanisms SHALL generate time and date values, including hours, minutes, and seconds	2.1.5.1 a	ii. All systems shall include a real-time clock as part of the system's hardware. The system shall maintain an absolute record of the time and date or a record relative to some event whose time and data are known and recorded.	11, May, 2011 @ 1007 Documentation: Pass Functional: Pass.	16, June, 2011 @ 1402 Documentation: Pass Functional: Pass The Instructions to Kiosk Voters dialog opens with the current system date and time displayed	11, May, 2011 @ 1007 Documentation: Pass Functional: Pass.	16, May, 2011 @ 1319 Documentation: Pass Functional: EED Passed IVAdmin does not display the time and date values, including but not limited to hours, minutes, and seconds as required by 5.6.1.10.	19, May, 2011 @ 0940 Documentation: Insufficient Robustness Functional: The voting system does not generate time and date values	23, May, 2011 @ 1143 17, June, 2011 @ 1328 Documentation: Pass Functional: Pass	16, May, 2011 @ 1147 Documentation: Pass Functional: Pass	1		
	5.6.1.11 Timekeeping precision				x	Agree with Requirement	The precision of the timekeeping mechanism SHALL be able to distinguish and properly order all log events.			11, May, 2011 @ 1007 Documentation: Pass Functional: Pass	16, June, 2011 @ 1402 Documentation: Pass Functional: Pass The time keeping mechanism implemented by the voting system is of a precision such that all log events are distinguishable and properly ordered	11, May, 2011 @ 1007 Documentation: Pass Functional: Pass	17, May, 2011 @ 1440 Documentation: Insufficient Robustness Functional: Pass	9, May, 2011 @ 1319 Documentation: Pass Functional: Pass	20, May, 2011 @ 1055 17, June, 2011 @ 1328 Documentation: Insufficient Robustness Functional: Unable to determine if the log events are distinguishable and properly ordered	16, May, 2011 @ 1311 Documentation: Pass Functional: Pass	1		
	5.6.1.12 System clock security		x	x		Would recommend that the "system administrator" role be changed to indicate an appropriately authorized election official	Only the system administrator SHALL be permitted to set the system clock			11, May, 2011 @ 1041 Documentation: Insufficient Robustness Functional: Insufficient Robustness Non authorized user able to set the system clock	16, June, 2011 @ 1419 Documentation: Insufficient Robustness Functional: Pass No procedures found in the documentation. Logged on to the Mixing server and accessed the Date and Time option in the Control Panel function	11, May, 2011 @ 1041 Documentation: Insufficient Robustness Functional: Insufficient Robustness Non authorized user able to set the system clock	16, May, 2011 @ 1311 Documentation: Insufficient Robustness Functional: Unable to set the system clock. There is no documentation of system clock setting procedures.	9, May, 2011 @ 1319 Documentation: Insufficient Robustness Functional: The voting system does not generate time and date values	23, May, 2011 @ 1143 17, June, 2011 @ 1402 Documentation: Insufficient Robustness Functional: Unable to locate documentation on setting the system clock	16, May, 2011 @ 1311 Documentation: Insufficient Robustness Functional: Unable to locate documentation on setting the system clock	1		
	5.6.2 Communications Logging									Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			
	5.6.2.1 General				x	Agree with Requirement	All communications actions SHALL be logged.			11, May, 2011 @ 1117 Documentation: Insufficient Robustness Inspection: Pass Generated an event log and used the output to verify the logging capabilities	16, June, 2011 @ 1419 Documentation: Insufficient Robustness Inspection: Pass The Log viewer application in Linux allows for the real time audit of the voting process. VI Editor allows for the auditing of the communications	11, May, 2011 @ 1117 Documentation: Insufficient Robustness Inspection: Pass Generated an event log and used the output to verify the logging capabilities	17, May, 2011 @ 1455 Documentation: Insufficient Robustness Inspection: Pass	6, May, 2011 @ 1020 Documentation: Insufficient Robustness Inspection: Failed Unable to determine the logging capabilities of all of the voting system's forms of communication	25, April, 2011 12, May, 2011 @ 0945 17, June, 2011 @ 1402 Documentation: Insufficient Robustness Inspection: Failed Unable to determine the logging capabilities of all of the voting system's forms of communication	16, May, 2011 @ 1426 Documentation: Insufficient Robustness Inspection: Pass Unable to determine the logging capabilities of all forms of communication from the documentation	1		
	5.6.2.2 Log content	x		x		1) Enumerate, not using bullets, must be able to explicitly reference 2) Similar to 5.6.3.1, test method should be Inspection	The communications log SHALL contain at least the following entries:			Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	1		
		x		x		Agree with Requirement	Times when the communications are activated and deactivated;			11, May, 2011 @ 1239 Documentation: Insufficient Robustness Functional: Insufficient Robustness No listing of deactivation	16, June, 2011 @ 1419 Documentation: Pass Functional: Pass	11, May, 2011 @ 1239 Documentation: Insufficient Robustness Functional: Insufficient Robustness No listing of deactivation	13, May, 2011 @ 1331 Documentation: Insufficient Robustness Functional: Unable to set the system clock.	9, May, 2011 @ 0804 Documentation: Insufficient Robustness Functional: NT - due to lack of information	23, May, 2011 @ 1307 17, June, 2011 @ 1402 Documentation: Insufficient Robustness Functional: NT - due to lack of information	16, May, 2011 @ 1426 Documentation: Insufficient Robustness Functional: NT - due to lack of information	1		

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Manufacturer 3	Manufacturer 4	Manufacturer 5	Manufacturer 6	Manufacturer 7	Can be met today?	Need Modification	Delete
		x		x		Agree with Requirement	Services accessed;			11, May, 2011 @ 1239 Documentation: Insufficient Robustness Functional: Insufficient Robustness Not all services accessed listed	16, June, 2011 @ 1419 Documentation: Pass Functional: Pass	11, May, 2011 @ 1239 Documentation: Insufficient Robustness Functional: Insufficient Robustness Not all services accessed listed	13, May, 2011 @ 1318 Documentation: Insufficient Robustness Functional: NT - due to lack of information	9, May, 2011 @ 0929 Documentation: Insufficient Robustness Functional: NT - due to lack of information	23, May, 2011 @ 1307 17, June, 2011 @ 1402 Documentation: Insufficient Robustness Functional: NT - due to lack of information	16, May, 2011 @ 1503 Documentation: Insufficient Robustness Functional: NT - due to lack of information	1		
		x		x		Agree with Requirement	Identification of the device which data was transmitted to or received from;			11, May, 2011 @ 1455 Documentation: Insufficient Robustness Functional: Pass	16, June, 2011 @ 1532 Documentation: Pass Functional: Pass	11, May, 2011 @ 1455 Documentation: Insufficient Robustness Functional: Pass	13, May, 2011 @ 1043 Documentation: Insufficient Robustness Functional: NT - due to lack of information	9, May, 2011 @ 0810 Documentation: Insufficient Robustness Functional: NT - due to lack of information	23, May, 2011 @ 1307 17, June, 2011 @ 1402 Documentation: Insufficient Robustness Functional: NT - due to	17, May, 2011 @ 0917 Documentation: Insufficient Robustness Functional: NT - due to lack of information	1		
		x		x		Agree with Requirement	Identification of authorized entity; and			3, June, 2011 @ 1015 Documentation: Insufficient Robustness Functional: Insufficient Robustness	16, June, 2011 @ 1532 Documentation: Insufficient Robustness Functional: Insufficient Robustness	3, June, 2011 @ 1015 Documentation: Insufficient Robustness Functional: Insufficient Robustness	17, May, 2011 @ 1404 Documentation: Insufficient Robustness Functional: NT - due to lack of information	9, May, 2011 @ 1252 Documentation: Insufficient Robustness Functional: NT - due to lack of information	23, May, 2011 @ 1307 17, June, 2011 @ 1440 Documentation: Insufficient Robustness Functional: NT - due to lack of information	17, May, 2011 @ 1002 Documentation: Insufficient Robustness Functional: NT - due to lack of information	1		
		x		x		Agree with Requirement	Successful and unsuccessful attempts to access communications or services.			12, May, 2011 @ 0911 Documentation: Insufficient Robustness Functional: Insufficient Robustness Not all services access attempts listed	16, June, 2011 @ 1604 Documentation: Insufficient Robustness Functional: Pass	12, May, 2011 @ 0911 Documentation: Insufficient Robustness Functional: Insufficient Robustness Not all services access attempts listed	17, May, 2011 @ 1404 Documentation: Insufficient Robustness Functional: NT - due to lack of information	9, May, 2011 @ 1252 Documentation: Insufficient Robustness Functional: NT - due to lack of information	23, May, 2011 @ 1348 17, June, 2011 @ 1505 Documentation: Insufficient Robustness Functional: NT - due to lack of information	17, May, 2011 @ 1114 Documentation: Insufficient Robustness Functional: NT - due to lack of information	1		
	5.6.3 System Event Logging						This section describes requirements for the voting system to perform event logging for system maintenance troubleshooting, recording the history of system activity, and detecting unauthorized or malicious activity. The operating system, and/or applications software may perform the actual event logging. There may be multiple logs in use for any system component.	2.1.4 g	Record and report the date and time of normal and abnormal events	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			
								2.1.4 h	Maintain a permanent record of all original audit data that cannot be modified or overridden but may be augmented by designated authorized officials in order to adjust for errors or omissions (e.g., during the canvassing process)										
								2.1.4 i	Detect and record every event, including the occurrence of an error condition that the system cannot overcome, and time-dependent or programmed events that occur without the intervention of the voter or a polling place operator										
								2.1.5.1 a	ii. All systems shall include a real-time clock as part of the system's hardware. The system shall maintain an absolute record of the time and date or a record relative to some event whose time and data are known and recorded										
	5.6.3.1 Event log format		x			Agree with Requirement	The voting system SHALL log the following data for each event:			Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			
			x		x	Agree with Requirement	a. System ID;			12, May, 2011 @ 0911 Documentation: Insufficient Robustness Functional: Insufficient Robustness	16, June, 2011 @ 1604 Documentation: Insufficient Robustness Functional: Insufficient Robustness	12, May, 2011 @ 0911 Documentation: Insufficient Robustness Functional: Insufficient Robustness	17, May, 2011 @ 1404 Documentation: Insufficient Robustness Functional: NT - due to lack of information	9, May, 2011 @ 1252 Documentation: Insufficient Robustness Functional: NT - due to lack of information	23, May, 2011 @ 1348 17, June, 2011 @ 1505 Documentation: Insufficient Robustness Functional: NT - due to lack of information	17, May, 2011 @ 1114 Documentation: Insufficient Robustness Functional: NT - due to lack of information	1		
			x		x	Agree with Requirement	b. Unique event ID and/or type;			12, May, 2011 @ 0911 Documentation: Insufficient Robustness Functional: Insufficient Robustness	16, June, 2011 @ 1604 Documentation: Insufficient Robustness Functional: Insufficient Robustness	12, May, 2011 @ 0911 Documentation: Insufficient Robustness Functional: Insufficient Robustness	17, May, 2011 @ 1404 Documentation: Insufficient Robustness Functional: NT - due to lack of information	9, May, 2011 @ 1252 Documentation: Insufficient Robustness Functional: NT - due to lack of information	23, May, 2011 @ 1348 17, June, 2011 @ 1505 Documentation: Insufficient Robustness Functional: NT - due to lack of information	17, May, 2011 @ 1114 Documentation: Insufficient Robustness Functional: NT - due to lack of information	1		
			x		x	Agree with Requirement	c. Timestamp;	2.1.5.1 a	iii.All audit record entries shall include the time-and-date stamp.	12, May, 2011 @ 0911 Documentation: Insufficient Robustness Functional: Insufficient Robustness	16, June, 2011 @ 1604 Documentation: Insufficient Robustness Functional: Insufficient Robustness	12, May, 2011 @ 0911 Documentation: Insufficient Robustness Functional: Insufficient Robustness	17, May, 2011 @ 1404 Documentation: Insufficient Robustness Functional: NT - due to lack of information	9, May, 2011 @ 1252 Documentation: Insufficient Robustness Functional: NT - due to lack of information	23, May, 2011 @ 1348 17, June, 2011 @ 1505 Documentation: Insufficient Robustness Functional: NT - due to lack of information	17, May, 2011 @ 1114 Documentation: Insufficient Robustness Functional: NT - due to lack of information	1		

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Manufacturer 3	Manufacturer 4	Manufacturer 5	Manufacturer 6	Manufacturer 7	Can be met today?	Need Modification	Delete
			x		x	Agree with Requirement	d. Success or failure of event, if applicable;			12, May, 2011 @ 0911 Documentation: Insufficient Robustness Functional: Insufficient Robustness	16, June, 2011 @ 1604 Documentation: Insufficient Robustness Functional: Insufficient Robustness	12, May, 2011 @ 0911 Documentation: Insufficient Robustness Functional: Insufficient Robustness	17, May, 2011 @ 1404 Documentation: Insufficient Robustness Functional: NT - due to lack of information	9, May, 2011 @ 1252 Documentation: Insufficient Robustness Functional: NT - due to lack of information	23, May, 2011 @ 1348 17, June, 2011 @ 1505 Documentation: Insufficient Robustness Functional: NT - due to lack of information	17, May, 2011 @ 1114 Documentation: Insufficient Robustness Functional: NT - due to lack of information	1		
			x		x	Agree with Requirement	e. User ID triggering the event, if applicable; and			12, May, 2011 @ 0911 Documentation: Insufficient Robustness Functional: Insufficient Robustness	16, June, 2011 @ 1604 Documentation: Insufficient Robustness Functional: Insufficient Robustness	12, May, 2011 @ 0911 Documentation: Insufficient Robustness Functional: Insufficient Robustness	17, May, 2011 @ 1404 Documentation: Insufficient Robustness Functional: NT - due to lack of information	9, May, 2011 @ 1252 Documentation: Insufficient Robustness Functional: NT - due to lack of information	23, May, 2011 @ 1348 17, June, 2011 @ 1505 Documentation: Insufficient Robustness Functional: NT - due to lack of information	17, May, 2011 @ 1114 Documentation: Insufficient Robustness Functional: NT - due to lack of information	1		
			x		x	Agree with Requirement	f. Jurisdiction, if applicable.			12, May, 2011 @ 0911 Documentation: Insufficient Robustness Functional: Insufficient Robustness	16, June, 2011 @ 1604 Documentation: Insufficient Robustness Functional: Insufficient Robustness	12, May, 2011 @ 0911 Documentation: Insufficient Robustness Functional: Insufficient Robustness	17, May, 2011 @ 1404 Documentation: Insufficient Robustness Functional: NT - due to lack of information	9, May, 2011 @ 1252 Documentation: Insufficient Robustness Functional: NT - due to lack of information	23, May, 2011 @ 1348 17, June, 2011 @ 1505 Documentation: Insufficient Robustness Functional: NT - due to lack of information	17, May, 2011 @ 1114 Documentation: Insufficient Robustness Functional: NT - due to lack of information	1		
	5.6.3.2 Critical events	x		x	x	Define a critical event. The requirement as it is now leaves room for interpretation in regards to the scope of the requirement	All critical events SHALL be recorded in the system event log.	2.1.5.1 c	The voting system shall display and report critical status messages using clear indicators or English language text.	Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT - Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT - Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT - Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT - Due to lack of access, lack of credentials given		1	
	5.6.3.3 System events		x		x	This section would be better served to be broken out into subparagraphs. Referencing back to a row, or a bullet in a cell is many times problematic Additionally the requirement only states "voting system" this is a broad scope of equipment and software. Does this apply to the O/S, The voting system application, or both? General Comment for this table would be to recommend that the term "include but not limited to" be avoided, as this term creates ambiguity and potential for inconsistent interpretation of the requirement	At a minimum the voting system SHALL log the events described in Table 5-2.	2.1.5.1 b		Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met		1	
	Error and exception messages					System interrupts at a operating system / hardware level could be potentially destructive. Source code can be analyzed for an understanding of exception handling routines then a script can be written to invoke a system interrupts that would result in an entry into exception handling routines.	5.6.3.3.a1 - The source and disposition of system interrupts resulting in entry into exception handling routines.	System interrupts at a operating system / hardware level could be potentially dangerous. Source code can be analyzed for an understanding of exception handling routines then a script can be written to invoke a system interrupts that would result in an entry into exception handling routines.		14, May, 2011 @ 0954 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 0954 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1140 Documentation: Insufficient Robustness Functional: NT due to lack of access	23, May, 2011 @ 1030 Documentation: Insufficient Robustness Functional: NT N/T due to lack of clarity for this requirement	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access		1	
						Agree with Requirement	5.6.3.3.a2 - Messages generated by exception handlers.	System interrupts at a operating system / hardware level could be potentially dangerous. Source code can be analyzed for an understanding of exception handling routines then a script can be written to invoke a system interrupts that would result in an entry		14, May, 2011 @ 1006 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1006 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1140 Documentation: Insufficient Robustness Functional: NT due to lack of access	23, May, 2011 @ 1030 Documentation: Insufficient Robustness Functional: NT N/T due to lack of clarity for this requirement	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Manufacturer 3	Manufacturer 4	Manufacturer 5	Manufacturer 6	Manufacturer 7	Can be met today?	Need Modification	Delete
						Agree with Requirement	5.6.3.3.a3 - The identification code and number of occurrences for each hardware and software error or failure.			14, May, 2011 @ 1006 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete	14, May, 2011 @ 1006 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1140 Documentation: Insufficient Robustness Functional: NT due to lack of access	23, May, 2011 @ 1030 Documentation: Insufficient Robustness Functional: NT N/T due to lack of clarity for this requirement	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
						the term "physical violations of security" needs to be better defined as to what is included. I.e. computer room security, motion sensors, chassis alarms, etc.	5.6.3.3.a4 - Notification of physical violations of security.	Supplemental information should be given for this requirement do we test for chassis alarms or alarms on the server cages? Or does this apply to a compromised door?		14, May, 2011 @ 1007 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1007 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1140 Documentation: Insufficient Robustness Functional: NT due to lack of access	23, May, 2011 @ 1030 Documentation: Insufficient Robustness Functional: NT Equipment delivered is a MAC-Mini and the voting system will run on a server running MAC OS X. The Mac mini cannot be taken apart without potentially damaging the equipment.	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
						Agree with Requirement	5.6.3.3.a5 - Other exception events such as power failures, failure of critical hardware components, data transmission errors or other types of operating anomalies.			14, May, 2011 @ 1023 N/T due to lack of access to system	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1023 N/T due to lack of access to system	15, June, 2011 @ 1140 Documentation: Insufficient Robustness Functional: NT due to lack of access	23, May, 2011 @ 1052 Documentation: Insufficient Robustness Functional: Pass	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
						the term "fault" is ambiguous, needs to be more clearly defined.	5.6.3.3.a6 - All faults and the recovery actions taken.	This is a very broad requirement and the scope needs to be defined.		14, May, 2011 @ 1006 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI	14, May, 2011 @ 1006 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1140 Documentation: Insufficient Robustness Functional: NT due to lack of access	23, May, 2011 @ 1052 N/T due to lack of clarity for this requirement	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
						define "ordinary", and seems to be in conflict with bullet 2	5.6.3.3.a7 - Error and exception messages such as ordinary timer system interrupts and normal I/O system interrupts do not need to be logged.	Define "normal"		14, May, 2011 @ 1006 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the	14, May, 2011 @ 1006 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1140 Documentation: Insufficient Robustness Functional: NT due to lack of access	23, May, 2011 @ 1052 Documentation: Insufficient Robustness Functional: NT N/T due to lack of clarity for this requirement	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
	Critical system status messages					1] More detail/criteria is needed to define what is considered critical. "includes but not limited to" creates a large potential for gaps to occur, as well as disagreements by a manufacturer as to what is deemed critical.				Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			
			x		x	Agree with Requirement	Critical system status messages	2.1.5.1 b		Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	1		
			x			Agree with Requirement Though Diagnostics and status messages upon startup do not seem to be critical type message	5.6.3.3.b1 - Critical system status messages Critical system status messages other than information messages displayed by the device during the course of normal operations. Includes but not limited to: Diagnostic and status messages upon startup.			14, May, 2011 @ 1059 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1059 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1140 Documentation: Insufficient Robustness Functional: NT due to lack of access	23, May, 2011 @ 1108 Documentation: Insufficient Robustness Functional: No system and diagnostic messages displayed upon startup.	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Manufacturer 3	Manufacturer 4	Manufacturer 5	Manufacturer 6	Manufacturer 7	Can be met today?	Need Modification	Delete
			x			Agree with Requirement	5.6.3.3.b2 - The "zero totals" check conducted before starting the voting period.			14, May, 2011 @ 1133 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1133 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1140 Documentation: Insufficient Robustness Functional: NT due to lack of access	23, May, 2011 @ 1138 Documentation: NA Functional: NA NA - system is a ballot delivery system	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
	Non-critical status messages		x		x	1) need better criteria for determining what is non-critical versus what is critical status messages. 2) need clarification as to what is meant by "data quality monitor". This term seems to be very subjective and open to interpretation. Likely to cause significant disagreement as to what is included.	5.6.3.3.c - Non-critical status messages Non-critical status messages that are generated by the data quality monitor or by software and hardware condition monitors.	Define "non-critical"		14, May, 2011 @ 1144 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1144 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1140 Documentation: Insufficient Robustness Functional: NT due to lack of access	23, May, 2011 @ 1139 Documentation: Insufficient Robustness Functional: NT N/T due to lack of clarity for this requirement	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access		1	
	Events that require election official intervention					Agree with Requirement	5.6.3.3.d - Events that require election official intervention Events that require election official intervention, so that each election official access can be monitored and access sequence can be constructed.			14, May, 2011 @ 1144 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1144 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1140 Documentation: Insufficient Robustness Functional: NT due to lack of access	23, May, 2011 @ 1140 Documentation: Insufficient Robustness Functional: NT The admin page only has limited options. None of these options allow for the administrator to change any voting systems setting or perform any procedures. Therefore this requirement is not testable since there are no procedures for the administrator to perform	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
	Shutdown and restarts					Recommend adding "Power up" to this line item	5.6.3.3.e - Shutdown and restarts Both normal and abnormal shutdowns and restarts.	Abnormal restarts will not be able to log since there is physically no power to write to file. But the voting system shall differentiate between a normal and abnormal shutdown. Additional verbiage may be required to further explain that the test is looking to accomplish		14, May, 2011 @ 1150 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1150 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1140 Documentation: Insufficient Robustness Functional: NT due to lack of access	23, May, 2011 @ 1151 Documentation: Insufficient Robustness Functional: Pass	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	NT: Without access or a remote testing session the requirements in this section cannot be adequately assessed.	1		
	Changes to system configuration settings					Recommend additional specificity , rather than alluding to "other system configuration settings"	5.6.3.3.f - Changes to system configuration settings Configuration settings include but are not limited to registry keys, kernel settings, logging settings, and other system configuration settings.	No registry in Unix/Linux/Mac OSX operating systems. No kernel setting in Windows operating systems.		14, May, 2011 @ 1155 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1155 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1310 Documentation: Insufficient Robustness Functional: NT due to lack of access	23, May, 2011 @ 1435 Documentation: Insufficient Robustness Functional: NT Registry keys not tested. Kernel settings - Pass Network settings - Fail	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
	Integrity checks for executables, configuration files, data and logs					Should explicitly call out "logs" in description	5.6.3.3.g - Integrity checks for executables, configuration files, data, and logs Integrity checks that may indicate possible tampering with files and data.			14, May, 2011 @ 1205 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1205 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1310 Documentation: Insufficient Robustness Functional: NT due to lack of access	23, May, 2011 @ 1500 Documentation: Insufficient Robustness Functional: NT Found no procedures to check the integrity of said elements	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		

GAP Analysis Matrix	Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Manufacturer 3	Manufacturer 4	Manufacturer 5	Manufacturer 6	Manufacturer 7	Can be met today?	Need Modification	Delete
The addition and deletion of files					Recommend additional detail as to file types. Would not recommend having to track temporary files that are automatically handled within the system	5.6.3.3.h - The addition and deletion of files Files added or deleted from the system.			14, May, 2011 @ 1210 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1210 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1310 Documentation: Insufficient Robustness Functional: NT due to lack of access	23, May, 2011 @ 1511 Documentation: Insufficient Robustness Functional: Pass	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
System readiness results					Agree with Requirement	5.6.3.3.i1 - System readiness results Includes but not limited to: System pass or fail of hardware and software test for system readiness.	"system readiness" needs to be defined. is it a test like "POST" that is conducted every time the voting system is started? Is it a manual procedure that should be conducted before running the voting system?		14, May, 2011 @ 1217 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1217 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1310 Documentation: Insufficient Robustness Functional: NT due to lack of access	23, May, 2011 @ 1513 Documentation: Insufficient Robustness Functional: NT NT: System does not have a procedure for readiness test.	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
					Agree with Requirement	5.6.3.3.i2 - Identification of the software release, identification of the election to be processed, kiosk locations, and the results of the software and hardware diagnostic tests.	"system readiness" needs to be defined. is it a test like "POST" that is conducted every time the voting system is started? Is it a manual procedure that should be conducted before running the voting system?		14, May, 2011 @ 1217 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1217 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1310 Documentation: Insufficient Robustness Functional: NT due to lack of access	23, May, 2011 @ 1517 Documentation: Insufficient Robustness Functional: NT NT: System does not have a procedure for readiness test.	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
					Agree with Requirement	5.6.3.3.i3 - Pass or fail of ballot style compatibility and integrity test.	"system readiness" needs to be defined. is it a test like "POST" that is conducted every time the voting system is started? Is it a manual procedure that should be conducted before running the voting system?		14, May, 2011 @ 1217 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1217 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1348 Documentation: Insufficient Robustness Functional: NT due to lack of access	23, May, 2011 @ 1526 Documentation: Insufficient Robustness Functional: NT NT: System does not have a procedure for readiness test.	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	NT: Without access or a remote testing session the requirements in this section cannot be adequately assessed.	1		
					Agree with Requirement	5.6.3.3.i4 - Pass or fail of system test data removal.	What is "system test data"? "system readiness" needs to be defined. is it a test like "POST" that is conducted every time the voting system is started? Is it a manual procedure that should be conducted before running the voting system?	NT system does not have a procedure for readyness test.	14, May, 2011 @ 1217 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1217 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1348 Documentation: Insufficient Robustness Functional: NT due to lack of access	23, May, 2011 @ 1526 Documentation: Insufficient Robustness Functional: NT NT: System does not have a procedure for readiness test.	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
Removable media events					Agree with Requirement	5.6.3.3.j - Removable media events Removable media that is inserted into or removed from the system.			14, May, 2011 @ 1219 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1219 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1348 Documentation: Insufficient Robustness Functional: NT due to lack of access	23, May, 2011 @ 1528 Documentation: Insufficient Robustness Functional: Pass	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
Backup and restore					Agree with Requirement	5.6.3.3.k - Backup and restore Successful and failed attempts to perform backups and restores.			14, May, 2011 @ 1223 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1223 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1348 Documentation: Insufficient Robustness Functional: NT due to lack of access	23, May, 2011 @ 1531 Documentation: Insufficient Robustness Functional: Pass	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
Authentication related events					Agree with Requirement	5.6.3.3.l1 - Authentication related events Includes but not limited to: Login/logoff events (both successful and failed attempts).			14, May, 2011 @ 1224 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1224 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1400 Documentation: Insufficient Robustness Functional: NT due to lack of access	24, May, 2011 @ 1030 Documentation: Insufficient Robustness Functional: Pass	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Manufacturer 3	Manufacturer 4	Manufacturer 5	Manufacturer 6	Manufacturer 7	Can be met today?	Need Modification	Delete
						Agree with Requirement	5.6.3.3.L2 - Account lockout events.			14, May, 2011 @ 1233 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1233 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1400 Documentation: Insufficient Robustness Functional: NT due to lack of access	24, May, 2011 @ 1040 Documentation: Insufficient Robustness Functional: NT	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
						Agree with Requirement	5.6.3.3.L3 - Password changes.			14, May, 2011 @ 1235 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1235 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1400 Documentation: Insufficient Robustness Functional: NT due to lack of access	24, May, 2011 @ 1050 Documentation: Insufficient Robustness Functional: No entry in audit logs for the password change	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
	Access control related events					Agree with Requirement	5.6.3.3.m1 - Access control related events Includes but not limited to: Use of privileges.			14, May, 2011 @ 1239 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1239 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1400 Documentation: Insufficient Robustness Functional: NT due to lack of access	24, May, 2011 @ 1054 Documentation: Insufficient Robustness Functional: NT NT: System does not have a procedure for readiness test.	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
						Agree with Requirement	5.6.3.3.m2 - Attempts to exceed privileges.			14, May, 2011 @ 1245 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1245 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1400 Documentation: Insufficient Robustness Functional: NT due to lack of access	24, May, 2011 @ 1102 Documentation: Insufficient Robustness Functional: NT	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
						Recommend removal of "...and underlying system resources", as this is beyond the scope of the voting system applications logging scope.	5.6.3.3.m3 - All access attempts to application and underlying system resources.			14, May, 2011 @ 1250 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1250 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1440 Documentation: Insufficient Robustness Functional: NT due to lack of access	24, May, 2011 @ 1103 Documentation: Insufficient Robustness Functional: Voting system does not recognize attempts at accessing underlying system resources are not logged.	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
						Agree with Requirement	5.6.3.3.m4 - Changes to the access control configuration of the system.			14, May, 2011 @ 1255 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1255 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1440 Documentation: Insufficient Robustness Functional: NT due to lack of access	24, May, 2011 @ 1110 Documentation: Insufficient Robustness Functional: NT	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
	User account and role (or groups) management activity					Agree with Requirement	5.6.3.3.n1 - User account and role (or groups) management activity Includes but not limited to: Addition and deletion of user accounts and roles.			14, May, 2011 @ 1306 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1306 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1440 Documentation: Insufficient Robustness Functional: NT due to lack of access	24, May, 2011 @ 1111 Documentation: Insufficient Robustness Functional: Addition and deletion of user accounts not logged.	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
						Agree with Requirement	5.6.3.3.n2 - User account and role suspension and reactivation.			14, May, 2011 @ 1300 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1300 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1440 Documentation: Insufficient Robustness Functional: NT due to lack of access	24, May, 2011 @ 1237 Documentation: Insufficient Robustness Functional: NT: Functionality not avaible on curent equipment	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
						Agree with Requirement	5.6.3.3.n3 - Changes to account or role security attributes such as password length, access levels, login restrictions, permissions.			14, May, 2011 @ 1311 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1311 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1440 Documentation: Insufficient Robustness Functional: NT due to lack of access	24, May, 2011 @ 1237 Documentation: Insufficient Robustness Functional: NT: Functionality not avaible on curent equipment	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Manufacturer 3	Manufacturer 4	Manufacturer 5	Manufacturer 6	Manufacturer 7	Can be met today?	Need Modification	Delete
						Agree with Requirement	5.6.3.3.n4 - Administrator account and role password resets.			14, May, 2011 @ 1311 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1311 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1440 Documentation: Insufficient Robustness Functional: NT due to lack of access	24, May, 2011 @ 1237 Documentation: Insufficient Robustness Functional: NT: Functionality not avaible on curent equipment	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
	Installation, upgrading, patching, or modification of software or firmware					1) This line item needs to be explicitly broken out to individual requirements. The potential scope is very large. In an initial certification, upgrading/patching/modification may well not be available. 2) "Cryptographic hash" needs to be defined. Would recommend using "hash code" instead.	5.6.3.3.o - Installation, upgrading, patching, or modification of software or firmware Logging for installation, upgrading, patching, or modification of software or firmware include logging what was installed, upgraded, or modified as well as a cryptographic hash or other secure identifier of the old and new versions of the data.			14, May, 2011 @ 1314 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1314 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1440 Documentation: Insufficient Robustness Functional: NT due to lack of access	24, May, 2011 @ 1240 Documentation: Insufficient Robustness Functional: NT Functionality not avaible on curent equipment Due to lack of procedure	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
	Changes to configuration settings					This requirement should be split out to more explicitly address either voting system applications or the underlying operating system	5.6.3.3.p1 - Changes to configuration settings Includes but not limited to: Changes to critical function settings. At a minimum critical function settings include location of ballot definition file, contents of the ballot definition file, vote reporting, location of logs, and system configuration settings.			14, May, 2011 @ 1320 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1320 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1515 Documentation: Insufficient Robustness Functional: NT due to lack of access	24, May, 2011 @ 1241 Documentation: Insufficient Robustness Functional: NT: Voting system does not log the change to configuration settings	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
						This requirement should be split out to more explicitly address either voting system applications or the underlying operating system	5.6.3.3.p2 - Changes to settings including but not limited to enabling and disabling services.			14, May, 2011 @ 1325 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1325 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1515 Documentation: Insufficient Robustness Functional: NT due to lack of access	24, May, 2011 @ 1244 Documentation: Insufficient Robustness Functional: Voting system does not log the enabling and disabling of services	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
						This requirement should be split out to more explicitly address either voting system applications or the underlying operating system	5.6.3.3.p3 - Starting and stopping processes.			14, May, 2011 @ 1331 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1331 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1515 Documentation: Insufficient Robustness Functional: NT due to lack of access	24, May, 2011 @ 1248 Documentation: Insufficient Robustness Functional: See Req 5.6.3.3.p2 Voting system does not log the Starting and stopping processes.	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
	Abnormal process exits					Agree with Requirement	5.6.3.3.q - Abnormal process exits All abnormal process exits.			14, May, 2011 @ 1332 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1332 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1515 Documentation: Insufficient Robustness Functional: NT due to lack of access	24, May, 2011 @ 1249 Documentation: Insufficient Robustness Functional: Documentation: Insufficient Robustness Functional: See Req 5.6.3.3.p2 Voting system does not log the Abnormal process	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
	Successful and failed database connection attempts (if a database is utilized)					Agree with Requirement	5.6.3.3.r - Successful and failed database connection attempts (if a database is utilized). All database connection attempts.			14, May, 2011 @ 1340 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1340 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1515 Documentation: Insufficient Robustness Functional: NT due to lack of access	24, May, 2011 @ 1250 Documentation: Insufficient Robustness Functional: NT Lack of information on the database	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
	Changes to cryptographic keys					Recommend adding "key zeroization"	5.6.3.3.s - Changes to cryptographic keys At a minimum critical cryptographic settings include key addition, key removal, and re-keying.			14, May, 2011 @ 1341 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Insufficient Robustness Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete this section	14, May, 2011 @ 1341 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1515 Documentation: Insufficient Robustness Functional: NT due to lack of access	24, May, 2011 @ 1253 Documentation: Insufficient Robustness Functional: NT: Lack of procedures	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Manufacturer 3	Manufacturer 4	Manufacturer 5	Manufacturer 6	Manufacturer 7	Can be met today?	Need Modification	Delete
	Voting events					Recommend including successful delivery of appropriate ballot style to voter Agree with Requirement	5.6.3.3.t1 - Voting events Includes: Opening and closing the voting period.			14, May, 2011 @ 1345 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Pass Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete	14, May, 2011 @ 1345 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1515 Documentation: Insufficient Robustness Functional: NT due to lack of access	24, May, 2011 @ 1300 Documentation: Not Applicable Inspection: Not Applicable System is a ballot delivery system	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
						Agree with Requirement	5.6.3.3.t2 - Casting a vote.			14, May, 2011 @ 1350 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Pass Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete	14, May, 2011 @ 1350 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1515 Documentation: Insufficient Robustness Functional: NT due to lack of access	24, May, 2011 @ 1300 Documentation: Not Applicable Inspection: Not Applicable System is a ballot delivery system	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
						Agree with Requirement	5.6.3.3.t3 - Success or failure of log and election results exportation.			14, May, 2011 @ 1355 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	Documentation: Pass Functional: NT Without access the requirements in this section cannot be adequately assessed. Due to problems with the setup of the Manufacturer system SLI was unable to complete	14, May, 2011 @ 1355 Documentation: Insufficient Robustness Functional: NT Due to lack of access, lack of credentials given	15, June, 2011 @ 1515 Documentation: Insufficient Robustness Functional: NT due to lack of access	24, May, 2011 @ 1300 Documentation: Not Applicable Inspection: Not Applicable System is a ballot delivery system	15, June, 2011 @ 0925 Documentation: Insufficient Robustness Functional: NT due to lack of access	Documentation: Insufficient Robustness Functional: NT - due to lack of access	1		
							Section totals										66	4	
	5.7 Incident Response									Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			
	5.7.1 Incident Response Support		x							Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			
	5.7.1.1 Critical events		x		x	1) Recommend that NIST/FVAP list minimum criteria of what should be classified as critical, in order to create a consistency for this requirement 2) Recommend removal of "e.g." and giving specific criteria that must be met, as in 1) above	Manufacturers SHALL document what types of system operations or security events (e.g., failure of critical component, detection of malicious code, unauthorized access to restricted data) are classified as critical.			6, May, 2011 @ 0900 Documentation: Insufficient Robustness Functional: NA While the 'System Security Specifications' document had a section entitled 'Critical Components of the Security', there was no comprehensive list identifying what types of system operations or security events are classified as critical. Insufficient Robustness	1, June, 2011 @ 1201 Documentation: Pass Manufacturer's 'ODBP plan.pdf' document details security controls (including physical, logical, and procedural measures) that will be implemented during the election process as the ODBP voting system is deployed in four environments: Kiosk sites, data centers, election office, and communication channels. Examples of security controls detailed by Manufacturer include: a. Physical: voting stations, peripherals, and connections will be protected by tamper evident seals b. Procedural: Voting station access is controlled by the kiosk	6, May, 2011 @ 0900 Documentation: Insufficient Robustness Functional: NA While the 'System Security Specifications' document had a section entitled 'Critical Components of the Security', there was no comprehensive list identifying what types of system operations or security events are classified as critical. Insufficient Robustness	4, May, 2011 @ 1330 Documentation: Insufficient Robustness There was no documentation provided related to critical events.	10, May, 2011 @ 0955 Documentation: Insufficient Robustness	9, May, 2011 @ 1315 Documentation: Insufficient Robustness Tested: Insufficient Robustness There was no documentation provided related to critical events.	11, May, 2011 @ 0935 Documentation: Insufficient Robustness Functional: NT - lack of information.	1		
	5.7.1.2 Critical event alarm		x	x		Agree with Requirement	An alarm that notifies appropriate personnel SHALL be generated on the vote capture device, system server, or tabulation device, depending upon which device has the error, if a critical event is detected.			6, May, 2011 @ 0900 Documentation: Insufficient Robustness Functional: Insufficient Robustness No alarm could be triggered during functional test.	1, June, 2011 @ 1201 Documentation: Pass Functional: Insufficient Robustness Manufacturer's 'ODBP plan.pdf' document details alarms which are implemented to guarantee access from the kiosk sites to the VRDB and voting servers. 'Network monitoring: The network traffic will be continuously monitored to detect any suspicious behavior. Alarms will be activated in case any of these practices are detected'. During functional testing, SLI disconnected the touchscreen from the voting laptop. The touchscreen monitor displayed the message: 'no video input. Please	6, May, 2011 @ 0900 Documentation: Insufficient Robustness Functional: Insufficient Robustness No alarm could be triggered during functional test.	4, May, 2011 @ 1340 6, May, 2011 @0730 Documentation: Insufficient Robustness Functional: No alarm could be triggered during functional test.	10, May, 2011 @ 0955 Documentation: Insufficient Robustness Functional: No alarm could be triggered during functional test.	9, May, 2011 @ 1315 Documentation: Insufficient Robustness Functional: NT - Server due to lack of access. VCD: fail, no alarm	11, May, 2011 @ 0955 Documentation: Insufficient Robustness Functional: NT - lack of information	1		
							Section totals										2		
	5.8 Physical and Environmental Security		x			Recommend that additional specificity is added to explicitly call ouu whether each requirement is for the voting system (election creation machines and accumulation/tallying central servers included), or just the vote					Header is not an actionable item, it is met when all sub-requirements are met									

GAP Analysis Matrix	Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Manufacturer 3	Manufacturer 4	Manufacturer 5	Manufacturer 6	Manufacturer 7	Can be met today?	Need Modification	Delete
5.8.1 Physical Access		x								Header is not an actionable item, it is met when all sub-requirements are met								
5.8.1.1 Unauthorized physical access requirement		x		x	Agree with Requirement	Any unauthorized physical access SHALL leave physical evidence that an unauthorized event has taken place.			6, May, 2011 @ 0925 Documentation: Insufficient Robustness Functional: Insufficient Robustness While the 'System Security Specifications' document had a section entitled 'Critical Components of the Security', there was no comprehensive list identifying critical central server components nor the means by which unauthorized physical access could be recognized. Insufficient Robustness	31, May, 2011 @ 1405 1, June, 2011 @ 1245 Documentation: Pass Functional: Pass 'Procedures and System Description for Secure Remote Electronic Transmission of Ballots for Overseas Civilian and Military Voters'), Pages 22 - 27 detail physical, logical, and procedural measures to protect the central servers and the networking components. Specifically, one physical measure taken is labeled 'Surveillance: The data center will include video surveillance systems and the access to server rooms will be controlled with access cards and keypads'. Additionally, the document details	6, May, 2011 @ 0925 Documentation: Insufficient Robustness Functional: Insufficient Robustness While the 'System Security Specifications' document had a section entitled 'Critical Components of the Security', there was no comprehensive list identifying critical central server components nor the means by which unauthorized physical access could be recognized. Insufficient Robustness	4, May, 2011 @ 1400 Documentation: Insufficient Robustness Functional: Manufacturer provided no documentation related to physical security and the recognition of unauthorized events.	10, May, 2011 @ 1015 Documentation: Insufficient Robustness Functional: NT	9, May, 2011 @ 1430 Documentation: Insufficient Robustness Functional: NT due to lack of access.	11, May, 2011 @ 1200 Documentation: Insufficient Robustness Functional: NT due to lack of access.	1		
5.8.2 Physical Ports and Access Points		x				Contained (or referenced) in test plans			Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			
5.8.2.1 Non-essential ports		x		x	Recommend that "testing" be removed. In a production environment, would not want "test" ports/access points enabled.	The voting system SHALL disable physical ports and access points that are not essential to voting operations, testing, and auditing.			6, May, 2011 @ 1020 Documentation: Insufficient Robustness Functional: Insufficient Robustness While the 'System Security Specifications' document had a section entitled 'Critical Components of the Security', there was no mention of disabling non-essential physical ports or access points. During functional testing, SLI plugged a flash drive into an unused port and the device was accessible. Insufficient Robustness	31, May, 2011 @ 1405 1, June, 2011 @ 1245 Documentation: Insufficient Robustness Functional:Pass SLI could not locate any documentation which recommended the disabling of physical ports and access points on the voting central servers which are not essential to voting operations, testing, or auditing. During functional testing, SLI plugged a flash drive into an available port on the bridge server and the device was active. Insufficient Robustness Regarding the VCD, Manufacturer documentation states:	6, May, 2011 @ 1020 Documentation: Insufficient Robustness Functional: Insufficient Robustness While the 'System Security Specifications' document had a section entitled 'Critical Components of the Security', there was no mention of disabling non-essential physical ports or access points. During functional testing, SLI plugged a flash drive into an unused port and the device was accessible. Insufficient Robustness	4, May, 2011 @ 1400 Documentation: Insufficient Robustness Functional: Manufacturer's documentation did not address the disabling of non-essential ports.	10, May, 2011 @ 1025 Documentation: Insufficient Robustness Functional: USB inserted and recognized. NT: Kiosk due to no information received about a kiosk.	9, May, 2011 @ 1430 Documentation: Insufficient Robustness Functional: NT - due to lack of access.	11, May, 2011 @ 0935 Documentation: Insufficient Robustness Functional: NT due to lack of access.	1		
5.8.3 Physical Port Protection		x							Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			
5.8.3.1 Physical port shutdown requirement		x		x	Recommend changing Test Method to Functional	If a physical connection between the vote capture device and a component is broken, the affected vote capture device port SHALL be automatically disabled			6, May, 2011 @ 1345 Documentation: Insufficient Robustness Functional: Insufficient Robustness Manufacturer' VCD lacks any additional hardware components. It's voting internet site is accessible via a non-secure PC equipped with a display monitor and a keyboard but with no 'smart' voting components (such as a touch monitor or smartcard reader).	31, May, 2011 @ 1405 1, June, 2011 @ 1340 Documentation: Pass Functional: Insufficient Robustness Manufacturer's Vote Capture device includes a touch screen monitor, a smartcard reader, a printer, and a voting server. While section 11.1.1, 'Ballot Casting Process', states that 'any attempt to modify the Voting Laptops must be detected and reported,' there is no documentation to indicate that a the disconnection of a component from the VCD would cause its port to become disabled.	6, May, 2011 @ 1345 Documentation: Insufficient Robustness Functional: Insufficient Robustness Manufacturer' VCD lacks any additional hardware components. It's voting internet site is accessible via a non-secure PC equipped with a display monitor and a keyboard but with no 'smart' voting components (such as a touch monitor or smartcard reader).	6, May, 2011 @ 0800 Documentation: Not Applicable Functional: Not Applicable	10, May, 2011 @ 0955 Documentation: Not Applicable Functional: Not Applicable	9, May, 2011 @ 1035 Documentation: NA Functional: NA	11, May, 2011 @ 1230 Documentation: Insufficient Robustness Functional: NT due to lack of access.	1		

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Manufacturer 3	Manufacturer 4	Manufacturer 5	Manufacturer 6	Manufacturer 7	Can be met today?	Need Modification	Delete
	5.8.3.2 Physical component alarm requirement		x		x	Recommend changing Test Method to Functional	The voting system SHALL produce a visual alarm if a connected component is physically disconnected.			6, May, 2011 @ 1345 Documentation: Insufficient Robustness Functional: Insufficient Robustness Manufacturer's VCD does not have any components (no smartcard reader, no touchscreen monitor). The voting application is accessed from a computer with an internet browser. SLI considers the computer, its mouse, and its display monitor to be one component.	2, June, 2011 @ 0708 Documentation: Pass Functional: Insufficient Robustness Tested in conjunction with 5.8.3.1.	6, May, 2011 @ 1345 Documentation: Insufficient Robustness Functional: Insufficient Robustness Manufacturer's VCD does not have any components (no smartcard reader, no touchscreen monitor). The voting application is accessed from a computer with an internet browser. SLI considers the computer, its mouse, and its display monitor to be one component.	6, May, 2011 @ 0800 Not Testable: SLI did not have access to Vendor's central voting server.	10, May, 2011 @ 1045 Documentation: Insufficient Robustness Functional: No visual alarm was produced upon disconnecting the network cable from the central server. NA - Kiosk	9, May, 2011 @ 1430 Documentation: Insufficient Robustness Functional: NT - due to lack of access.	11, May, 2011 @ 1230 Not Testable. SLI did not have access to the Manufacturer central server.	1		
	5.8.3.3 Physical component event log requirement		x		x	Agree with Requirement				6, May, 2011 @ 1345 Documentation: Insufficient Robustness Functional: Insufficient Robustness While the 'System Security Specifications' document had a section entitled 'Critical Components of the Security', the document did not identify an event log nor any event that would cause an entry to be written to an event log.	31, May, 2011 @ 1405 1, June, 2011 @ 0708 Documentation: Pass Functional: Insufficient Robustness Per Section 8.2 of the Pnyx.core User Manual, 'The Log Viewer Application', 'all the services log their operations during the election process. These logs are stored in separate (each service has its own tables) database tables managed by the service. However, these logs pertain to functional voting processes, and not to physical security events on vote capture device hardware. Insufficient Robustness	6, May, 2011 @ 1345 Documentation: Insufficient Robustness Functional: Insufficient Robustness While the 'System Security Specifications' document had a section entitled 'Critical Components of the Security', the document did not identify an event log nor any event that would cause an entry to be written to an event log.	6, May, 2011 @ 0800 Documentation: Not Applicable Functional: Not Applicable	10, May, 2011 @ 1055 Documentation: Insufficient Robustness Functional: NT Manufacturer's documentation did not include any information related to event logging.	9, May, 2011 @ 1430 Documentation: NA Functional: NA	11, May, 2011 @ 1230 Documentation: Insufficient Robustness Functional: NT due to lack of access.	1		
	5.8.3.4					Recommend changing Test Method to Functional				6, May, 2011 @ 1345 Documentation: Pass Functional: Pass A disabled port could only be re-enabled by an authorized administrator.	1, June, 2011 @ 0708 Documentation: Pass Functional: Pass Tested in conjunction with 5.8.3.7.	6, May, 2011 @ 1345 Documentation: Pass Functional: Pass A disabled port could only be re-enabled by an authorized administrator.	6, May, 2011 @ 0800 Documentation: Insufficient Robustness Functional: NT - Vendor did not supply hardware for SLI testing.	10, May, 2011 @ 1100 11, May, 2011 @0815 Documentation: Insufficient Robustness Functional: Pass	9, May, 2011 @ 1430 Documentation: Insufficient Robustness Functional: NT due to lack of access.	11, May, 2011 @ 1300 Documentation: Insufficient Robustness Functional: NT due to lack of access.	1		
	5.8.3.5					If Implementing with custom designed vote capture device this requirement is applicable. If implementing with COTS products, this would not be applicable.				9, May, 2011 @ 0725 Documentation: Insufficient Robustness Functional: Insufficient Robustness Manufacturer's documentation did not provide guidelines for restricting physical access to ports supporting removable media which are not essential to the voting session.	1, June, 2011 @ 0708 Documentation: Pass Functional: Pass Manufacturer's documentation recommends that the VCD and its components be set up with tamper-proof seals. Pass.	9, May, 2011 @ 0725 Documentation: Insufficient Robustness Functional: Insufficient Robustness Manufacturer's documentation did not provide guidelines for restricting physical access to ports supporting removable media which are not essential to the voting session.	6, May, 2011 @ 0800 Documentation: Insufficient Robustness Functional: NT - Vendor did not supply hardware for SLI testing.	10, May, 2011 @ 1400 Documentation: Insufficient Robustness Functional: SLI inspection of the VCD revealed that unused ports on the VCD did not have their access restricted by doors, locks, seals, or panels. Insufficient Robustness	10, May, 2011 @ 0720 Documentation: Insufficient Robustness Functional: NT due to lack of access.	11, May, 2011 @ 1300 Documentation: Insufficient Robustness Functional: NT due to lack of access. SLI accessed the voting system via a SLI computer with a web browser. The VCD ports were accessible and there were no covers, doors, locks, seals, or panels.	1		
	5.8.3.6					If implementing with custom designed vote capture device this requirement is applicable. If implementing with COTS products, this would not be applicable.				9, May, 2011 @ 0725 Documentation: Insufficient Robustness Functional: Insufficient Robustness Manufacturer's provided documentation did not provide guidelines related to the recognition of physical tampering or unauthorized access to ports and all other access points.	1, June, 2011 @ 0708 Documentation: Pass Functional: Pass When setting up the voting laptop, Manufacturer recommends checking the voting laptop to verify that all seals are in place and that they are neither broken or manipulated. Pass.	9, May, 2011 @ 0725 Documentation: Insufficient Robustness Functional: Insufficient Robustness Manufacturer's provided documentation did not provide guidelines related to the recognition of physical tampering or unauthorized access to ports and all other access points.	6, May, 2011 @ 0800 Documentation: Insufficient Robustness Functional: NT - Vendor did not supply hardware for SLI testing.	10, May, 2011 @ 1420 Documentation: Insufficient Robustness Functional: NT - due to lack of Kiosk.	10, May, 2011 @ 0720 Documentation: Insufficient Robustness Functional: NT due to lack of access.	11, May, 2011 @ 1300 Documentation: Insufficient Robustness Functional: NT due to lack of access. SLI was unable to locate any reference to physical tampering on VCDs.	1		

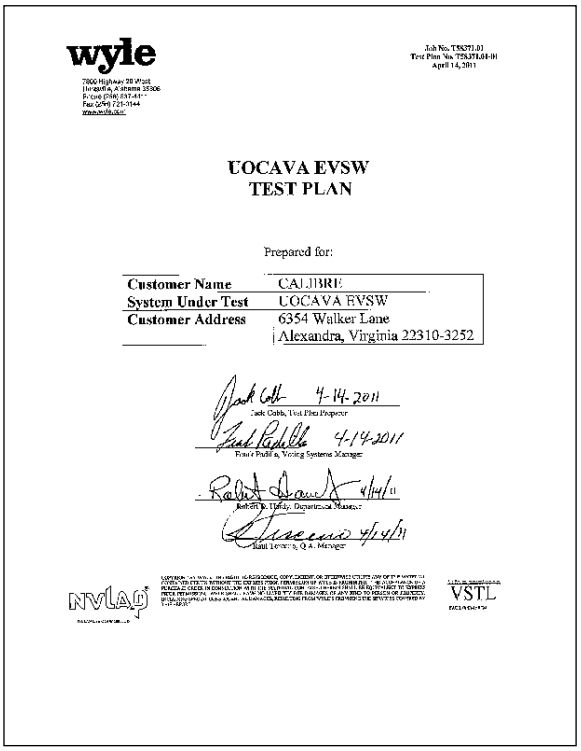
GAP Analysis Matrix	Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Manufacturer 3	Manufacturer 4	Manufacturer 5	Manufacturer 6	Manufacturer 7	Can be met today?	Need Modification	Delete
5.8.3.7					If implementing with custom designed vote capture device this requirement is applicable. If implementing with COTS products, this would not be applicable.				9, May, 2011 @ 0725 Documentation: Insufficient Robustness Functional: Insufficient Robustness Manufacturer's documentation did not include any guidelines as to the physical disabling of ports.	1, June, 2011 @ 0708 Documentation: Pass Functional: Pass VCD is designed such that physical ports can be manually disabled by an authorized administrator. Pass.	9, May, 2011 @ 0725 Documentation: Insufficient Robustness Functional: Insufficient Robustness Manufacturer's documentation did not include any guidelines as to the physical disabling of ports.	6, May, 2011 @ 0800 Documentation: Insufficient Robustness Functional: NT - Vendor did not supply hardware for SLI testing.	10, May, 2011 @ 1430 Documentation: Insufficient Robustness Functional: Pass	10, May, 2011 @ 0720 Documentation: Insufficient Robustness Functional: NT due to lack of access.	11, May, 2011 @ 1300 Documentation: Insufficient Robustness Functional: Pass VCDs are designed such that physical ports can be manually disabled by an authorized administrator. Manufacturer did not supply Kiosk hardware. SLI accessed the voting system on an SLI computer via a web browser.	1		
5.8.4 Door Cover and Panel Security		x		x	Enumerate the activities				9, May, 2011 @ 0725 Documentation: Insufficient Robustness Functional: Insufficient Robustness SLI set up the manufacturer voting system per the documentation provided by manufacturer, which did not detail the use of tamper evident or tamper resistant countermeasures. There were no locks or seals on the voting system hardware.	1, June, 2011 @ 0708 Documentation: Pass Functional: Pass manufacturer's documentation recommended tamper-proof seals. Pass.	9, May, 2011 @ 0725 Documentation: Insufficient Robustness Functional: Insufficient Robustness SLI set up the manufacturer voting system per the documentation provided by manufacturer, which did not detail the use of tamper evident or tamper resistant countermeasures. There were no locks or seals on the voting system hardware.	6, May, 2011 @ 0800 Documentation: Insufficient Robustness Functional: NT - Vendor did not supply hardware for SLI testing.	10, May, 2011 @ 1432 Documentation: Insufficient Robustness Functional: NT	10, May, 2011 @ 0720 Documentation: Insufficient Robustness Functional: NT due to lack of access.	11, May, 2011 @ 1300 Documentation: Insufficient Robustness Functional: NT due to lack of access. manufacturer did not supply Kiosk hardware, nor did it recommend the use of covers and panels for Kiosk hardware.	1		
5.8.5 Secure Paper Record Receptacle		x		x	Agree with Requirement				9, May, 2011 @ 0725 Documentation: NA Functional: NA Not Applicable. Manufacturer did not provide paper record containers.	Documentation: Pass Functional: NT While Manufacturer's documentation includes a 'secure receptacle monitored by the Kiosk Official' ('ODBP Voting Laptop 1.0 Voter's Manual, Version 1.0), no receptacle was included with SLI's documentation. Not Testable.	9, May, 2011 @ 0725 Documentation: NA Functional: NA Not Applicable. Manufacturer did not provide paper record containers.	6, May, 2011 @ 0800 Documentation: Insufficient Robustness Functional: NT - Vendor did not supply hardware for SLI testing.	10, May, 2011 @ 1440 Documentation: Insufficient Robustness Functional: NT No paper record container was provided.	10, May, 2011 @ 0720 Documentation: Insufficient Robustness Functional: NT due to lack of access.	11, May, 2011 @ 1300 Not Applicable Manufacturer did not supply a paper record container.	1		
5.8.6.1		x		x	If implementing with custom designed vote capture device this requirement is applicable. If implementing with COTS products, this would not be applicable.				9, May, 2011 @ 0725 Documentation: Insufficient Robustness Functional: Insufficient Robustness SLI implemented the Manufacturer voting system per Manufacturer's provided documentation which did not address countermeasures for physical tampering.	1, June, 2011 @ 0708 Documentation: Pass Functional: NT While Manufacturer's documentation recommended the use of tamper-proof seals, SLI did not implement tamper-proof seals for testing purposes.	9, May, 2011 @ 0725 Documentation: Insufficient Robustness Functional: Insufficient Robustness SLI implemented the Manufacturer voting system per Manufacturer's provided documentation which did not address countermeasures for physical tampering.	6, May, 2011 @ 0800 Documentation: Insufficient Robustness Functional: NT - Vendor did not supply hardware for SLI testing. SLI did not have access to Manufacturer's central server.	10, May, 2011 @ 1445 Documentation: Insufficient Robustness Functional: NT No information on physical locks.	10, May, 2011 @ 0800 Documentation: Insufficient Robustness Functional: NT due to lack of access.	11, May, 2011 @ 1300 Not Applicable. Manufacturer did not supply a paper record container.	1		
5.8.6.2					Agree with Requirement				9, May, 2011 @ 0725 Documentation: Insufficient Robustness Functional: Insufficient Robustness SLI implemented the Manufacturer voting system per Manufacturer's provided documentation which did not address countermeasures for physical tampering. Insufficient Robustness	1, June, 2011 @ 0708 Documentation: Pass Functional: NA The Manufacturer voting system did not make use of locking systems.	9, May, 2011 @ 0725 Documentation: Insufficient Robustness Functional: Insufficient Robustness SLI implemented the Manufacturer voting system per Manufacturer's provided documentation which did not address countermeasures for physical tampering. Insufficient Robustness	6, May, 2011 @ 0800 Documentation: Insufficient Robustness Functional: NT - Vendor did not supply hardware for SLI testing.	10, May, 2011 @ 1450 Documentation: Insufficient Robustness Functional: NT - No locks implemented.	10, May, 2011 @ 0800 Documentation: Insufficient Robustness Functional: NT due to lack of access.	11, May, 2011 @ 1300 Tested: Insufficient Robustness Manufacturer did not supply Kiosk hardware nor did it recommend access locks be installed on Kiosk hardware.	1		
5.8.7 Media Protection		x		x	Recommend changing "person privacy related data" to "personally identifiable information (PII)", which is a				Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Manufacturer 3	Manufacturer 4	Manufacturer 5	Manufacturer 6	Manufacturer 7	Can be met today?	Need Modification	Delete
	5.8.7.1					Agree with Requirement				9, May, 2011 @ 0725 Documentation: Insufficient Robustness Functional: Insufficient Robustness SLI implemented the Manufacturer voting system per Manufacturer's provided documentation which did not provide guidelines for the handling of paper records. Insufficient Robustness SLI set up Manufacturer's voting system per documentation provided by Manufacturer which did not include guidelines related to physical security. Insufficient Robustness All hardware in SLI's implementation of Manufacturer's voting system had unique serial	1, June, 2011 @ 0708 Documentation: Pass Functional: NT Manufacturer's 'ODBP Project Manual for Kiosk Officials', Section 6.3, recommended that 'At the end of the day', Manufacturer's Kiosk process recommends collecting 'all papers over the room, including config sheets, incident reports, Voter Certificates, evaluation surveys, etc.' and placing 'them into the maroon bag'. The maroon bag is sealed with the serial number of the seal noted. The voting official takes the maroon bag with him to his room. Pass. Not Testable. While	9, May, 2011 @ 0725 Documentation: Insufficient Robustness Functional: Insufficient Robustness SLI implemented the Manufacturer voting system per Manufacturer's provided documentation which did not provide guidelines for the handling of paper records. Insufficient Robustness SLI set up Manufacturer's voting system per documentation provided by Manufacturer which did not include guidelines related to physical security. Insufficient Robustness All hardware in SLI's implementation of Manufacturer's voting system had unique serial numbers. Pass.	6, May, 2011 @ 0815 Documentation: Insufficient Robustness Functional: Insufficient Robustness - Vendor did not supply hardware for SLI testing.	10, May, 2011 @ 1455 Documentation: Insufficient Robustness Functional: Insufficient Robustness due to lack of informaton.	10, May, 2011 @ 0800 Documentation: Insufficient Robustness Functional:Insufficient Robustness due to lack of access.	11, May, 2011 @ 1300 Documentation: Insufficient Robustness Functional: Insufficient Robustness 5.8.7.1.a – Manufacturer did not supply Kiosk hardware nor did it recommend access locks be installed on Kiosk hardware. Insufficient Robustness 5.8.7.1.b Manufacturer did not supply Kiosk hardware nor did it recommend access locks be installed on Kiosk hardware. Insufficient Robustness 5.8.7.1.c – SLI utilized its own computer to access the Manufacturer voting system. The computer had a unique serial number. Pass.	1		
							Section totals										14		
	5.9 Penetration Resistance	x		x		Recommend referencing NIST SP dealing with hardening.				Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			
	5.9.1 Resistance to Penetration Attempts	x		x						Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			
	5.9.1.1 Resistant to attempts	x		x		Recommend defining resistant levels more definitively, and enumerating by device types within a voting system	The voting system SHALL be resistant to attempts to penetrate the system by any remote unauthorized entity.			Documentation: Pass Functional: Pass Resistance to Attempts: Only ports 80 and 443 were open and both ports resisted all known exploits (over 200) to the Apache Server using those ports.	Documentation: Pass Functional: Pass Resistant to Attempts: Only 4 machines visible to network and all machines resisted all known exploits	Documentation: Pass Functional: Pass Resistance to Attempts: Only ports 80 and 443 were open and both ports resisted all known exploits (over 200) to the Apache Server using those ports.	Not tested due to security concerns of remote penetration testing.	13, June, 2011 @ 0815 Documentation: Insufficient Robustness Functional: Pass Resistant to Attempts: Only ports 80 and 443 were open and both ports resisted all known exploits (over 200) to the Apache Server using those ports.	Documentation: Insufficient Robustness Functional: NT due to lack of access.	Documentation: Insufficient Robustness Functional: NT due to lack of access.	1		
	5.9.1.2 System information disclosure	x		x		1) Recommend defining "appropriate functionality" by device types within a voting system. 2) Recommend referencing NIST SP dealing with hardening.	The voting system SHALL be configured to minimize ports, responses and information disclosure about the system while still providing appropriate functionality			Documentation: Pass Functional: Pass System Information Disclosure: Both ports (80 and 443) responded and disclosed web server as Apache 2.2.3 and OpenSSL 0.9.8e-fips-rel5. Port (22) responded and disclosed ssh server as OpenSSH 4.3.	Documentation: Pass Functional: Pass System Information Disclosure: 1 machine port (22) responded and disclosed ssh server as version 3.6.1p2 1 machine had 5 ports (135, 139, 445, 3389, 43329) open but no additional information. 1 machine port (53) responded but did not disclose any additional information.	Documentation: Pass Functional: Pass System Information Disclosure: Both ports (80 and 443) responded and disclosed web server as Apache 2.2.3 and OpenSSL 0.9.8e-fips-rel5. Port (22) responded and disclosed ssh server as OpenSSH 4.3.	Not tested due to security concerns of remote penetration testing.	13, June, 2011 @ 0905 Documentation: Insufficient Robustness Functional: Pass System Information Disclosure: Both ports (80 and 443) responded and disclosed web server as Apache 2.2.14. Port 123 responded and disclose service ntp as NTPv4.	Documentation: Insufficient Robustness Functional: NT due to lack of access.	Documentation: Insufficient Robustness Functional: NT due to lack of access.		1	
	5.9.1.3 System access	x		x		Enumerate the activities	The voting system SHALL provide no access, information or services to unauthorized entities.			Documentation: Pass Functional: Pass System Access: All 215 exploits were unsuccessful.	Documentation: Pass Functional: Pass System Access: All 35 exploits were unsuccessful.	Documentation: Pass Functional: Pass System Access: All 215 exploits were unsuccessful.	Not tested due to security concerns of remote penetration testing.	Documentation: Insufficient Robustness Functional: Pass System Access: All 253 exploits were	Documentation: Insufficient Robustness Functional: NT due to lack of access.	Documentation: Insufficient Robustness Functional: NT due to lack of access.	1		
	5.9.1.4 Interfaces	x		x		Recommend closing all ports and shutting down all services not needed to perform voting activities	All interfaces SHALL be penetration resistant including TCP/IP, wireless, and modems from any point in the system.			Documentation: Pass Functional: Pass Interfaces: All 215 exploits were unsuccessful.	Documentation: Pass Functional: Pass Interfaces: All 35 exploits were unsuccessful.	Documentation: Pass Functional: Pass Interfaces: All 215 exploits were unsuccessful.	Not tested due to security concerns of remote penetration testing.	Documentation: Insufficient Robustness Functional: Pass Interfaces: All 253 exploits were	Documentation: Insufficient Robustness Functional: NT due to lack of access.	Documentation: Insufficient Robustness Functional: NT due to lack of access.	1		
	5.9.1.5 Documentation	x		x		Agree with Requirement	The configuration and setup to attain penetration resistance SHALL be clearly and completely documented.			Documentation: Insufficient Robustness Documentation: Machine was preconfigured by manufacturer.	Documentation: Insufficient Robustness Machine was preconfigured by manufacturer.	Documentation: Insufficient Robustness Documentation: Machine was preconfigured by manufacturer.	Documentation: Insufficient Robustness	Documentation: Insufficient Robustness Documentation: Machine was preconfigured by manufacturer.	Documentation: Insufficient Robustness	Documentation: Insufficient Robustness	1		

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Manufacturer 3	Manufacturer 4	Manufacturer 5	Manufacturer 6	Manufacturer 7	Can be met today?	Need Modification	Delete
	5.9.2 Penetration Resistance Test and Evaluation	x				This section is oriented to the VSTL. As such it should not be in the requirements document that manufacturer's are held to, but in a "Program Manual" that outlines the scope of a certification campaign.				Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			
	5.9.2.1 Scope	x				Define Test Method "Penetration" versus "Functional"	The scope of penetration testing SHALL include all the voting system components. The scope of penetration testing includes but is not limited to the following:			Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			
		x		x		Agree with Requirement	System server;			Documentation: Pass Functional: Pass Using standard network exploitation tools, all machines and ports were identified.	Documentation: Pass Functional: Pass Using standard network exploitation tools, all machines and ports were identified.	Documentation: Pass Functional: Pass Using standard network exploitation tools, all machines and ports were identified.	Not tested due to security concerns of remote penetration testing.	Documentation: Pass Functional: Pass Using standard network exploitation tools, all machines and ports were identified.	Documentation: Insufficient Robustness Functional: NT due to lack of access.	Documentation: Insufficient Robustness Functional: NT due to lack of access.	1		
		x		x		Agree with Requirement	Vote capture devices;			Documentation: Pass Functional: Pass Using standard network exploitation tools, all machines and ports were identified.	Documentation: Pass Functional: Pass Using standard network exploitation tools, all machines and ports were identified.	Documentation: Pass Functional: Pass Using standard network exploitation tools, all machines and ports were identified.	Not tested due to security concerns of remote penetration testing.	Documentation: Pass Functional: Pass Using standard network exploitation tools, all machines and ports were identified.	Documentation: Insufficient Robustness Functional: NT due to lack of access.	Documentation: Insufficient Robustness Functional: NT due to lack of access.	1		
		x		x		Agree with Requirement	Tabulation device;			Documentation: Pass Functional: Pass Using standard network exploitation tools, all machines and ports were identified.	Documentation: Pass Functional: Pass Using standard network exploitation tools, all machines and ports were identified.	Documentation: Pass Functional: Pass Using standard network exploitation tools, all machines and ports were identified.	Not tested due to security concerns of remote penetration testing.	Documentation: Pass Functional: Pass Using standard network exploitation tools, all machines and ports were identified.	Documentation: Insufficient Robustness Functional: NT due to lack of access.	Documentation: Insufficient Robustness Functional: NT due to lack of access.	1		
		x		x		Agree with Requirement	All items setup and configured per Technical Data Package (TDP) recommendations;			Documentation: Pass Functional: Pass Using standard network exploitation tools, all machines and ports were identified.	Documentation: Pass Functional: Pass Using standard network exploitation tools, all machines and ports were identified.	Documentation: Pass Functional: Pass Using standard network exploitation tools, all machines and ports were identified.	Not tested due to security concerns of remote penetration testing.	Documentation: Pass Functional: Pass Using standard network exploitation tools, all machines and ports were identified.	Documentation: Insufficient Robustness Functional: NT due to lack of access.	Documentation: Insufficient Robustness Functional: NT due to lack of access.	1		
		x		x		Agree with Requirement	Local wired and wireless networks; and			Documentation: Pass Functional: Pass Using standard network exploitation tools, all machines and ports were identified.	Documentation: Pass Functional: Pass Using standard network exploitation tools, all machines and ports were identified.	Documentation: Pass Functional: Pass Using standard network exploitation tools, all machines and ports were identified.	Not tested due to security concerns of remote penetration testing.	Documentation: Pass Functional: Pass Using standard network exploitation tools, all machines and ports were identified.	Documentation: Insufficient Robustness Functional: NT due to lack of access.	Documentation: Insufficient Robustness Functional: NT due to lack of access.	1		
		x		x		Agree with Requirement	Internet connections.			Documentation: Pass Functional: Pass	Documentation: Pass Functional: Pass	Documentation: Pass Functional: Pass	Not tested due to security concerns of remote penetration testing.	Documentation: Pass Functional: Pass Using standard network exploitation tools, all machines and ports were identified.	Documentation: Insufficient Robustness Functional: NT due to lack of access.	Documentation: Insufficient Robustness Functional: NT due to lack of access.	1		
	5.9.2.2 Test environment	x		x		1) This requirement appears to be oriented to the VSTL, not the manufacturer. 2) This may not be feasible for all systems. Have encountered systems that are cloud base, for example.	Penetration testing SHALL be conducted on a voting system set up in a controlled lab environment. Setup and configuration SHALL be conducted in accordance with the TDP, and SHALL replicate the real world environment in which the voting system will be used.			Documentation: NA Functional: NA Test Environment: Machines were installed on internal VSTL network.	Documentation: NA Functional: NA Test Environment: Machines were installed on internal VSTL network.	Documentation: NA Functional: NA Test Environment: Machines were installed on internal VSTL network.	Not tested due to security concerns of remote penetration testing.	Documentation: Insufficient Robustness Test Environment: Machine was installed on internal VSTL network.	Documentation: Insufficient Robustness Functional: NT due to lack of access.	Documentation: Insufficient Robustness Functional: NT due to lack of access.			1
	5.9.2.3 White box testing	x		x		1) This requirement appears to be oriented to the VSTL, not the manufacturer. 2) The original text is not a definition of white box testing. 3) With added text, the source code review that would be required would be prohibitive from a cost/benefit viewpoint.	The penetration testing team SHALL conduct white box testing using manufacturer supplied documentation and voting system architecture information. Documentation includes the TDP and user documentation. The testing team SHALL have access to any relevant information regarding the voting system configuration. This includes, but is not limited to, network layout and Internet Protocol addresses for system devices and components. The testing team SHALL be provided any source code included in the TDP.			Documentation: NA Functional: NA White Box Testing: Vendor documentation was reviewed but no source code provided.	Documentation: NA Functional: NA White Box Testing: Vendor documentation was reviewed but no source code provided.	Documentation: NA Functional: NA White Box Testing: Vendor documentation was reviewed but no source code provided.	Vendor documentation was reviewed but no source code provided.	Documentation: Insufficient Robustness Functional: NT White Box Testing: Vendor documentation was reviewed but no source code provided.	Documentation: Insufficient Robustness Functional: NT due to lack of access.	Documentation: Insufficient Robustness Functional: NT due to lack of access.			1
	5.9.2.4 Focus and priorities	x				1) This requirement appears to be oriented to the VSTL, not the manufacturer.	Penetration testing seeks out vulnerabilities in the voting system that might be used to change the outcome of an election, interfere with voter ability to cast ballots, ballot counting, or compromise ballot secrecy. The penetration testing team SHALL prioritize testing efforts based on the following:			Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met	Header is not an actionable item, it is met when all sub-requirements are met			1
		x		x	x		a. Threat scenarios for the voting system under investigation;			Documentation: NA Functional: Pass Using standard network exploitation tools, all machines and ports were identified. 215 exploits were attempted with no success.	Documentation: NA Functional: Pass Using standard network exploitation tools, all machines and ports were identified. 35 exploits were attempted with no success.	Documentation: NA Functional: Pass Using standard network exploitation tools, all machines and ports were identified. 215 exploits were attempted with no success.	Not tested due to security concerns of remote penetration testing.	Documentation: NA Functional: Pass Focus and Priorities: Using standard network exploitation tools, all machines and ports were identified. 253 exploits were attempted with no success.	Documentation: Insufficient Robustness Functional: NT due to lack of access.	Documentation: Insufficient Robustness Functional: NT due to lack of access.			1

GAP Analysis Matrix		Planned SLI Functional	Planned SLI Inspection	SLI Functional	SLI Inspection	SLI Comments	Reference/Documentation	VVSG para.	VVSG 2005 Reference	Manufacturer 1	Manufacturer 2	Manufacturer 3	Manufacturer 4	Manufacturer 5	Manufacturer 6	Manufacturer 7	Can be met today?	Need Modification	Delete
		x		x	x		b. Remote attacks SHALL be prioritized over in-person attacks;			Documentation: NA Functional: Pass Focus and Priorities: Using standard network exploitation tools, all machines and ports were identified. 215 exploits were attempted with no success.	Documentation: NA Functional: Pass Using standard network exploitation tools, all machines and ports were identified. 35 exploits were attempted with no success.	Documentation: NA Functional: Pass Focus and Priorities: Using standard network exploitation tools, all machines and ports were identified. 215 exploits were attempted with no success.	Not tested due to security concerns of remote penetration testing.	Documentation: NA Functional: Pass Focus and Priorities: Using standard network exploitation tools, all machines and ports were identified. 253 exploits were attempted with no success.	Documentation: Insufficient Robustness Functional: NT due to lack of access.	Documentation: Insufficient Robustness Functional: NT due to lack of access.			1
		x		x	x		c. Attacks with a large impact SHALL be prioritized over attacks with a more narrow impact; and			Documentation: NA Functional: PassFocus and Priorities: Using standard network exploitation tools, all machines and ports were identified. 215 exploits were attempted with no success.	Documentation: NA Functional: Pass Using standard network exploitation tools, all machines and ports were identified. 35 exploits were attempted with no success.	Documentation: NA Functional: PassFocus and Priorities: Using standard network exploitation tools, all machines and ports were identified. 215 exploits were attempted with no success.	Not tested due to security concerns of remote penetration testing.	Documentation: NA Functional: Pass Focus and Priorities: Using standard network exploitation tools, all machines and ports were identified. 253 exploits were attempted with no success.	Documentation: Insufficient Robustness Functional: NT due to lack of access.	Documentation: Insufficient Robustness Functional: NT due to lack of access.			1
		x		x	x		d. Attacks that can change the outcome of an election SHALL be prioritized over attacks that compromise ballot secrecy or cause non-selective denial of service.			Documentation: NA Functional: Pass Focus and Priorities: Using standard network exploitation tools, all machines and ports were identified. 215 exploits were attempted with no success.	Documentation: NA Functional: Pass Using standard network exploitation tools, all machines and ports were identified. 35 exploits were attempted with no success.	Documentation: NA Functional: Pass Focus and Priorities: Using standard network exploitation tools, all machines and ports were identified. 215 exploits were attempted with no success.	Not tested due to security concerns of remote penetration testing.	Documentation: NA Functional: Pass Focus and Priorities: Using standard network exploitation tools, all machines and ports were identified. 253 exploits were attempted with no success.	Documentation: Insufficient Robustness Functional: NT due to lack of access.	Documentation: Insufficient Robustness Functional: NT due to lack of access.			1

Appendix F – Wyle Laboratories Test Plan and Test Report



wyle

7800 Highway 20 West
Huntsville, Alabama 35806
Phone (256) 837-4411
Fax (256) 721-0144
www.wyle.com

Job No. T58371.01
Test Plan No. T58371.01-01
April 14, 2011

UOCAVA EVSW
TEST PLAN

Prepared for:

Customer Name	CALIBRE
System Under Test	UOCAVA EVSW
Customer Address	6354 Walker Lane Alexandra, Virginia 22310-3252

Jack Cobb, Test Plan Preparer — 4-14-2011

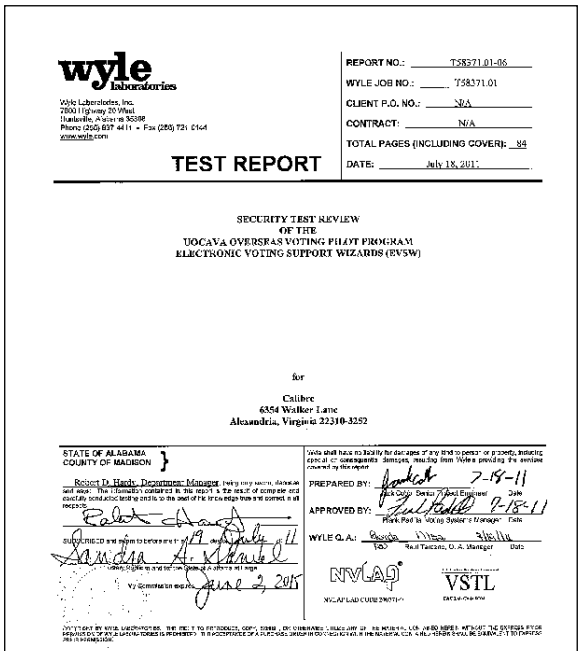
Frank Padilla, Voting Systems Manager — 4-14-2011

Robert D. Hardy, Department Manager — 4/14/11

Saul Terrazas, Q.A. Manager — 4/14/11

NVLAP

VSTL



wyle laboratories

Wyle Laboratories, Inc.
7800 Highway 20 West
Huntsville, Alabama 35806
Phone (256) 837-4411 • Fax (256) 721-0144
www.wyle.com

TEST REPORT

REPORT NO.: T58371.01-05
WYLE JOB NO.: T58371.01
CLIENT P.O. NO.: N/A
CONTRACT: N/A
TOTAL PAGES (INCLUDING COVER): 84
DATE: July 18, 2011

SECURITY TEST REVIEW
OF THE
UOCAVA OVERSEAS VOTING PILOT PROGRAM
ELECTRONIC VOTING SUPPORT WIZARDS (EVSW)

for

Calibre
6354 Walker Lane
Alexandria, Virginia 22310-3252

STATE OF ALABAMA
COUNTY OF MADISON

Robert D. Hardy, Department Manager, being duly sworn, deposes and says: The information contained in this report is the result of complete and exactly conducted testing and to the best of his knowledge and belief is correct in all respects.

SUBSCRIBED and sworn to before me this 19 day of July, 11

Notary Public in and for the State of Alabama at Large

My Commission expires June 2, 2015

Wyle shall have no liability for damages of any kind to person or property, including special or consequential damages, resulting from Wyle's providing the services covered by this report.

PREPARED BY: Jack Cobb, Senior Test Level Engineer — 7-18-11 Date

APPROVED BY: Frank Padilla, Voting Systems Manager — 7-18-11 Date

WYLE Q.A.: Saul Terrazas, Q.A. Manager — 7/18/11 Date

NVLAP
NVLAP LAB CODE 200676-0

VSTL

wyle

7800 Highway 20 West
Huntsville, Alabama 35806
Phone (256) 837-4411
Fax (256) 721-0144
www.wyle.com

Job No. T58371.01
Test Plan No. T58371.01-01
April 14, 2011

UOCAVA EVSW
TEST PLAN

Prepared for:

Customer Name	CALIBRE
System Under Test	UOCAVA EVSW
Customer Address	6354 Walker Lane Alexandra, Virginia 22310-3252

Jack Cobb 4-14-2011
Jack Cobb, Test Plan Preparer

Frank Padilla 4-14-2011
Frank Padilla, Voting Systems Manager

Robert D. Hardy 4/14/11
Robert D. Hardy, Department Manager

Raul Terceno 4/14/11
Raul Terceno, Q.A. Manager

NVLAP LAB CODE 200771-0

U.S. Election Assistance Commission
VSTL
EAC Lab Code 0704

Revisions

REVISION Original

wyle laboratories

REPORT NO. Test Plan

DATE April 14, 2011

REV	DATE	PAGE OR PARAGRAPH AFFECTED	DESCRIPTION OF CHANGES
---	4-14-11	Entire Document	Original Release

TABLE OF CONTENTS

APPENDICES

1.0 INTRODUCTION

The purpose of this Test Plan is to document the procedures that Wyle will follow to perform testing of the Electronic Voting Support Wizards (EVSW) and the [redacted], to the security requirements set forth in Section 5 "Security" of the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements.

At test conclusion, the results of all testing performed as part of this test program will be submitted to the Federal Voter Assistance Program in the form of a final report.

1.1 References

The documents listed below were used in the development of the Test Plan and will be utilized to perform certification testing.

- Uniform and Overseas Citizens Absentee Voting Act Pilot Program Testing Requirements, August 25, 2010
- NIST 800-63 Electronic Authentication Guideline Standards
- Wyle Laboratories' Quality Assurance Program Manual, Revision 5
- ISO 10012-1, "Quality Assurance Requirements for Measuring Equipment"
- NIST SP800-57
- FIPS 140-2

A listing of the Technical Package Documents (TDP) submitted for this test effort is listed in Section 2.0 Deliverable Materials.

1.2 Terms and Abbreviations

Table 1-1 defines all terms and abbreviations applicable to the development of this Test Plan.

Table 1-1 Terms and Abbreviations

Term	Abbreviation	Definition
Commercial Off the Shelf	COTS	---
[redacted]	[redacted]	---
Election Management System	EMS	---
Equipment Under Test	EUT	---
Electronic Voting Support Wizards	EVSW	---
Federal Voter Assistance Program	FVAP	Government organization that provides U.S. citizens worldwide a broad range of non-partisan information and assistance to facilitate their participation in the democratic process.

1.0 INTRODUCTION (CONTINUED)

1.2 Terms and Abbreviations (continued)

Table 1-1 Terms and Abbreviations (continued)

Term	Abbreviation	Definition
Help America Vote Act	HAVA	Act created by United States Congress in 2002.
National Institute of Standards and Technology	NIST	Government organization created to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhances economic security and improves our quality of life.
Specimen Under Test	SUT	---
Technical Data Package	TDP	Manufacturer documentation related to the voting system required to be submitted as a precondition of certification testing.
Uniformed and Overseas Citizens Absentee Voting Act	UOCAVA	U.S. federal law dealing with elections and voting rights for the U.S. citizens residing overseas.
Voting System Test Laboratory	VSTL	EAC accredited third party test laboratory.
Wyle Operating Procedure	WoP	Wyle Test Method or Test Procedure

1.3 Testing Responsibilities

Wyle, an accredited VSTL, will test the EVSW and [redacted] as specified in this Test Plan. The testing will verify that the submitted systems conform to Section 5 of the UOCAVA Pilot Program Testing Requirements.

All testing will be conducted under the guidance of Wyle, by personnel verified by Wyle to be qualified to perform the testing.

1.3.1 Project Schedule

The following table provides the contractual dates agreement between FVAP and Wyle:

Deliverable	Time	Date
Start Date	---	March 21, 2011
Test Plan, Test Cases and Test Matrix Delivery	20 Days	April 18, 2011
Test Case Execution	30 Days	May 30, 2011
Test Report Submission	10 Days	June 13, 2011

1.0 INTRODUCTION (CONTINUED)

1.4 Target of Evaluation Description

This test campaign will evaluate two different types of systems: Electronic Voting Support Wizards (EVSW) and the [redacted]. The EVSW's are electronic ballot delivery systems. The scope for testing the EVSW's will be limited to the following:

- Verifying the voting system distributes the ballot only to the intended voter;
- The information on the ballot or about the voter cannot be accessed by unauthorized persons;
- The EVSW's meet the applicable requirements from Section 5 "Security" of the UOCAVA Pilot Program Testing Requirements.

Below is an illustration of the scope for these systems.

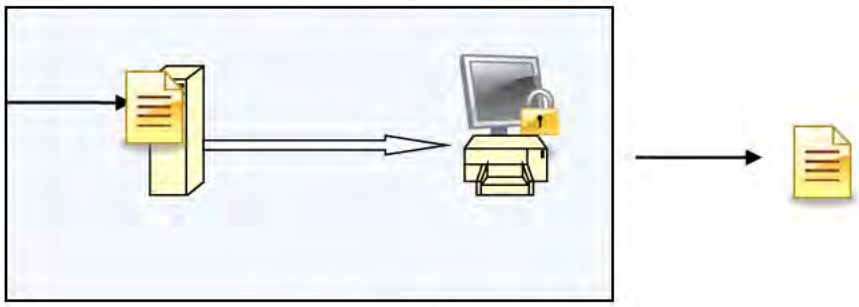


Figure 1-1 EVSW Ballot Delivery Illustration

This test campaign will include the following four EVSW's:

- [redacted]
- [redacted]
- [redacted]
- [redacted]

This test campaign also includes solutions for end-to-end voting remotely. These systems include voter registration, ballot delivery and voted ballot accumulation. The scope for testing these systems will verify supported functionality functions as designed and that the systems meet the applicable requirements from the UOCAVA Pilot Program Testing Requirements Section 5 Security. Below is an illustration from the UOCAVA Pilot Program Testing Requirements illustrating the scope for these systems.

1.0 INTRODUCTION (CONTINUED)

1.4 Target of Evaluation Description (continued)

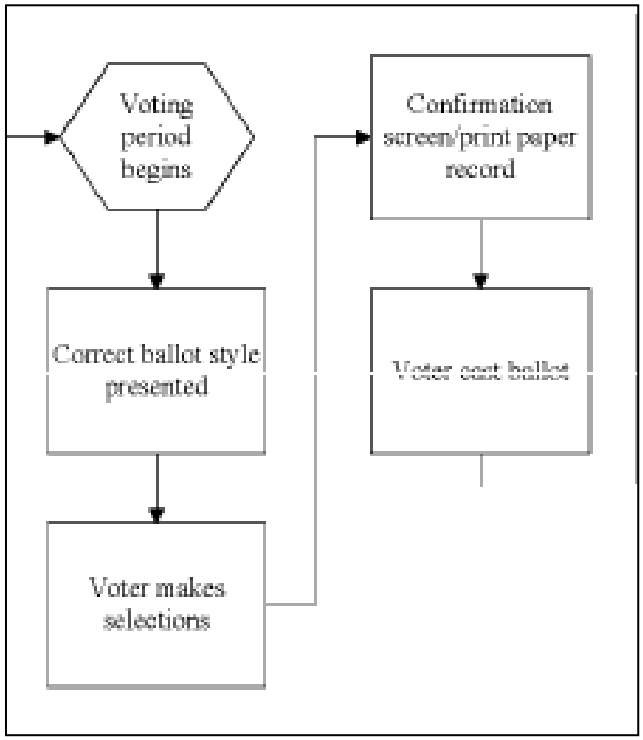


Figure 1-1 [redacted] End-to-End System Illustration

This test campaign includes one end-to-end solution:

[redacted]

2.0 MATERIALS REQUIRED FOR TESTING

The materials required for this test campaign include test software and hardware as well as the system hardware and software. Some manufacturers submitted test systems consisting of preloaded software on manufacturer's hardware platforms in Wyle's control. Other manufacturers had live systems that Wyle only had remote access to. This hardware is not being documented in this section.

Table 2-1 Submitted Hardware and Software

Submitted System Under Test (SUT)	Hardware Platform
[redacted] UOCAVA Overseas Voting Server	Apple PowerPC G4 CPU
[redacted] Host Operating System	OS X version 10.5.8
[redacted] Host Software Environment	Ruby on Rails,

2.0 MATERIALS REQUIRED FOR TESTING (CONTINUED)

Table 2-2 Remote Hardware and Software

Remote System Under Test (SUT)	Hardware Platform
[redacted]	Microsoft Windows Azure Hosted Service
[redacted] Server	multi-node ESXi cluster virtual machines with
[redacted] Software	LAMP Platform (Linux, Apache, MySQL and Perl)
[redacted] Encryption Processor	Laptop
[redacted]	Information Requested from Vendor

Table 2-3 Documentation

Document Name	Document Version
[redacted] Elector User Guide	1.0.2
[redacted] User Manual	None
[redacted] FVAP Setup Notes	None
[redacted] FVAP Usage Notes	None
[redacted] Responses to RFI	None
[redacted] Online Help (document)	Dated 7/14/2010
[redacted] Privacy Policy	Dated July, 2010
[redacted] Administration User Doc.	Dated 9/21/2010
[redacted] Level Design and Architecture	1.0
[redacted] Security Overview	1.0
[redacted] System Functionality	None

Table 2-4 Test Equipment and Software

Equipment	Description	Serial Number
Client Terminal (Wyle Lab)	Dell Desktop Optiplex 780	40RYCP1
Client Terminal (Wyle Lab)	Dell Desktop Optiplex 780	40SWCP1
Client Software	Browser, Internet Explorer 8.0	N/A
Client Software	Browser, Safari 5.0.4	N/A

3.0 TEST SPECIFICATIONS

3.1 Requirements

The strategy for evaluating the documented systems described in Section 2 of this document is to divide the UOCAVA Section 5 requirements into three main test areas: functional, cryptographic, and penetration.. Wyle has determined this to be the most efficient and thorough approach. The individual requirements have been mapped to specific test cases in Appendix A "Requirements Matrix" for each system under test.

3.1.1 Functional Tests

The functional test area will focus on inspection, review and execution as the primary test methods. Individual test cases have been design using manufacturer's documentation, architectural documents and security specifications. These test cases are being submitted with this Test Plan as Appendix B. Each test case is defined with a written script. The test consists of executing each step of the script, recording observations and relevant data as each step completes. The date and time of the start and stop of each test will be recorded. At the end of each test, the test conductor will collect all log records and all input and output data.
As the test is conducted any unexpected conditions or incorrect actions will be recorded and any suspected malfunction will be recorded as an exception report and provided to the vendor. The test conductor will continue the test case unless the malfunction invalidates or prevents further testing.

The functional tests are designs to cover the requirements in the following sections of the UOCAVA Pilot Program Testing Requirements:

5.1 Access Control

5.2 Identification and Authentication

5.4 Voting System Integrity Management

5.5 Communication Security

5.6 Logging

5.7 Incident Response

3.1.2 Cryptographic Tests

The cryptographic test area will focus on inspection, review and execution as the primary test methods. All cryptography will be tested for functionality, strength and NIST compliance, no matter which one of the three purposes it serves in the voting system, Confidentiality, Authentication or Random Number Generation (RNG). Those systems that generate cryptographic keys internally will be tested for key management. This includes the generation method, security of the generation method, seed values and RNG health tests. Key establishment and handling will also be tested. Individual test cases have been designed using "Use Case" and verification. These test cases are being submitted with this Test Plan as Appendix C. These tests consist of executing each step while, recording observations and relevant data as each step completes.

3.0 TEST SPECIFICATIONS (CONTINUED)

3.1 Requirements (continued)

3.1.2 Cryptographic Tests (continued)

The cryptographic tests are designs to cover the requirements in the following sections:

5.3 Cryptography

3.1.3 Penetration Tests

The penetration test area will be broken into two phases: discovery and exploratory. The discovery phase will consists of performing scans while the system is running with leveraged and unleveraged credentials. These scans will provide information about the ports, protocols, and hardware configurations as well as simulating certain portions of an attack on vulnerable areas of the system. The information gathered will be provided to a certified security professional, who will analyze the results and determine the best method and types of attacks to be performed during the exploratory phase of testing.

The exploratory phase of the penetration test will have specific test cases designed and executed. These test cases are based on all information gathered during discovery, any subsequent observations made during the exploratory phase and any Rules Of Engagement (ROE) previously agreed upon by the Wyle and manufacturer.

The penetration tests are designs to cover the requirements in the following sections:

5.8 Physical and Environmental Security

5.9 Penetration Resistance

4.0 TEST DATA

4.1 Data Recording

All equipment utilized for test data recording shall be identified in the test data package. The output test data shall be recorded in an appropriate manner as to allow for data analysis. Additionally, all test results, including functional test data, shall be recorded on the relevant test execution log. Results shall also be recorded real-time in engineering log books.

4.2 Test Data Acceptance Criteria

Wyle shall evaluate all test results against the requirements set forth in Section 5 “Security” of the UOCAVA Pilot Program Testing Requirements. Each SUT shall be evaluated for its performance against the referenced requirements. The acceptable range for system performance and the expected results for each test case shall be derived from the system documentation.

4.0 TEST DATA (CONTINUED)

4.2 Test Data Acceptance Criteria

These parameters shall encompass the test tolerances, the minimum number of combinations or alternatives of input and output conditions that can be exercised to constitute an acceptable test of the parameters involved, and the maximum number of interrupts, halts or other system breaks that may occur due to non-test conditions (excluding events from which recovery occurs automatically or where a relevant status message is displayed).

5.0 TEST PROCEDURE AND CONDITIONS

This section describes Wyle's proposed test procedures and the conditions under which those tests shall be conducted. The following subsections describe test procedures and a statement of the criteria by which readiness and successful completion shall be indicated and measured.

5.1 Test Facilities

All testing shall be conducted at the Wyle, Huntsville, AL facility unless otherwise annotated. All instrumentation, measuring, and test equipment used in the performance of this test campaign shall be listed on the Instrumentation equipment Sheet for each test and shall be calibrated in accordance with Wyle Laboratories' Quality Assurance Program, which complies with the requirements of ANSI/NCSL Z540-1 and ISO 10012-1. Standards used in performing all calibrations are traceable to the National Institute of Standards and Technology (NIST) by report number and date. When no national standards exist, the standards are traceable to international standards or the basis for calibration is otherwise documented.
Unless otherwise specified herein, all remaining tests, including system level functional testing, shall be performed at standard ambient conditions:

- Temperature: 25°C ± 10°C (77°F ± 18°F)
- Relative Humidity: 20 to 90%
- Atmospheric Pressure: Local Site Pressure

Unless otherwise specified herein, the following tolerances shall be used:

- Time ± 5%
- Temperature ± 3.6°F (2°C)
- Vibration Amplitude ± 10%
- Vibration Frequency ± 2%
- Random Vibration Acceleration
  20 to 500 Hertz ± 1.5 dB
  500 to 2000 Hertz ± 3.0 dB
- Random Overall grms ± 1.5 dB

Deviations to the tolerances on Page No. 2 of 11 shall be submitted by the test responsible agency with sufficient engineering information to substantiate the deviation request, but only when best effort technique and system limitations indicate the need for a deviation.

5.0 TEST PROCEDURE AND CONDITIONS (CONTINUED)

5.2 Test Set-Up

All voting machine equipment (hardware and software), shall be received and documented utilizing Wyle Receiving Ticket (WL-218, Nov'85) and proper QA procedures. When voting system hardware is received, Wyle Laboratories Shipping and Receiving personnel shall notify Wyle Laboratories QA personnel. With Wyle Laboratories QA personnel present, each test article shall be unpacked and inspected for obvious signs of degradation and/or damage that may have occurred during transit. Noticeable degradation and/or damage, if present, shall be recorded, photographs shall be taken, and the manufacturer representative shall be notified.
Wyle Laboratories QA personnel shall record the serial numbers and part numbers. Comparison shall be made between those numbers recorded and those listed on the shipper's manifest. Any discrepancies noted shall be brought to the attention of the manufacturer representative for resolution.

TDP items, including all manuals, and all source code modules received shall be inventoried and maintained by the Wyle Laboratories Project Engineer assigned to testing.

For hardware test setup, the system shall be configured as it would be for normal field use. This includes connecting all supporting equipment and peripherals. Wyle personnel shall properly configure and initialize the system, and verify that it is ready to be tested. Wyle shall develop the system performance levels to be measured during operational tests.

5.3 Test Sequence

There is no required test sequence for this test campaign. All systems will be tested for each test area.

5.4 Test Operation Procedures

Wyle Laboratories shall provide the step-by-step procedures for each test case to be conducted. Each step is assigned a test step number and this number, along with critical test data and test procedures information, shall be tabulated onto a Test Control Record for control and the recording of test results.

Any test failures shall be recorded on WH1066, Notice of Anomaly form. These Anomalies shall be reported to the manufacturer.

APPENDIX A
REQUIREMENTS MATRIX

[redacted]

REQUIREMENTS MATRIX

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
Section 5	**Security**		
5.1	**Access Control**		
	This section states requirements for the identification of authorized system users, processes and devices and the authentication or verification of those identities as a prerequisite to granting access to system processes and data. It also includes requirements to limit and control access to critical system components to protect system and data integrity, availability, confidentiality, and accountability. This section applies to all entities attempting to physically enter voting system facilities or to request services or data from the voting system.		
5.1.1	**Separation of Duties**		
5.1.1.1	The voting system SHALL allow the definition of personnel roles with segregated duties and responsibilities on critical processes to prevent a single person from compromising the integrity of the system.	1	Host Server Administration Test Case
5.1.1.2	The voting system SHALL ensure that only authorized roles, groups, or individuals have access to election data.	1	Host Server Administration Test Case
5.1.1.3	The voting system SHALL require at least two persons from a predefined group for validating the election configuration information, accessing the cast vote records, and starting the tabulation process..	N/A	
5.1.2	**Voting System Access**		
	The voting system SHALL provide access control mechanisms designed to permit authorized access and to prevent unauthorized access to the system.	5	Discovery Penetration Test Case
		1	Host Server Administration Test Case
5.1.2.1	The voting system SHALL identify and authenticate each person, to whom access is granted, and the specific functions and data to which each person holds authorized access.	10	Local Ballot Delivery Test Case
		4	Normal Ballot Delivery Test Case
		1	Host Server Administration Test Case
5.1.2.2	The voting system SHALL allow the administrator group or role to configure permissions and functionality for each identity, group or role to include account and group/role creation, modification, and deletion.	1	Host Server Administration Test Case
5.1.2.3	The voting system's default access control permissions SHALL implement the least privileged role or group needed.	1	Host Server Administration Test Case
5.1.2.4	The voting system SHALL prevent a lower-privilege process from modifying a higher-privilege process.	1	Host Server Administration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.1.2.5	The voting system SHALL NOT require its execution as an operating system privileged account and SHALL NOT require the use of an operating system privileged account for its operation.	N/A	
5.1.2.6	The voting system SHALL log the identification of all personnel accessing or attempting to access the voting system to the system event log.	5	Discovery Penetration Test Case
		4	Normal Ballot Delivery Test Case
		1	Host Server Administration Test Case
		10	Local Ballot Delivery Test Case
5.1.2.7	The *(voting system)* SHALL provide tools for monitoring access to the system. These tools SHALL provide specific users real time display of persons accessing the system as well as reports from logs.	5	Discovery Penetration Test Case
		1	Host Server Administration Test Case
5.1.2.8	Vote capture device located at the remote voting location and the central server SHALL have the capability to restrict access to the voting system after a preset number of login failures. a. The lockout threshold SHALL be configurable by appropriate administrators/operators b. The voting system SHALL log the event c. The voting system SHALL immediately send a notification to appropriate administrators/operators of the event. d. The voting system SHALL provide a mechanism for the appropriate administrators/operators to reactivate the account after appropriate confirmation.	5	Discovery Penetration Test Case
		1	Host Server Administration Test Case
5.1.2.9	The voting system SHALL log a notification when any account has been locked out.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.1.2.10	Authenticated sessions on critical processes SHALL have an inactivity time-out control that will require personnel re-authentication when reached. This time-out SHALL be implemented for administration and monitor consoles on all voting system devices.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.1.2.11	Authenticated sessions on critical processes SHALL have a screen-lock functionality that can be manually invoked.	N/A	
5.2	**Identification and Authentication**		
	Authentication mechanisms and their associated strength may vary from one voting system capability and architecture to another but all must meet the minimum requirement to maintain integrity and trust. It is important to consider a range of roles individuals may assume when operating different components in the voting system and each may require different authentication mechanisms. The requirements described in this section vary from role to role. For instance, a kiosk worker will have different identification and authentication characteristics than a voter. Also, for selected critical functions there may be cases where split knowledge or dual authorization is necessary to ensure security. This is especially relevant for critical cryptographic key management functions.		
5.2.1	**Authentication**		
5.2.1.1	Authentication mechanisms supported by the voting system SHALL support authentication strength of at least 1/1,000,000.	11	Host Server Security Test Case
5.2.1.2	The voting system SHALL authenticate users per the minimum authentication methods outlined below. Refer to document for the table layout: http://www.eac.gov/assets/1/AssetManager/UOCAVA_Pilot_Program_Requirements-03.24.10.pdf Table 5-1 Roles : Section 5 | Page 59	11	Host Server Security Test Case
5.2.1.3	The voting system SHALL provide multiple authentication methods to support multi-factor authentication.	4	Normal Ballot Delivery Test Case
		11	Host Server Security Test Case
5.2.1.4	When private or secret authentication data is stored by the voting system, it SHALL be protected to ensure that the confidentiality and integrity of the data are not violated.	11	Host Server Security Test Case
5.2.1.5	The voting system SHALL provide a mechanism to reset a password if it is forgotten, in accordance with the system access/security policy.	1	Host Server Administration Test Case
5.2.1.6	The voting system SHALL allow the administrator group or role to specify password strength for all accounts including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters per NIST 800-63 Electronic Authentication Guideline Standards.	1	Host Server Administration Test Case
5.2.1.7	The voting system SHALL enforce password histories and allow the administrator to configure the history length when passwords are stored by the system.	1	Host Server Administration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.2.1.8	The voting system SHALL ensure that the user name is not used in the password.	1	Host Server Administration Test Case
5.2.1.9	The voting system SHALL provide a means to automatically expire passwords.	1	Host Server Administration Test Case
5.2.1.10	The voting system servers and vote capture devices SHALL identify and authenticate one another using NIST - approved cryptographic authentication methods at the 112 bits of security.	3	Cryptography Test Case
5.2.1.11	Remote voting location site Virtual Private Network (VPN) connections (i.e., vote capture devices) to voting servers SHALL be authenticated using strong mutual cryptographic authentication at the 112 bits of security.	N/A	
5.2.1.12	Message authentication SHALL be used for applications to protect the integrity of the message content using a schema with 112 bits of security.	N/A	
5.2.1.13	IPsec, SSL, or TLS and MAC mechanisms SHALL all be configured to be compliant with FIPS 140-2 using approved algorithm suites and protocols.	3	Cryptography Test Case
5.3	**Cryptography**		
	Cryptography serves several purposes in voting systems. They include: Confidentiality: where necessary the confidentiality of voting records can be provided by encryption; Authentication: data and programs can be authenticated by a digital signature or message authentication codes (MAC), or by comparison of the cryptographic hashes of programs or data with the reliably known hash values of the program or data. If the program or data are altered, then that alteration is detected when the signature or MAC is verified, or the hash on the data or program is compared to the known hash value. Typically the programs loaded on voting systems and the ballot definitions used by voting systems are verified by the systems, while systems apply digital signatures to authenticate the critical audit data that they output. For remote connections cryptographic user authentication mechanism SHALL be based on strong authentication methods; and Random number generation: random numbers are used for several purposes including the creation of cryptographic keys for cryptographic algorithms and methods to provide the services listed above, and as identifiers for voting records that can be used to identify or correlate the records without providing any information that could identify the voter.		
5.3.1	**General Cryptography Requirements**		
5.3.1.1	All cryptographic functionality SHALL be implemented using NIST-approved cryptographic algorithms/schemas, or use published and credible cryptographic algorithms/schemas/protocols.	3	Cryptography Test Case
5.3.1.2	Cryptographic algorithms and schemas SHALL be implemented with a security strength equivalent to at least 112 bits of security to protect sensitive voting information and election records.	3	Cryptography Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.3.1.3	Cryptography used to protect information in-transit over public telecommunication networks SHALL use NIST-approved algorithms and cipher suites. In addition the implementations of these algorithms SHALL be NIST-approved (Cryptographic Algorithm Validation Program).	3	Cryptography Test Case
5.3.2	**Key Management**		
	The following requirements apply to voting systems that generate cryptographic keys internally.		
5.3.2.1	Cryptographic keys generated by the voting system SHALL use a NIST-approved key generation method, or a published and credible key generation method.	3	Cryptography Test Case
5.3.2.2	Compromising the security of the key generation method (e.g., guessing the seed value to initialize the deterministic random number generator (RNG)) SHALL require as least as many operations as determining the value of the generated key.	N/T	
5.3.2.3	If a seed key is entered during the key generation process, entry of the key SHALL meet the key entry requirements in 5.3.3.1. If intermediate key generation values are output from the cryptographic module, the values SHALL be output either in encrypted form or under split knowledge procedures.	3	Cryptography Test Case
5.3.2.4	Cryptographic keys used to protect information in-transit over public telecommunication networks SHALL use NIST-approved key generation methods. If the approved key generation method requires input from a random number generator, then an approved (FIPS 140-2) random number generator SHALL be used.	3	Cryptography Test Case
5.3.2.5	Random number generators used to generate cryptographic keys SHALL implement one or more health tests that provide assurance that the random number generator continues to operate as intended (e.g., the entropy source is not stuck).	3	Cryptography Test Case
5.3.3	**Key Establishment**		
	Key establishment may be performed by automated methods (e.g., use of a public key algorithm), manual methods (use of a manually transported key loading device), or a combination of automated and manual methods.		
5.3.3.1	Secret and private keys established using automated methods SHALL be entered into and output from a voting system in encrypted form. Secret and private keys established using manual methods may be entered into or output from a system in plaintext form.	3	Cryptography Test Case
5.3.4.1	Cryptographic keys stored within the voting system SHALL NOT be stored in plaintext. Keys stored outside the voting system SHALL be protected from disclosure or modification.	3	Cryptography Test Case
5.3.4.2	The voting system SHALL provide methods to zeroize all plaintext secret and private cryptographic keys within the system.	3	Cryptography Test Case
5.3.4.3	The voting system SHALL support the capability to reset cryptographic keys to new values.	3	Cryptography Test Case
5.4	**Voting System Integrity Management**		
	This section addresses the secure deployment and operation of the voting system, including the protection of removable media and protection against malicious software.		

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.4.1	**Protecting the Integrity of the Voting System**		
5.4.1.1	The integrity and authenticity of each individual cast vote SHALL be protected from any tampering or modification during transmission.	N/A	
5.4.1.2	The integrity and authenticity of each individual cast vote SHALL be preserved by means of a digital signature during storage.	N/A	
5.4.1.3	Cast vote data SHALL NOT be permanently stored on the vote capture device.	4	Normal Ballot Delivery Test Case
5.4.1.4	The integrity and authenticity of the electronic ballot box SHALL be protected by means of a digital signature.	N/A	
5.4.1.5	The voting system SHALL use malware detection software to protect against known malware that targets the operating system, services, and applications.	5	Discovery Penetration Test Case
5.4.1.6	The voting system SHALL provide a mechanism for updating malware detection signatures.	5	Discovery Penetration Test Case
5.4.1.7	The voting system SHALL provide the capability for kiosk workers to validate the software used on the vote capture devices as part of the daily initiation of kiosk operations.	N/A	
5.5	**Communications Security**		
	This section provides requirements for communications security. These requirements address ensuring the integrity of transmitted information and protecting the voting system from external communications-based threats.		
5.5.1	**Data Transmission Security**		
5.5.1.1	Voting systems that transmit data over communications links SHALL provide integrity protection for data in transit through the generation of integrity data (digital signatures and/or message authentication codes) for outbound traffic and verification of the integrity data for inbound traffic.	11	Host Server Security Test Case
5.5.1.2	Voting systems SHALL use at a minimum TLS 1.0, SSL 3.1 or equivalent protocols, including all updates to both protocols and implementations as of the date of the submission (e.g., RFC 5746 for TLS 1.0).	3	Cryptography Test Case
5.5.1.3	Voting systems deploying VPNs SHALL configure them to only allow FIPS-compliant cryptographic algorithms and cipher suites.	N/A	
5.5.1.4	Each communicating device SHALL have a unique system identifier.	5	Discovery Penetration Test Case
5.5.1.5	Each device SHALL mutually strongly authenticate using the system identifier before additional network data packets are processed.	6	Remote Terminal Security Test Case
		1	Host Server Administration Test Case
5.5.1.6	Data transmission SHALL preserve the secrecy of voters' ballot selections and SHALL prevent the violation of ballot secrecy and integrity.	5	Discovery Penetration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.5.2	**External Threats**		
	Voting systems SHALL implement protections against external threats to which the system may be susceptible.	5	Discovery Penetration Test Case
		6	Remote Terminal Security Test Case
		1	Host Server Administration Test Case
5.5.2.1	Voting system components SHALL have the ability to enable or disable physical network interfaces.	1	Host Server Administration Test Case
5.5.2.2	The number of active ports and associated network services and protocols SHALL be restricted to the minimum required for the voting system to function.	11	Host Server Security Test Case
5.5.2.3	The voting system SHALL block all network connections that are not over a mutually authenticated channel.	11	Host Server Security Test Case
5.6	**Logging**		
5.6.1	**Log Management**		
5.6.1.1	The voting system SHALL implement default settings for secure log management activities, including log generation, transmission, storage, analysis, and disposal.	1	Host Server Administration Test Case
5.6.1.2	Logs SHALL only be accessible to authorized roles.	1	Host Server Administration Test Case
5.6.1.3	The voting system SHALL restrict log access to append-only for privileged logging processes and read-only for authorized roles.	1	Host Server Administration Test Case
5.6.1.4	The voting system SHALL log logging failures, log clearing, and log rotation.	1	Host Server Administration Test Case
5.6.1.5	The voting system SHALL store log data in a publicly documented format, such as XML, or include a utility to export log data into a publicly documented format.	1	Host Server Administration Test Case
5.6.1.6	The voting system SHALL ensure that each jurisdiction's event logs and each component's logs are separable from each other.	N/A	
5.6.1.7	The voting system SHALL include an application or program to view, analyze, and search event logs.	1	Host Server Administration Test Case
5.6.1.8	All logs SHALL be preserved in a useable manner prior to voting system decommissioning.	1	Host Server Administration Test Case
5.6.1.9	Logs SHALL NOT contain any data that could violate the privacy of the voter's identity.	4	Normal Ballot Delivery Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.6.1.10	Timekeeping mechanisms SHALL generate time and date values, including hours, minutes, and seconds.	1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
		10	Local Ballot Delivery Test Case
5.6.1.11	The precision of the timekeeping mechanism SHALL be able to distinguish and properly order all log events.	10	Local Ballot Delivery Test Case
		4	Normal Ballot Delivery Test Case
5.6.1.12	Only the system administrator SHALL be permitted to set the system clock.	1	Host Server Administration Test Case
5.6.2	**Communication Logging**		
5.6.2.1	All communications actions SHALL be logged.	5	Discovery Penetration Test Case
		4	Normal Ballot Delivery Test Case
		1	Host Server Administration Test Case
		3	Cryptography Test Case
5.6.2.2	The communications log SHALL contain at least the following entries: Times when the communications are activated and deactivated; Services accessed; Identification of the device which data was transmitted to or received from; Identification of authorized entity; and Successful and unsuccessful attempts to access communications or services.	4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case
5.6.3	**System Event Logging**		
	This section describes requirements for the voting system to perform event logging for system maintenance troubleshooting, recording the history of system activity, and detecting unauthorized or malicious activity. The operating system, and/or applications software may perform the actual event logging. There may be multiple logs in use for any system component.		

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.6.3.1	The voting system SHALL log the following data for each event: a. System ID; b. Unique event ID and/or type; c. Timestamp; d. Success or failure of event, if applicable; e. User ID triggering the event, if applicable; and f. Jurisdiction, if applicable.	4	Normal Ballot Delivery Test Case
		1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
		7	Recovery form hardware error Test Case
5.6.3.2	All critical events SHALL be recorded in the system event log.	7	Recovery form hardware error Test Case
		4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case
5.6.3.3	At a minimum the voting system SHALL log the events described in the table below. NOTE: See "Table 5-2 System Events" in document - page 71	1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
		3	Cryptography Test Case
		7	Recovery form hardware error Test Case
		5	Discovery Penetration Test Case
5.7	**Incident Response**		
5.7.1	**Incident Response Support**		
5.7.1.1	Manufacturers SHALL document what types of system operations or security events (e.g., failure of critical component, detection of malicious code, unauthorized access to restricted data) are classified as critical.	N/A	
5.7.1.2	An alarm that notifies appropriate personnel SHALL be generated on the vote capture device, system server, or tabulation device, depending upon which device has the error, if a critical event is detected.	N/A	
5.8	**Physical and Environmental Security**		
5.8.1	**Physical Access**		
5.8.1.1	Any unauthorized physical access SHALL leave physical evidence that an unauthorized event has taken place.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.8.2.1	The voting system SHALL disable physical ports and access points that are not essential to voting operations, testing, and auditing.	11	Host Server Security Test Case
5.8.3.1	If a physical connection between the vote capture device and a component is broken, the affected vote capture device port SHALL be automatically disabled.	N/A	
5.8.3.2	The voting system SHALL produce a visual alarm if a connected component is physically disconnected.	N/A	
5.8.3.3	An event log entry that identifies the name of the affected device SHALL be generated if a vote capture device component is disconnected.	7	Recovery form hardware error Test Case
5.8.3.4	Disabled ports SHALL only be re-enabled by authorized administrators.	1	Host Server Administration Test Case
5.8.3.5	Vote capture devices SHALL be designed with the capability to restrict physical access to voting device ports that accommodate removable media with the exception of ports used to activate a voting session.	N/A	
5.8.3.6	Vote capture devices SHALL be designed to give a physical indication of tampering or unauthorized access to ports and all other access points, if used as described in the manufacturer's documentation.	N/A	
5.8.3.7	Vote capture devices SHALL be designed such that physical ports can be manually disabled by an authorized administrator.	N/A	
5.8.4	**Door Cover and Panel Security**		
5.8.4.1	Access points such as covers and panels SHALL be secured by locks or tamper evident or tamper resistant countermeasures and SHALL be implemented so that kiosk workers can monitor access to vote capture device components through these points.	N/A	
5.8.5	**Secure Paper Record Receptacle**		
	If the voting system provides paper record containers then they SHALL be designed such that any unauthorized physical access results in physical evidence that an unauthorized event has taken place.	N/A	
5.8.6	**Secure Physical Lock and Key**		
5.8.6.1	Voting equipment SHALL be designed with countermeasures that provide physical indication that unauthorized attempts have been made to access locks installed for security purposes.	N/A	
5.8.6.2	Manufacturers SHALL provide locking systems for securing vote capture devices that can make use of keys that are unique to each owner.	N/A	
5.8.7	**Media Protection**		
	These requirements apply to all media, both paper and digital, that contain personal privacy related data or other protected or sensitive types of information.		

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.8.7.1	The voting system SHALL meet the following requirements: a. All paper records (including rejected ones) printed at the kiosk locations SHALL be deposited in a secure container; b. Vote capture device hardware, software and sensitive information (e.g., electoral roll) SHALL be physically protected to prevent unauthorized modification or disclosure; and c. Vote capture device hardware components, peripherals and removable media SHALL be identified and registered by means of a unique serial number or other identifier.	N/A	
5.9	**Penetration Resistance**		
5.9.1	**Resistance to Penetration Attempt**		
5.9.1.1	The voting system SHALL be resistant to attempts to penetrate the system by any remote unauthorized entity.	5	Discovery Penetration Test Case
5.9.1.2	The voting system SHALL be configured to minimize ports, responses and information disclosure about the system while still providing appropriate functionality.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.9.1.3	The voting system SHALL provide no access, information or services to unauthorized entities.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.9.1.4	All interfaces SHALL be penetration resistant including TCP/IP, wireless, and modems from any point in the system.	11	Host Server Security Test Case
5.9.1.5	The configuration and setup to attain penetration resistance SHALL be clearly and completely documented.	N/A	
5.9.2.1	The scope of penetration testing SHALL include all the voting system components. The scope of penetration testing includes but is not limited to the following: System server; Vote capture devices; Tabulation device; All items setup and configured per Technical Data Package (TDP) recommendations; Local wired and wireless networks; and 03/09/2011 Internet connections.	5	Discovery Penetration Test Case
5.9.2.2	Penetration testing SHALL be conducted on a voting system set up in a controlled lab environment. Setup and configuration SHALL be conducted in accordance with the TDP, and SHALL replicate the real world environment in which the voting system will be used.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.9.2.3	The penetration testing team SHALL conduct white box testing using manufacturer supplied documentation and voting system architecture information. Documentation includes the TDP and user documentation. The testing team SHALL have access to any relevant information regarding the voting system configuration. This includes, but is not limited to, network layout and Internet Protocol addresses for system devices and components. The testing team SHALL be provided any source code included in the TDP.	N/A	
5.9.2.04	Penetration testing seeks out vulnerabilities in the voting system that might be used to change the outcome of an election, interfere with voter ability to cast ballots, ballot counting, or compromise ballot secrecy. The penetration testing team SHALL prioritize testing efforts based on the following: a. Threat scenarios for the voting system under investigation; b. Remote attacks SHALL be prioritized over in-person attacks; c. Attacks with a large impact SHALL be prioritized over attacks with a more narrow impact; and d. Attacks that can change the outcome of an election SHALL be prioritized over attacks that compromise ballot secrecy or cause non-selective denial of service.	5	Discovery Penetration Test Case

[redacted]

REQUIREMENTS MATRIX

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
Section 5	**Security**		
5.1	**Access Control**		
	This section states requirements for the identification of authorized system users, processes and devices and the authentication or verification of those identities as a prerequisite to granting access to system processes and data. It also includes requirements to limit and control access to critical system components to protect system and data integrity, availability, confidentiality, and accountability. This section applies to all entities attempting to physically enter voting system facilities or to request services or data from the voting system.		
5.1.1	**Separation of Duties**		
5.1.1.1	The voting system SHALL allow the definition of personnel roles with segregated duties and responsibilities on critical processes to prevent a single person from compromising the integrity of the system.	1	Host Server Administration Test Case
5.1.1.2	The voting system SHALL ensure that only authorized roles, groups, or individuals have access to election data.	1	Host Server Administration Test Case
5.1.1.3	The voting system SHALL require at least two persons from a predefined group for validating the election configuration information, accessing the cast vote records, and starting the tabulation process..	N/A	
5.1.2	**Voting System Access**		
	The voting system SHALL provide access control mechanisms designed to permit authorized access and to prevent unauthorized access to the system.		
5.1.2.1	The voting system SHALL identify and authenticate each person to whom access is granted, and the specific functions and data to which each person holds authorized access.	1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
5.1.2.2	The voting system SHALL allow the administrator group or role to configure permissions and functionality for each identity, group or role to include account and group/role creation, modification, and deletion.	1	Host Server Administration Test Case
5.1.2.3	The voting system's default access control permissions SHALL implement the least privileged role or group needed.	1	Host Server Administration Test Case
5.1.2.4	The voting system SHALL prevent a lower-privilege process from modifying a higher-privilege process.	1	Host Server Administration Test Case
5.1.2.5	The voting system SHALL NOT require its execution as an operating system privileged account and SHALL NOT require the use of an operating system privileged account for its operation.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.1.2.6	The voting system SHALL log the identification of all personnel accessing or attempting to access the voting system to the system event log.	7	Recovery form hardware error Test Case
		1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case
5.1.2.7	The *(voting system)* SHALL provide tools for monitoring access to the system. These tools SHALL provide specific users real time display of persons accessing the system as well as reports from logs.	1	Host Server Administration Test Case
5.1.2.8	Vote capture device located at the remote voting location and the central server SHALL have the capability to restrict access to the voting system after a preset number of login failures. a. The lockout threshold SHALL be configurable by appropriate administrators/operators b. The voting system SHALL log the event c. The voting system SHALL immediately send a notification to appropriate administrators/operators of the event. d. The voting system SHALL provide a mechanism for the appropriate administrators/operators to reactivate the account after appropriate confirmation.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.1.2.9	The voting system SHALL log a notification when any account has been locked out.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.1.2.10	Authenticated sessions on critical processes SHALL have an inactivity time-out control that will require personnel re-authentication when reached. This time-out SHALL be implemented for administration and monitor consoles on all voting system devices.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.1.2.11	Authenticated sessions on critical processes SHALL have a screen-lock functionality that can be manually invoked.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.2	**Identification and Authentication**		
	Authentication mechanisms and their associated strength may vary from one voting system capability and architecture to another but all must meet the minimum requirement to maintain integrity and trust. It is important to consider a range of roles individuals may assume when operating different components in the voting system and each may require different authentication mechanisms. The requirements described in this section vary from role to role. For instance, a kiosk worker will have different identification and authentication characteristics than a voter. Also, for selected critical functions there may be cases where split knowledge or dual authorization is necessary to ensure security. This is especially relevant for critical cryptographic key management functions.		
5.2.1	**Authentication**		
5.2.1.1	Authentication mechanisms supported by the voting system SHALL support authentication strength of at least 1/1,000,000.	11	Host Server Security Test Case
5.2.1.2	The voting system SHALL authenticate users per the minimum authentication methods outlined below. Refer to document for the table layout: http://www.eac.gov/assets/1/AssetManager/UOCAVA_Pilot_Program_Requirments-03.24.10.pdf Table 5-1 Roles : Section 5 | Page 59	11	Host Server Security Test Case
5.2.1.3	The voting system SHALL provide multiple authentication methods to support multi-factor authentication.	1	Host Server Administration Test Case
5.2.1.4	When private or secret authentication data is stored by the voting system, it SHALL be protected to ensure that the confidentiality and integrity of the data are not violated.	11	Host Server Security Test Case
5.2.1.5	The voting system SHALL provide a mechanism to reset a password if it is forgotten, in accordance with the system access/security policy.	1	Host Server Administration Test Case
5.2.1.6	The voting system SHALL allow the administrator group or role to specify password strength for all accounts including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters per NIST 800-63 Electronic Authentication Guideline Standards.	1	Host Server Administration Test Case
5.2.1.7	The voting system SHALL enforce password histories and allow the administrator to configure the history length when passwords are stored by the system.	1	Host Server Administration Test Case
5.2.1.8	The voting system SHALL ensure that the user name is not used in the password.	1	Host Server Administration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.2.1.9	The voting system SHALL provide a means to automatically expire passwords.	1	Host Server Administration Test Case
5.2.1.10	The voting system servers and vote capture devices SHALL identify and authenticate one another using NIST - approved cryptographic authentication methods at the 112 bits of security.	3	Cryptography Test Case
5.2.1.11	Remote voting location site Virtual Private Network (VPN) connections (i.e., vote capture devices) to voting servers SHALL be authenticated using strong mutual cryptographic authentication at the 112 bits of security.	N/A	
5.2.1.12	Message authentication SHALL be used for applications to protect the integrity of the message content using a schema with 112 bits of security.	11	Host Server Security Test Case
5.2.1.13	IPsec, SSL, or TLS and MAC mechanisms SHALL all be configured to be compliant with FIPS 140-2 using approved algorithm suites and protocols.	3	Cryptography Test Case
5.3	**Cryptography**		
	Cryptography serves several purposes in voting systems. They include: Confidentiality: where necessary the confidentiality of voting records can be provided by encryption; Authentication: data and programs can be authenticated by a digital signature or message authentication codes (MAC), or by comparison of the cryptographic hashes of programs or data with the reliably known hash values of the program or data. If the program or data are altered, then that alteration is detected when the signature or MAC is verified, or the hash on the data or program is compared to the known hash value. Typically the programs loaded on voting systems and the ballot definitions used by voting systems are verified by the systems, while systems apply digital signatures to authenticate the critical audit data that they output. For remote connections cryptographic user authentication mechanism SHALL be based on strong authentication methods; and Random number generation: random numbers are used for several purposes including the creation of cryptographic keys for cryptographic algorithms and methods to provide the services listed above, and as identifiers for voting records that can be used to identify or correlate the records without providing any information that could identify the voter.		
5.3.1	**General Cryptography Requirements**		
5.3.1.1	All cryptographic functionality SHALL be implemented using NIST-approved cryptographic algorithms/schemas, or use published and credible cryptographic algorithms/schemas/protocols.	3	Cryptography Test Case
5.3.1.2	Cryptographic algorithms and schemas SHALL be implemented with a security strength equivalent to at least 112 bits of security to protect sensitive voting information and election records.	3	Cryptography Test Case
5.3.1.3	Cryptography used to protect information in-transit over public telecommunication networks SHALL use NIST-approved algorithms and cipher suites. In addition the implementations of these algorithms SHALL be NIST-approved (Cryptographic Algorithm Validation Program).	3	Cryptography Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.3.2	**Key Management**		
	The following requirements apply to voting systems that generate cryptographic keys internally.		
5.3.2.1	Cryptographic keys generated by the voting system SHALL use a NIST-approved key generation method, or a published and credible key generation method.	3	Cryptography Test Case
5.3.2.2	Compromising the security of the key generation method (e.g., guessing the seed value to initialize the deterministic random number generator (RNG)) SHALL require as least as many operations as determining the value of the generated key.	N/T	
5.3.2.3	If a seed key is entered during the key generation process, entry of the key SHALL meet the key entry requirements in 5.3.3.1. If intermediate key generation values are output from the cryptographic module, the values SHALL be output either in encrypted form or under split knowledge procedures.	3	Cryptography Test Case
5.3.2.4	Cryptographic keys used to protect information in-transit over public telecommunication networks SHALL use NIST-approved key generation methods. If the approved key generation method requires input from a random number generator, then an approved (FIPS 140-2) random number generator SHALL be used.	3	Cryptography Test Case
5.3.2.5	Random number generators used to generate cryptographic keys SHALL implement one or more health tests that provide assurance that the random number generator continues to operate as intended (e.g., the entropy source is not stuck).	3	Cryptography Test Case
5.3.3	**Key Establishment**		
	Key establishment may be performed by automated methods (e.g., use of a public key algorithm), manual methods (use of a manually transported key loading device), or a combination of automated and manual methods.		
5.3.3.1	Secret and private keys established using automated methods SHALL be entered into and output from a voting system in encrypted form. Secret and private keys established using manual methods may be entered into or output from a system in plaintext form.	3	Cryptography Test Case
5.3.4.1	Cryptographic keys stored within the voting system SHALL NOT be stored in plaintext. Keys stored outside the voting system SHALL be protected from disclosure or modification.	3	Cryptography Test Case
5.3.4.2	The voting system SHALL provide methods to zeroize all plaintext secret and private cryptographic keys within the system.	3	Cryptography Test Case
5.3.4.3	The voting system SHALL support the capability to reset cryptographic keys to new values.	3	Cryptography Test Case
5.4	**Voting System Integrity Management**		
	This section addresses the secure deployment and operation of the voting system, including the protection of removable media and protection against malicious software.		
5.4.1	**Protecting the Integrity of the Voting System**		
5.4.1.1	The integrity and authenticity of each individual cast vote SHALL be protected from any tampering or modification during transmission.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.4.1.2	The integrity and authenticity of each individual cast vote SHALL be preserved by means of a digital signature during storage.	N/A	
5.4.1.3	Cast vote data SHALL NOT be permanently stored on the vote capture device.	4	Normal Ballot Delivery Test Case
5.4.1.4	The integrity and authenticity of the electronic ballot box SHALL be protected by means of a digital signature.	N/A	
5.4.1.5	The voting system SHALL use malware detection software to protect against known malware that targets the operating system, services, and applications.	5	Discovery Penetration Test Case
5.4.1.6	The voting system SHALL provide a mechanism for updating malware detection signatures.	5	Discovery Penetration Test Case
5.4.1.7	The voting system SHALL provide the capability for kiosk workers to validate the software used on the vote capture devices as part of the daily initiation of kiosk operations.	N/A	
5.5	**Communications Security**		
	This section provides requirements for communications security. These requirements address ensuring the integrity of transmitted information and protecting the voting system from external communications-based threats.		
5.5.1	**Data Transmission Security**		
5.5.1.1	Voting systems that transmit data over communications links SHALL provide integrity protection for data in transit through the generation of integrity data (digital signatures and/or message authentication codes) for outbound traffic and verification of the integrity data for inbound traffic.	11	Host Server Security Test Case
5.5.1.2	Voting systems SHALL use at a minimum TLS 1.0, SSL 3.1 or equivalent protocols, including all updates to both protocols and implementations as of the date of the submission (e.g., RFC 5746 for TLS 1.0).	11	Host Server Security Test Case
5.5.1.3	Voting systems deploying VPNs SHALL configure them to only allow FIPS-compliant cryptographic algorithms and cipher suites.	N/A	
5.5.1.4	Each communicating device SHALL have a unique system identifier.	11	Host Server Security Test Case
5.5.1.5	Each device SHALL mutually strongly authenticate using the system identifier before additional network data packets are processed.	11	Host Server Security Test Case
5.5.1.6	Data transmission SHALL preserve the secrecy of voters' ballot selections and SHALL prevent the violation of ballot secrecy and integrity.	5	Discovery Penetration Test Case
5.5.2	**External Threats**		
	Voting systems SHALL implement protections against external threats to which the system may be susceptible.	5	Discovery Penetration Test Case
5.5.2.1	Voting system components SHALL have the ability to enable or disable physical network interfaces.	1	Host Server Administration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.5.2.2	The number of active ports and associated network services and protocols SHALL be restricted to the minimum required for the voting system to function.	11	Host Server Security Test Case
5.5.2.3	The voting system SHALL block all network connections that are not over a mutually authenticated channel.	11	Host Server Security Test Case
5.6	**Logging**		
5.6.1	**Log Management**		
5.6.1.1	The voting system SHALL implement default settings for secure log management activities, including log generation, transmission, storage, analysis, and disposal.	1	Host Server Administration Test Case
5.6.1.2	Logs SHALL only be accessible to authorized roles.	1	Host Server Administration Test Case
5.6.1.3	The voting system SHALL restrict log access to append-only for privileged logging processes and read-only for authorized roles.	1	Host Server Administration Test Case
5.6.1.4	The voting system SHALL log logging failures, log clearing, and log rotation.	1	Host Server Administration Test Case
5.6.1.5	The voting system SHALL store log data in a publicly documented format, such as XML, or include a utility to export log data into a publicly documented format.	1	Host Server Administration Test Case
5.6.1.6	The voting system SHALL ensure that each jurisdiction's event logs and each component's logs are separable from each other.	N/A	
5.6.1.7	The voting system SHALL include an application or program to view, analyze, and search event logs.	1	Host Server Administration Test Case
5.6.1.8	All logs SHALL be preserved in a useable manner prior to voting system decommissioning.	1	Host Server Administration Test Case
5.6.1.9	Logs SHALL NOT contain any data that could violate the privacy of the voter's identity.	4	Normal Ballot Delivery Test Case
5.6.1.10	Timekeeping mechanisms SHALL generate time and date values, including hours, minutes, and seconds.	4	Normal Ballot Delivery Test Case
		1	Host Server Administration Test Case
5.6.1.11	The precision of the timekeeping mechanism SHALL be able to distinguish and properly order all log events.	4	Normal Ballot Delivery Test Case
5.6.1.12	Only the system administrator SHALL be permitted to set the system clock.	N/A	
5.6.2	**Communication Logging**		

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.6.2.1	All communications actions SHALL be logged.	4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case
5.6.2.2	The communications log SHALL contain at least the following entries: Times when the communications are activated and deactivated; Services accessed; Identification of the device which data was transmitted to or received from; Identification of authorized entity; and Successful and unsuccessful attempts to access communications or services.	4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case
5.6.3	**System Event Logging**		
	This section describes requirements for the voting system to perform event logging for system maintenance troubleshooting, recording the history of system activity, and detecting unauthorized or malicious activity. The operating system, and/or applications software may perform the actual event logging. There may be multiple logs in use for any system component.		
5.6.3.1	The voting system SHALL log the following data for each event: a. System ID; b. Unique event ID and/or type; c. Timestamp; d. Success or failure of event, if applicable; e. User ID triggering the event, if applicable; and f. Jurisdiction, if applicable.	1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
		7	Recovery form hardware error Test Case
		5	Discovery Penetration Test Case
5.6.3.2	All critical events SHALL be recorded in the system event log.	5	Discovery Penetration Test Case
		4	Normal Ballot Delivery Test Case
		7	Recovery form hardware error Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.6.3.3	At a minimum the voting system SHALL log the events described in the table below. NOTE: See "Table 5-2 System Events" in document - page 71	1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case
		7	Recovery form hardware error Test Case
5.7	**Incident Response**		
5.7.1	**Incident Response Support**		
5.7.1.1	Manufacturers SHALL document what types of system operations or security events (e.g., failure of critical component, detection of malicious code, unauthorized access to restricted data) are classified as critical.	N/A	
5.7.1.2	An alarm that notifies appropriate personnel SHALL be generated on the vote capture device, system server, or tabulation device, depending upon which device has the error, if a critical event is detected.	N/A	
5.8	**Physical and Environmental Security**		
5.8.1	**Physical Access**		
5.8.1.1	Any unauthorized physical access SHALL leave physical evidence that an unauthorized event has taken place.	N/A	
5.8.2.1	The voting system SHALL disable physical ports and access points that are not essential to voting operations, testing, and auditing.	11	Host Server Security Test Case
5.8.3.1	If a physical connection between the vote capture device and a component is broken, the affected vote capture device port SHALL be automatically disabled.	N/A	
5.8.3.2	The voting system SHALL produce a visual alarm if a connected component is physically disconnected.	N/A	
5.8.3.3	An event log entry that identifies the name of the affected device SHALL be generated if a vote capture device component is disconnected.	7	Recovery form hardware error Test Case
5.8.3.4	Disabled ports SHALL only be re-enabled by authorized administrators.	1	Host Server Administration Test Case
5.8.3.5	Vote capture devices SHALL be designed with the capability to restrict physical access to voting device ports that accommodate removable media with the exception of ports used to activate a voting session.	N/A	
5.8.3.6	Vote capture devices SHALL be designed to give a physical indication of tampering or unauthorized access to ports and all other access points, if used as described in the manufacturer's documentation.	N/A	
5.8.3.7	Vote capture devices SHALL be designed such that physical ports can be manually disabled by an authorized administrator.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.8.4	**Door Cover and Panel Security**		
5.8.4.1	Access points such as covers and panels SHALL be secured by locks or tamper evident or tamper resistant countermeasures and SHALL be implemented so that kiosk workers can monitor access to vote capture device components through these points.	N/A	
5.8.5	**Secure Paper Record Receptacle**		
	If the voting system provides paper record containers then they SHALL be designed such that any unauthorized physical access results in physical evidence that an unauthorized event has taken place.	N/A	
5.8.6	**Secure Physical Lock and Key**		
5.8.6.1	Voting equipment SHALL be designed with countermeasures that provide physical indication that unauthorized attempts have been made to access locks installed for security purposes.	N/A	
5.8.6.2	Manufacturers SHALL provide locking systems for securing vote capture devices that can make use of keys that are unique to each owner.	N/A	
5.8.7	**Media Protection**		
	These requirements apply to all media, both paper and digital, that contain personal privacy related data or other protected or sensitive types of information.		
5.8.7.1	The voting system SHALL meet the following requirements: a. All paper records (including rejected ones) printed at the kiosk locations SHALL be deposited in a secure container; b. Vote capture device hardware, software and sensitive information (e.g., electoral roll) SHALL be physically protected to prevent unauthorized modification or disclosure; and c. Vote capture device hardware components, peripherals and removable media SHALL be identified and registered by means of a unique serial number or other identifier.	N/A	
5.9	**Penetration Resistance**		
5.9.1	**Resistance to Penetration Attempts**		
5.9.1.1	The voting system SHALL be resistant to attempts to penetrate the system by any remote unauthorized entity.	5	Discovery Penetration Test Case
		11	Host Server Security Test Case
5.9.1.2	The voting system SHALL be configured to minimize ports, responses and information disclosure about the system while still providing appropriate functionality.	5	Discovery Penetration Test Case
		11	Host Server Security Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.9.1.3	The voting system SHALL provide no access, information or services to unauthorized entities.	5	Discovery Penetration Test Case
		1	Host Server Administration Test Case
5.9.1.4	All interfaces SHALL be penetration resistant including TCP/IP, wireless, and modems from any point in the system.	11	Host Server Security Test Case
5.9.1.5	The configuration and setup to attain penetration resistance SHALL be clearly and completely documented.	N/A	
5.9.2.1	The scope of penetration testing SHALL include all the voting system components. The scope of penetration testing includes but is not limited to the following: System server; Vote capture devices; Tabulation device; All items setup and configured per Technical Data Package (TDP) recommendations; Local wired and wireless networks; and 03/09/2011 Internet connections.	5	Discovery Penetration Test Case
5.9.2.2	Penetration testing SHALL be conducted on a voting system set up in a controlled lab environment. Setup and configuration SHALL be conducted in accordance with the TDP, and SHALL replicate the real world environment in which the voting system will be used.	N/A	
5.9.2.3	The penetration testing team SHALL conduct white box testing using manufacturer supplied documentation and voting system architecture information. Documentation includes the TDP and user documentation. The testing team SHALL have access to any relevant information regarding the voting system configuration. This includes, but is not limited to, network layout and Internet Protocol addresses for system devices and components. The testing team SHALL be provided any source code included in the TDP.	N/A	
5.9.2.04	Penetration testing seeks out vulnerabilities in the voting system that might be used to change the outcome of an election, interfere with voter ability to cast ballots, ballot counting, or compromise ballot secrecy. The penetration testing team SHALL prioritize testing efforts based on the following: a. Threat scenarios for the voting system under investigation; b. Remote attacks SHALL be prioritized over in-person attacks; c. Attacks with a large impact SHALL be prioritized over attacks with a more narrow impact; and d. Attacks that can change the outcome of an election SHALL be prioritized over attacks that compromise ballot secrecy or cause non-selective denial of service.	5	Discovery Penetration Test Case

[redacted]

REQUIREMENTS MATRIX

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
Section 5	**Security**		
5.1	**Access Control**		
	This section states requirements for the identification of authorized system users, processes and devices and the authentication or verification of those identities as a prerequisite to granting access to system processes and data. It also includes requirements to limit and control access to critical system components to protect system and data integrity, availability, confidentiality, and accountability. This section applies to all entities attempting to physically enter voting system facilities or to request services or data from the voting system.		
5.1.1	**Separation of Duties**		
5.1.1.1	The voting system SHALL allow the definition of personnel roles with segregated duties and responsibilities on critical processes to prevent a single person from compromising the integrity of the system.	1	Host Server Administration Test Case
5.1.1.2	The voting system SHALL ensure that only authorized roles, groups, or individuals have access to election data.	5	Discovery Penetration Test Case
5.1.1.3	The voting system SHALL require at least two persons from a predefined group for validating the election configuration information, accessing the cast vote records, and starting the tabulation process..	N/A	
5.1.2	**Voting System Access**		
	The voting system SHALL provide access control mechanisms designed to permit authorized access and to prevent unauthorized access to the system.		
5.1.2.1	The voting system SHALL identify and authenticate each person to whom access is granted, and the specific functions and data to which each person holds authorized access.	4	Normal Ballot Delivery Test Case
		1	Host Server Administration Test Case
		12	Voter Registration Request Test Case
5.1.2.2	The voting system SHALL allow the administrator group or role to configure permissions and functionality for each identity, group or role to include account and group/role creation, modification, and deletion.	1	Host Server Administration Test Case
5.1.2.3	The voting system's default access control permissions SHALL implement the least privileged role or group needed.	1	Host Server Administration Test Case
5.1.2.4	The voting system SHALL prevent a lower-privilege process from modifying a higher-privilege process.	1	Host Server Administration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.1.2.5	The voting system SHALL NOT require its execution as an operating system privileged account and SHALL NOT require the use of an operating system privileged account for its operation.	N/A	
5.1.2.6	The voting system SHALL log the identification of all personnel accessing or attempting to access the voting system to the system event log.	4	Normal Ballot Delivery Test Case
		1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
		12	Voter Registration Request Test Case
5.1.2.7	The *(voting system)* SHALL provide tools for monitoring access to the system. These tools SHALL provide specific users real time display of persons accessing the system as well as reports from logs.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.1.2.8	Vote capture device located at the remote voting location and the central server SHALL have the capability to restrict access to the voting system after a preset number of login failures. a. The lockout threshold SHALL be configurable by appropriate administrators/operators b. The voting system SHALL log the event c. The voting system SHALL immediately send a notification to appropriate administrators/operators of the event. d. The voting system SHALL provide a mechanism for the appropriate administrators/operators to reactivate the account after appropriate confirmation.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.1.2.9	The voting system SHALL log a notification when any account has been locked out.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.1.2.10	Authenticated sessions on critical processes SHALL have an inactivity time-out control that will require personnel re-authentication when reached. This time-out SHALL be implemented for administration and monitor consoles on all voting system devices.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.1.2.11	Authenticated sessions on critical processes SHALL have a screen-lock functionality that can be manually invoked.	N/A	
5.2	**Identification and Authentication**		
	Authentication mechanisms and their associated strength may vary from one voting system capability and architecture to another but all must meet the minimum requirement to maintain integrity and trust. It is important to consider a range of roles individuals may assume when operating different components in the voting system and each may require different authentication mechanisms. The requirements described in this section vary from role to role. For instance, a kiosk worker will have different identification and authentication characteristics than a voter. Also, for selected critical functions there may be cases where split knowledge or dual authorization is necessary to ensure security. This is especially relevant for critical cryptographic key management functions.		
5.2.1	**Authentication**		
5.2.1.1	Authentication mechanisms supported by the voting system SHALL support authentication strength of at least 1/1,000,000.	11	Host Server Security Test Case
5.2.1.2	The voting system SHALL authenticate users per the minimum authentication methods outlined below. Refer to document for the table layout: http://www.eac.gov/assets/1/AssetManager/UOCAVA_Pilot_Program_Requirments-03.24.10.pdf Table 5-1 Roles : Section 5 | Page 59	11	Host Server Security Test Case
5.2.1.3	The voting system SHALL provide multiple authentication methods to support multi-factor authentication.	1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
		12	Voter Registration Request Test Case
5.2.1.4	When private or secret authentication data is stored by the voting system, it SHALL be protected to ensure that the confidentiality and integrity of the data are not violated.	11	Host Server Security Test Case
5.2.1.5	The voting system SHALL provide a mechanism to reset a password if it is forgotten, in accordance with the system access/security policy.	1	Host Server Administration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.2.1.6	The voting system SHALL allow the administrator group or role to specify password strength for all accounts including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters per NIST 800-63 Electronic Authentication Guideline Standards.	1	Host Server Administration Test Case
5.2.1.7	The voting system SHALL enforce password histories and allow the administrator to configure the history length when passwords are stored by the system.	1	Host Server Administration Test Case
5.2.1.8	The voting system SHALL ensure that the user name is not used in the password.	1	Host Server Administration Test Case
5.2.1.9	The voting system SHALL provide a means to automatically expire passwords.	1	Host Server Administration Test Case
5.2.1.10	The voting system servers and vote capture devices SHALL identify and authenticate one another using NIST - approved cryptographic authentication methods at the 112 bits of security.	3	Cryptography Test Case
5.2.1.11	Remote voting location site Virtual Private Network (VPN) connections (i.e., vote capture devices) to voting servers SHALL be authenticated using strong mutual cryptographic authentication at the 112 bits of security.	N/A	
5.2.1.12	Message authentication SHALL be used for applications to protect the integrity of the message content using a schema with 112 bits of security.	11	Host Server Security Test Case
5.2.1.13	IPsec, SSL, or TLS and MAC mechanisms SHALL all be configured to be compliant with FIPS 140-2 using approved algorithm suites and protocols.	3	Cryptography Test Case
5.3	**Cryptography**		
	Cryptography serves several purposes in voting systems. They include: Confidentiality: where necessary the confidentiality of voting records can be provided by encryption; Authentication: data and programs can be authenticated by a digital signature or message authentication codes (MAC), or by comparison of the cryptographic hashes of programs or data with the reliably known hash values of the program or data. If the program or data are altered, then that alteration is detected when the signature or MAC is verified, or the hash on the data or program is compared to the known hash value. Typically the programs loaded on voting systems and the ballot definitions used by voting systems are verified by the systems, while systems apply digital signatures to authenticate the critical audit data that they output. For remote connections cryptographic user authentication mechanism SHALL be based on strong authentication methods; and		

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.3	**Cryptography (continued)**		
	Random number generation: random numbers are used for several purposes including the creation of cryptographic keys for cryptographic algorithms and methods to provide the services listed above, and as identifiers for voting records that can be used to identify or correlate the records without providing any information that could identify the voter.		
5.3.1	**General Cryptography Requirements**		
5.3.1.1	All cryptographic functionality SHALL be implemented using NIST-approved cryptographic algorithms/schemas, or use published and credible cryptographic algorithms/schemas/protocols.	3	Cryptography Test Case
5.3.1.2	Cryptographic algorithms and schemas SHALL be implemented with a security strength equivalent to at least 112 bits of security to protect sensitive voting information and election records.	3	Cryptography Test Case
5.3.1.3	Cryptography used to protect information in-transit over public telecommunication networks SHALL use NIST-approved algorithms and cipher suites. In addition the implementations of these algorithms SHALL be NIST-approved (Cryptographic Algorithm Validation Program).	3	Cryptography Test Case
5.3.2	**Key Management**		
	The following requirements apply to voting systems that generate cryptographic keys internally.		
5.3.2.1	Cryptographic keys generated by the voting system SHALL use a NIST-approved key generation method, or a published and credible key generation method.	3	Cryptography Test Case
5.3.2.2	Compromising the security of the key generation method (e.g., guessing the seed value to initialize the deterministic random number generator (RNG)) SHALL require as least as many operations as determining the value of the generated key.	N/T	
5.3.2.3	If a seed key is entered during the key generation process, entry of the key SHALL meet the key entry requirements in 5.3.3.1. If intermediate key generation values are output from the cryptographic module, the values SHALL be output either in encrypted form or under split knowledge procedures.	3	Cryptography Test Case
5.3.2.4	Cryptographic keys used to protect information in-transit over public telecommunication networks SHALL use NIST-approved key generation methods. If the approved key generation method requires input from a random number generator, then an approved (FIPS 140-2) random number generator SHALL be used.	3	Cryptography Test Case
5.3.2.5	Random number generators used to generate cryptographic keys SHALL implement one or more health tests that provide assurance that the random number generator continues to operate as intended (e.g., the entropy source is not stuck).	3	Cryptography Test Case
5.3.3	**Key Establishment**		
	Key establishment may be performed by automated methods (e.g., use of a public key algorithm), manual methods (use of a manually transported key loading device), or a combination of automated and manual methods.		

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.3.3.1	Secret and private keys established using automated methods SHALL be entered into and output from a voting system in encrypted form. Secret and private keys established using manual methods may be entered into or output from a system in plaintext form.	3	Cryptography Test Case
5.3.4.1	Cryptographic keys stored within the voting system SHALL NOT be stored in plaintext. Keys stored outside the voting system SHALL be protected from disclosure or modification.	3	Cryptography Test Case
5.3.4.2	The voting system SHALL provide methods to zeroize all plaintext secret and private cryptographic keys within the system.	3	Cryptography Test Case
5.3.4.3	The voting system SHALL support the capability to reset cryptographic keys to new values.	3	Cryptography Test Case
5.4	**Voting System Integrity Management**		
	This section addresses the secure deployment and operation of the voting system, including the protection of removable media and protection against malicious software.		
5.4.1	**Protecting the Integrity of the Voting System**		
5.4.1.1	The integrity and authenticity of each individual cast vote SHALL be protected from any tampering or modification during transmission.	N/A	
5.4.1.2	The integrity and authenticity of each individual cast vote SHALL be preserved by means of a digital signature during storage.	N/A	
5.4.1.3	Cast vote data SHALL NOT be permanently stored on the vote capture device.	4	Normal Ballot Delivery Test Case
5.4.1.4	The integrity and authenticity of the electronic ballot box SHALL be protected by means of a digital signature.	N/A	
5.4.1.5	The voting system SHALL use malware detection software to protect against known malware that targets the operating system, services, and applications.	5	Discovery Penetration Test Case
5.4.1.6	The voting system SHALL provide a mechanism for updating malware detection signatures.	5	Discovery Penetration Test Case
5.4.1.7	The voting system SHALL provide the capability for kiosk workers to validate the software used on the vote capture devices as part of the daily initiation of kiosk operations.	N/A	
5.5	**Communications Security**		
	This section provides requirements for communications security. These requirements address ensuring the integrity of transmitted information and protecting the voting system from external communications-based threats.		

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.5.1	**Data Transmission Security**		
5.5.1.1	Voting systems that transmit data over communications links SHALL provide integrity protection for data in transit through the generation of integrity data (digital signatures and/or message authentication codes) for outbound traffic and verification of the integrity data for inbound traffic.	3	Cryptography Test Case
5.5.1.2	Voting systems SHALL use at a minimum TLS 1.0, SSL 3.1 or equivalent protocols, including all updates to both protocols and implementations as of the date of the submission (e.g., RFC 5746 for TLS 1.0).	11	Host Server Security Test Case
5.5.1.3	Voting systems deploying VPNs SHALL configure them to only allow FIPS-compliant cryptographic algorithms and cipher suites.	N/A	
5.5.1.4	Each communicating device SHALL have a unique system identifier.	11	Host Server Security Test Case
5.5.1.5	Each device SHALL mutually strongly authenticate using the system identifier before additional network data packets are processed.	11	Host Server Security Test Case
5.5.1.6	Data transmission SHALL preserve the secrecy of voters' ballot selections and SHALL prevent the violation of ballot secrecy and integrity.	5	Discovery Penetration Test Case
5.5.2	**External Threats**		
	Voting systems SHALL implement protections against external threats to which the system may be susceptible.	5	Discovery Penetration Test Case
5.5.2.1	Voting system components SHALL have the ability to enable or disable physical network interfaces.	1	Host Server Administration Test Case
5.5.2.2	The number of active ports and associated network services and protocols SHALL be restricted to the minimum required for the voting system to function.	11	Host Server Security Test Case
5.5.2.3	The voting system SHALL block all network connections that are not over a mutually authenticated channel.	11	Host Server Security Test Case
5.6	**Logging**		
5.6.1	**Log Management**		
5.6.1.1	The voting system SHALL implement default settings for secure log management activities, including log generation, transmission, storage, analysis, and disposal.	1	Host Server Administration Test Case
5.6.1.2	Logs SHALL only be accessible to authorized roles.	1	Host Server Administration Test Case
5.6.1.3	The voting system SHALL restrict log access to append-only for privileged logging processes and read-only for authorized roles.	1	Host Server Administration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.6.1.4	The voting system SHALL log logging failures, log clearing, and log rotation.	1	Host Server Administration Test Case
5.6.1.5	The voting system SHALL store log data in a publicly documented format, such as XML, or include a utility to export log data into a publicly documented format.	1	Host Server Administration Test Case
5.6.1.6	The voting system SHALL ensure that each jurisdiction's event logs and each component's logs are separable from each other.	N/A	
5.6.1.7	The voting system SHALL include an application or program to view, analyze, and search event logs.	1	Host Server Administration Test Case
5.6.1.8	All logs SHALL be preserved in a useable manner prior to voting system decommissioning.	1	Host Server Administration Test Case
5.6.1.9	Logs SHALL NOT contain any data that could violate the privacy of the voter's identity.	4	Normal Ballot Delivery Test Case
5.6.1.10	Timekeeping mechanisms SHALL generate time and date values, including hours, minutes, and seconds.	4	Normal Ballot Delivery Test Case
		1	Host Server Administration Test Case
5.6.1.11	The precision of the timekeeping mechanism SHALL be able to distinguish and properly order all log events.	4	Normal Ballot Delivery Test Case
5.6.1.12	Only the system administrator SHALL be permitted to set the system clock.	NA	
5.6.2	**Communication Logging**		
5.6.2.1	All communications actions SHALL be logged.	3	Cryptography Test Case
		5	Discovery Penetration Test Case
		4	Normal Ballot Delivery Test Case
		1	Host Server Administration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.6.2.2	The communications log SHALL contain at least the following entries: Times when the communications are activated and deactivated; Services accessed; Identification of the device which data was transmitted to or received from; Identification of authorized entity; and Successful and unsuccessful attempts to access communications or services.	5	Discovery Penetration Test Case
		4	Normal Ballot Delivery Test Case
5.6.3	**System Event Logging**		
	This section describes requirements for the voting system to perform event logging for system maintenance troubleshooting, recording the history of system activity, and detecting unauthorized or malicious activity. The operating system, and/or applications software may perform the actual event logging. There may be multiple logs in use for any system component.		
5.6.3.1	The voting system SHALL log the following data for each event: a. System ID; b. Unique event ID and/or type; c. Timestamp; d. Success or failure of event, if applicable; e. User ID triggering the event, if applicable; and f. Jurisdiction, if applicable.	7	Recovery From Hardware Error Test Case
		4	Normal Ballot Delivery Test Case
		1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.6.3.2	All critical events SHALL be recorded in the system event log.	5	Discovery Penetration Test Case
		4	Normal Ballot Delivery Test Case
		7	Recovery From Hardware Error Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.6.3.3	At a minimum the voting system SHALL log the events described in the table below. NOTE: See "Table 5-2 System Events" in document - page 71	4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case
		3	Cryptography Test Case
		1	Host Server Administration Test Case
		7	Recovery From Hardware Error Test Case
5.7	**Incident Response**		
5.7.1	**Incident Response Support**		
5.7.1.1	Manufacturers SHALL document what types of system operations or security events (e.g., failure of critical component, detection of malicious code, unauthorized access to restricted data) are classified as critical.	N/A	
5.7.1.2	An alarm that notifies appropriate personnel SHALL be generated on the vote capture device, system server, or tabulation device, depending upon which device has the error, if a critical event is detected.	N/A	
5.8	**Physical and Environmental Security**		
5.8.1	**Physical Access**		
5.8.1.1	Any unauthorized physical access SHALL leave physical evidence that an unauthorized event has taken place.	N/A	
5.8.2.1	The voting system SHALL disable physical ports and access points that are not essential to voting operations, testing, and auditing.	11	Host Server Security Test Case
5.8.3.1	If a physical connection between the vote capture device and a component is broken, the affected vote capture device port SHALL be automatically disabled.	N/A	
5.8.3.2	The voting system SHALL produce a visual alarm if a connected component is physically disconnected.	N/A	
5.8.3.3	An event log entry that identifies the name of the affected device SHALL be generated if a vote capture device component is disconnected.	7	Recovery From Hardware Error Test Case
5.8.3.4	Disabled ports SHALL only be re-enabled by authorized administrators.	1	Host Server Administration Test Case
5.8.3.5	Vote capture devices SHALL be designed with the capability to restrict physical access to voting device ports that accommodate removable media with the exception of ports used to activate a voting session.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.8.3.6	Vote capture devices SHALL be designed to give a physical indication of tampering or unauthorized access to ports and all other access points, if used as described in the manufacturer's documentation.	N/A	
5.8.3.7	Vote capture devices SHALL be designed such that physical ports can be manually disabled by an authorized administrator.	N/A	
5.8.4	**Door Cover and Panel Security**		
5.8.4.1	Access points such as covers and panels SHALL be secured by locks or tamper evident or tamper resistant countermeasures and SHALL be implemented so that kiosk workers can monitor access to vote capture device components through these points.	N/A	
5.8.5	**Secure Paper Record Receptacle**		
	If the voting system provides paper record containers then they SHALL be designed such that any unauthorized physical access results in physical evidence that an unauthorized event has taken place.	N/A	
5.8.6	**Secure Physical Lock and Key**		
5.8.6.1	Voting equipment SHALL be designed with countermeasures that provide physical indication that unauthorized attempts have been made to access locks installed for security purposes.	N/A	
5.8.6.2	Manufacturers SHALL provide locking systems for securing vote capture devices that can make use of keys that are unique to each owner.	N/A	
5.8.7	**Media Protection**		
	These requirements apply to all media, both paper and digital, that contain personal privacy related data or other protected or sensitive types of information.		
5.8.7.1	The voting system SHALL meet the following requirements: a. All paper records (including rejected ones) printed at the kiosk locations SHALL be deposited in a secure container; b. Vote capture device hardware, software and sensitive information (e.g., electoral roll) SHALL be physically protected to prevent unauthorized modification or disclosure; and c. Vote capture device hardware components, peripherals and removable media SHALL be identified and registered by means of a unique serial number or other identifier.	N/A	
5.9	**Penetration Resistance**		
5.9.1	**Resistance to Penetration Attempts**		
5.9.1.1	The voting system SHALL be resistant to attempts to penetrate the system by any remote unauthorized entity.	5	Discovery Penetration Test Case
		11	Host Server Security Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.9.1.2	The voting system SHALL be configured to minimize ports, responses and information disclosure about the system while still providing appropriate functionality.	5	Discovery Penetration Test Case
		11	Host Server Security Test Case
5.9.1.3	The voting system SHALL provide no access, information or services to unauthorized entities.	5	Discovery Penetration Test Case
		1	Host Server Administration Test Case
5.9.1.4	All interfaces SHALL be penetration resistant including TCP/IP, wireless, and modems from any point in the system.	11	Host Server Security Test Case
5.9.1.5	The configuration and setup to attain penetration resistance SHALL be clearly and completely documented.	N/A	
5.9.2.1	The scope of penetration testing SHALL include all the voting system components. The scope of penetration testing includes but is not limited to the following: System server; Vote capture devices; Tabulation device; All items setup and configured per Technical Data Package (TDP) recommendations; Local wired and wireless networks; and 03/09/2011 Internet connections.	5	Discovery Penetration Test Case
5.9.2.2	Penetration testing SHALL be conducted on a voting system set up in a controlled lab environment. Setup and configuration SHALL be conducted in accordance with the TDP, and SHALL replicate the real world environment in which the voting system will be used.	N/A	
5.9.2.3	The penetration testing team SHALL conduct white box testing using manufacturer supplied documentation and voting system architecture information. Documentation includes the TDP and user documentation. The testing team SHALL have access to any relevant information regarding the voting system configuration. This includes, but is not limited to, network layout and Internet Protocol addresses for system devices and components. The testing team SHALL be provided any source code included in the TDP.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.9.2.04	Penetration testing seeks out vulnerabilities in the voting system that might be used to change the outcome of an election, interfere with voter ability to cast ballots, ballot counting, or compromise ballot secrecy. The penetration testing team SHALL prioritize testing efforts based on the following: a. Threat scenarios for the voting system under investigation; b. Remote attacks SHALL be prioritized over in-person attacks; c. Attacks with a large impact SHALL be prioritized over attacks with a more narrow impact; and d. Attacks that can change the outcome of an election SHALL be prioritized over attacks that compromise ballot secrecy or cause non-selective denial of service.	5	Discovery Penetration Test Case

[redacted]

REQUIREMENTS MATRIX

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
Section 5	**Security**		
5.1	**Access Control**		
	This section states requirements for the identification of authorized system users, processes and devices and the authentication or verification of those identities as a prerequisite to granting access to system processes and data. It also includes requirements to limit and control access to critical system components to protect system and data integrity, availability, confidentiality, and accountability. This section applies to all entities attempting to physically enter voting system facilities or to request services or data from the voting system.		
5.1.1	**Separation of Duties**		
5.1.1.1	The voting system SHALL allow the definition of personnel roles with segregated duties and responsibilities on critical processes to prevent a single person from compromising the integrity of the system.	1	Host Server Administration Test Case
5.1.1.2	The voting system SHALL ensure that only authorized roles, groups, or individuals have access to election data.	1	Host Server Administration Test Case
5.1.1.3	The voting system SHALL require at least two persons from a predefined group for validating the election configuration information, accessing the cast vote records, and starting the tabulation process..	N/A	
5.1.2	**Voting System Access**		
	The voting system SHALL provide access control mechanisms designed to permit authorized access and to prevent unauthorized access to the system.	5	Discovery Penetration Test Case
		1	Host Server Administration Test Case
5.1.2.1	The voting system SHALL identify and authenticate each person to whom access is granted, and the specific functions and data to which each person holds authorized access.	1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
5.1.2.2	The voting system SHALL allow the administrator group or role to configure permissions and functionality for each identity, group or role to include account and group/role creation, modification, and deletion.	1	Host Server Administration Test Case
5.1.2.3	The voting system's default access control permissions SHALL implement the least privileged role or group needed.	1	Host Server Administration Test Case
5.1.2.4	The voting system SHALL prevent a lower-privilege process from modifying a higher-privilege process.	1	Host Server Administration Test Case
5.1.2.5	The voting system SHALL NOT require its execution as an operating system privileged account and SHALL NOT require the use of an operating system privileged account for its operation.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.1.2.6	The voting system SHALL log the identification of all personnel accessing or attempting to access the voting system to the system event log.	1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case
5.1.2.7	The *(voting system)* SHALL provide tools for monitoring access to the system. These tools SHALL provide specific users real time display of persons accessing the system as well as reports from logs.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.1.2.8	Vote capture device located at the remote voting location and the central server SHALL have the capability to restrict access to the voting system after a preset number of login failures. a. The lockout threshold SHALL be configurable by appropriate administrators/operators b. The voting system SHALL log the event c. The voting system SHALL immediately send a notification to appropriate administrators/operators of the event. d. The voting system SHALL provide a mechanism for the appropriate administrators/operators to reactivate the account after appropriate confirmation.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.1.2.9	The voting system SHALL log a notification when any account has been locked out.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.1.2.10	Authenticated sessions on critical processes SHALL have an inactivity time-out control that will require personnel re-authentication when reached. This time-out SHALL be implemented for administration and monitor consoles on all voting system devices.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.1.2.11	Authenticated sessions on critical processes SHALL have a screen-lock functionality that can be manually invoked.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.2	**Identification and Authentication**		
	Authentication mechanisms and their associated strength may vary from one voting system capability and architecture to another but all must meet the minimum requirement to maintain integrity and trust. It is important to consider a range of roles individuals may assume when operating different components in the voting system and each may require different authentication mechanisms. The requirements described in this section vary from role to role. For instance, a kiosk worker will have different identification and authentication characteristics than a voter. Also, for selected critical functions there may be cases where split knowledge or dual authorization is necessary to ensure security. This is especially relevant for critical cryptographic key management functions.		
5.2.1	**Authentication**		
5.2.1.1	Authentication mechanisms supported by the voting system SHALL support authentication strength of at least 1/1,000,000.	11	Host Server Security Test Case
5.2.1.2	The voting system SHALL authenticate users per the minimum authentication methods outlined below. Refer to document for the table layout: http://www.eac.gov/assets/1/AssetManager/UOCAVA_Pilot_Program_Requirments-03.24.10.pdf Table 5-1 Roles : Section 5 | Page 59	11	Host Server Security Test Case
5.2.1.3	The voting system SHALL provide multiple authentication methods to support multi-factor authentication.	4	Normal Ballot Delivery Test Case
		11	Host Server Security Test Case
5.2.1.4	When private or secret authentication data is stored by the voting system, it SHALL be protected to ensure that the confidentiality and integrity of the data are not violated.	11	Host Server Security Test Case
5.2.1.5	The voting system SHALL provide a mechanism to reset a password if it is forgotten, in accordance with the system access/security policy.	1	Host Server Administration Test Case
5.2.1.6	The voting system SHALL allow the administrator group or role to specify password strength for all accounts including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters per NIST 800-63 Electronic Authentication Guideline Standards.	1	Host Server Administration Test Case
5.2.1.7	The voting system SHALL enforce password histories and allow the administrator to configure the history length when passwords are stored by the system.	1	Host Server Administration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.2.1.8	The voting system SHALL ensure that the user name is not used in the password.	1	Host Server Administration Test Case
5.2.1.9	The voting system SHALL provide a means to automatically expire passwords.	1	Host Server Administration Test Case
5.2.1.10	The voting system servers and vote capture devices SHALL identify and authenticate one another using NIST - approved cryptographic authentication methods at the 112 bits of security.	3	Cryptography Test Case
5.2.1.11	Remote voting location site Virtual Private Network (VPN) connections (i.e., vote capture devices) to voting servers SHALL be authenticated using strong mutual cryptographic authentication at the 112 bits of security.	N/A	
5.2.1.12	Message authentication SHALL be used for applications to protect the integrity of the message content using a schema with 112 bits of security.	11	Host Server Security Test Case
5.2.1.13	IPsec, SSL, or TLS and MAC mechanisms SHALL all be configured to be compliant with FIPS 140-2 using approved algorithm suites and protocols.	3	Cryptography Test Case
5.3	**Cryptography**		
	Cryptography serves several purposes in voting systems. They include: Confidentiality: where necessary the confidentiality of voting records can be provided by encryption; Authentication: data and programs can be authenticated by a digital signature or message authentication codes (MAC), or by comparison of the cryptographic hashes of programs or data with the reliably known hash values of the program or data. If the program or data are altered, then that alteration is detected when the signature or MAC is verified, or the hash on the data or program is compared to the known hash value. Typically the programs loaded on voting systems and the ballot definitions used by voting systems are verified by the systems, while systems apply digital signatures to authenticate the critical audit data that they output. For remote connections cryptographic user authentication mechanism SHALL be based on strong authentication methods; and Random number generation: random numbers are used for several purposes including the creation of cryptographic keys for cryptographic algorithms and methods to provide the services listed above, and as identifiers for voting records that can be used to identify or correlate the records without providing any information that could identify the voter.		
5.3.1	**General Cryptography Requirements**		
5.3.1.1	All cryptographic functionality SHALL be implemented using NIST-approved cryptographic algorithms/schemas, or use published and credible cryptographic algorithms/schemas/protocols.	3	Cryptography Test Case
5.3.1.2	Cryptographic algorithms and schemas SHALL be implemented with a security strength equivalent to at least 112 bits of security to protect sensitive voting information and election records.	3	Cryptography Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.3.1.3	Cryptography used to protect information in-transit over public telecommunication networks SHALL use NIST-approved algorithms and cipher suites. In addition the implementations of these algorithms SHALL be NIST-approved (Cryptographic Algorithm Validation Program).	3	Cryptography Test Case
5.3.2	**Key Management**		
	The following requirements apply to voting systems that generate cryptographic keys internally.		
5.3.2.1	Cryptographic keys generated by the voting system SHALL use a NIST-approved key generation method, or a published and credible key generation method.	3	Cryptography Test Case
5.3.2.2	Compromising the security of the key generation method (e.g., guessing the seed value to initialize the deterministic random number generator (RNG)) SHALL require as least as many operations as determining the value of the generated key.	N/T	
5.3.2.3	If a seed key is entered during the key generation process, entry of the key SHALL meet the key entry requirements in 5.3.3.1. If intermediate key generation values are output from the cryptographic module, the values SHALL be output either in encrypted form or under split knowledge procedures.	3	Cryptography Test Case
5.3.2.4	Cryptographic keys used to protect information in-transit over public telecommunication networks SHALL use NIST-approved key generation methods. If the approved key generation method requires input from a random number generator, then an approved (FIPS 140-2) random number generator SHALL be used.	3	Cryptography Test Case
5.3.2.5	Random number generators used to generate cryptographic keys SHALL implement one or more health tests that provide assurance that the random number generator continues to operate as intended (e.g., the entropy source is not stuck).	3	Cryptography Test Case
5.3.3	**Key Establishment**		
	Key establishment may be performed by automated methods (e.g., use of a public key algorithm), manual methods (use of a manually transported key loading device), or a combination of automated and manual methods.		
5.3.3.1	Secret and private keys established using automated methods SHALL be entered into and output from a voting system in encrypted form. Secret and private keys established using manual methods may be entered into or output from a system in plaintext form.	3	Cryptography Test Case
5.3.4.1	Cryptographic keys stored within the voting system SHALL NOT be stored in plaintext. Keys stored outside the voting system SHALL be protected from disclosure or modification.	3	Cryptography Test Case
5.3.4.2	The voting system SHALL provide methods to zeroize all plaintext secret and private cryptographic keys within the system.	3	Cryptography Test Case
5.3.4.3	The voting system SHALL support the capability to reset cryptographic keys to new values.	3	Cryptography Test Case
5.4	**Voting System Integrity Management**		
	This section addresses the secure deployment and operation of the voting system, including the protection of removable media and protection against malicious software.		

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.4.1	**Protecting the Integrity of the Voting System**		
5.4.1.1	The integrity and authenticity of each individual cast vote SHALL be protected from any tampering or modification during transmission.	N/A	
5.4.1.2	The integrity and authenticity of each individual cast vote SHALL be preserved by means of a digital signature during storage.	N/A	
5.4.1.3	Cast vote data SHALL NOT be permanently stored on the vote capture device.	4	Normal Ballot Delivery Test Case
5.4.1.4	The integrity and authenticity of the electronic ballot box SHALL be protected by means of a digital signature.	N/A	
5.4.1.5	The voting system SHALL use malware detection software to protect against known malware that targets the operating system, services, and applications.	5	Discovery Penetration Test Case
5.4.1.6	The voting system SHALL provide a mechanism for updating malware detection signatures.	5	Discovery Penetration Test Case
5.4.1.7	The voting system SHALL provide the capability for kiosk workers to validate the software used on the vote capture devices as part of the daily initiation of kiosk operations.	N/A	
5.5	**Communications Security**		
	This section provides requirements for communications security. These requirements address ensuring the integrity of transmitted information and protecting the voting system from external communications-based threats.		
5.5.1	**Data Transmission Security**		
5.5.1.1	Voting systems that transmit data over communications links SHALL provide integrity protection for data in transit through the generation of integrity data (digital signatures and/or message authentication codes) for outbound traffic and verification of the integrity data for inbound traffic.	11	Host Server Security Test Case
5.5.1.2	Voting systems SHALL use at a minimum TLS 1.0, SSL 3.1 or equivalent protocols, including all updates to both protocols and implementations as of the date of the submission (e.g., RFC 5746 for TLS 1.0).	3	Cryptography Test Case
5.5.1.3	Voting systems deploying VPNs SHALL configure them to only allow FIPS-compliant cryptographic algorithms and cipher suites.	N/A	
5.5.1.4	Each communicating device SHALL have a unique system identifier.	11	Host Server Security Test Case
5.5.1.5	Each device SHALL mutually strongly authenticate using the system identifier before additional network data packets are processed.	11	Host Server Security Test Case
5.5.1.6	Data transmission SHALL preserve the secrecy of voters' ballot selections and SHALL prevent the violation of ballot secrecy and integrity.	5	Discovery Penetration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.5.2	**External Threats**		
	Voting systems SHALL implement protections against external threats to which the system may be susceptible.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.5.2.1	Voting system components SHALL have the ability to enable or disable physical network interfaces.	1	Host Server Administration Test Case
5.5.2.2	The number of active ports and associated network services and protocols SHALL be restricted to the minimum required for the voting system to function.	11	Host Server Security Test Case
5.5.2.3	The voting system SHALL block all network connections that are not over a mutually authenticated channel.	11	Host Server Security Test Case
5.6	**Logging**		
5.6.1	**Log Management**		
5.6.1.1	The voting system SHALL implement default settings for secure log management activities, including log generation, transmission, storage, analysis, and disposal.	1	Host Server Administration Test Case
5.6.1.2	Logs SHALL only be accessible to authorized roles.	1	Host Server Administration Test Case
5.6.1.3	The voting system SHALL restrict log access to append-only for privileged logging processes and read-only for authorized roles.	1	Host Server Administration Test Case
5.6.1.4	The voting system SHALL log logging failures, log clearing, and log rotation.	1	Host Server Administration Test Case
5.6.1.5	The voting system SHALL store log data in a publicly documented format, such as XML, or include a utility to export log data into a publicly documented format.	1	Host Server Administration Test Case
5.6.1.6	The voting system SHALL ensure that each jurisdiction's event logs and each component's logs are separable from each other.	N/A	
5.6.1.7	The voting system SHALL include an application or program to view, analyze, and search event logs.	1	Host Server Administration Test Case
5.6.1.8	All logs SHALL be preserved in a useable manner prior to voting system decommissioning.	1	Host Server Administration Test Case
5.6.1.9	Logs SHALL NOT contain any data that could violate the privacy of the voter's identity.	4	Normal Ballot Delivery Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.6.1.10	Timekeeping mechanisms SHALL generate time and date values, including hours, minutes, and seconds.	4	Normal Ballot Delivery Test Case
		1	Host Server Administration Test Case
		10	Local Ballot Delivery Test Case
5.6.1.11	The precision of the timekeeping mechanism SHALL be able to distinguish and properly order all log events.	4	Normal Ballot Delivery Test Case
5.6.1.12	Only the system administrator SHALL be permitted to set the system clock.	N/A	
5.6.2	**Communication Logging**		
5.6.2.1	All communications actions SHALL be logged.	4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case
		1	Host Server Administration Test Case
5.6.2.2	The communications log SHALL contain at least the following entries: Times when the communications are activated and deactivated; Services accessed; Identification of the device which data was transmitted to or received from; Identification of authorized entity; and Successful and unsuccessful attempts to access communications or services.	4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case
5.6.3	**System Event Logging**		
	This section describes requirements for the voting system to perform event logging for system maintenance troubleshooting, recording the history of system activity, and detecting unauthorized or malicious activity. The operating system, and/or applications software may perform the actual event logging. There may be multiple logs in use for any system component.		

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.6.3.1	The voting system SHALL log the following data for each event: a. System ID; b. Unique event ID and/or type; c. Timestamp; d. Success or failure of event, if applicable; e. User ID triggering the event, if applicable; and f. Jurisdiction, if applicable.	1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
		7	Recovery form hardware error Test Case
		5	Discovery Penetration Test Case
5.6.3.2	All critical events SHALL be recorded in the system event log.	5	Discovery Penetration Test Case
		4	Normal Ballot Delivery Test Case
		7	Recovery form hardware error Test Case
5.6.3.3	At a minimum the voting system SHALL log the events described in the table below. NOTE: See "Table 5-2 System Events" in document - page 71	1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case
		7	Recovery form hardware error Test Case
5.7	**Incident Response**		
5.7.1	**Incident Response Support**		
5.7.1.1	Manufacturers SHALL document what types of system operations or security events (e.g., failure of critical component, detection of malicious code, unauthorized access to restricted data) are classified as critical.	N/A	
5.7.1.2	An alarm that notifies appropriate personnel SHALL be generated on the vote capture device, system server, or tabulation device, depending upon which device has the error, if a critical event is detected.	N/A	
5.8	**Physical and Environmental Security**		
5.8.1	**Physical Access**		
5.8.1.1	Any unauthorized physical access SHALL leave physical evidence that an unauthorized event has taken place.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.8.2.1	The voting system SHALL disable physical ports and access points that are not essential to voting operations, testing, and auditing.	11	Host Server Security Test Case
5.8.3.1	If a physical connection between the vote capture device and a component is broken, the affected vote capture device port SHALL be automatically disabled.	N/A	
5.8.3.2	The voting system SHALL produce a visual alarm if a connected component is physically disconnected.	N/A	
5.8.3.3	An event log entry that identifies the name of the affected device SHALL be generated if a vote capture device component is disconnected.	7	Recovery form hardware error Test Case
5.8.3.4	Disabled ports SHALL only be re-enabled by authorized administrators.	1	Host Server Administration Test Case
5.8.3.5	Vote capture devices SHALL be designed with the capability to restrict physical access to voting device ports that accommodate removable media with the exception of ports used to activate a voting session.	N/A	
5.8.3.6	Vote capture devices SHALL be designed to give a physical indication of tampering or unauthorized access to ports and all other access points, if used as described in the manufacturer's documentation.	N/A	
5.8.3.7	Vote capture devices SHALL be designed such that physical ports can be manually disabled by an authorized administrator.	N/A	
5.8.4	**Door Cover and Panel Security**		
5.8.4.1	Access points such as covers and panels SHALL be secured by locks or tamper evident or tamper resistant countermeasures and SHALL be implemented so that kiosk workers can monitor access to vote capture device components through these points.	N/A	
5.8.5	**Secure Paper Record Receptacle**		
	If the voting system provides paper record containers then they SHALL be designed such that any unauthorized physical access results in physical evidence that an unauthorized event has taken place.	N/A	
5.8.6	**Secure Physical Lock and Key**		
5.8.6.1	Voting equipment SHALL be designed with countermeasures that provide physical indication that unauthorized attempts have been made to access locks installed for security purposes.	N/A	
5.8.6.2	Manufacturers SHALL provide locking systems for securing vote capture devices that can make use of keys that are unique to each owner.	N/A	
5.8.7	**Media Protection**		
	These requirements apply to all media, both paper and digital, that contain personal privacy related data or other protected or sensitive types of information.		

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.8.7.1	The voting system SHALL meet the following requirements: a. All paper records (including rejected ones) printed at the kiosk locations SHALL be deposited in a secure container; b. Vote capture device hardware, software and sensitive information (e.g., electoral roll) SHALL be physically protected to prevent unauthorized modification or disclosure; and c. Vote capture device hardware components, peripherals and removable media SHALL be identified and registered by means of a unique serial number or other identifier.	N/A	
5.9	**Penetration Resistance**		
5.9.1	**Resistance to Penetration Attempts**		
5.9.1.1	The voting system SHALL be resistant to attempts to penetrate the system by any remote unauthorized entity.	5	Discovery Penetration Test Case
		11	Host Server Security Test Case
5.9.1.2	The voting system SHALL be configured to minimize ports, responses and information disclosure about the system while still providing appropriate functionality.	5	Discovery Penetration Test Case
		11	Host Server Security Test Case
5.9.1.3	The voting system SHALL provide no access, information or services to unauthorized entities.	5	Discovery Penetration Test Case
		1	Host Server Administration Test Case
5.9.1.4	All interfaces SHALL be penetration resistant including TCP/IP, wireless, and modems from any point in the system.	11	Host Server Security Test Case
5.9.1.5	The configuration and setup to attain penetration resistance SHALL be clearly and completely documented.	N/A	
5.9.2.1	The scope of penetration testing SHALL include all the voting system components. The scope of penetration testing includes but is not limited to the following: System server; Vote capture devices; Tabulation device; All items setup and configured per Technical Data Package (TDP) recommendations; Local wired and wireless networks; and03/09/2011 Internet connections.	5	Discovery Penetration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.9.2.2	Penetration testing SHALL be conducted on a voting system set up in a controlled lab environment. Setup and configuration SHALL be conducted in accordance with the TDP, and SHALL replicate the real world environment in which the voting system will be used.	N/A	
5.9.2.3	The penetration testing team SHALL conduct white box testing using manufacturer supplied documentation and voting system architecture information. Documentation includes the TDP and user documentation. The testing team SHALL have access to any relevant information regarding the voting system configuration. This includes, but is not limited to, network layout and Internet Protocol addresses for system devices and components. The testing team SHALL be provided any source code included in the TDP.	N/A	
5.9.2.04	Penetration testing seeks out vulnerabilities in the voting system that might be used to change the outcome of an election, interfere with voter ability to cast ballots, ballot counting, or compromise ballot secrecy. The penetration testing team SHALL prioritize testing efforts based on the following: a. Threat scenarios for the voting system under investigation; b. Remote attacks SHALL be prioritized over in-person attacks; c. Attacks with a large impact SHALL be prioritized over attacks with a more narrow impact; and d. Attacks that can change the outcome of an election SHALL be prioritized over attacks that compromise ballot secrecy or cause non-selective denial of service.	5	Discovery Penetration Test Case

[redacted]

REQUIREMENTS MATRIX

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
Section 5	**Security**		
5.1	**Access Control**		
	This section states requirements for the identification of authorized system users, processes and devices and the authentication or verification of those identities as a prerequisite to granting access to system processes and data. It also includes requirements to limit and control access to critical system components to protect system and data integrity, availability, confidentiality, and accountability. This section applies to all entities attempting to physically enter voting system facilities or to request services or data from the voting system.		
5.1.1	**Separation of Duties**		
5.1.1.1	The voting system SHALL allow the definition of personnel roles with segregated duties and responsibilities on critical processes to prevent a single person from compromising the integrity of the system.	1	Host Server Administration Test Case
5.1.1.2	The voting system SHALL ensure that only authorized roles, groups, or individuals have access to election data.	1	Host Server Administration Test Case
5.1.1.3	The voting system SHALL require at least two persons from a predefined group for validating the election configuration information, accessing the cast vote records, and starting the tabulation process..	N/A	
5.1.2	**Voting System Access**		
	The voting system SHALL provide access control mechanisms designed to permit authorized access and to prevent unauthorized access to the system.	5	Discovery Penetration Test Case
		1	Host Server Administration Test Case
5.1.2.1	The voting system SHALL identify and authenticate each person to whom access is granted, and the specific functions and data to which each person holds authorized access.	1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
5.1.2.2	The voting system SHALL allow the administrator group or role to configure permissions and functionality for each identity, group or role to include account and group/role creation, modification, and deletion.	1	Host Server Administration Test Case
5.1.2.3	The voting system's default access control permissions SHALL implement the least privileged role or group needed.	1	Host Server Administration Test Case
5.1.2.4	The voting system SHALL prevent a lower-privilege process from modifying a higher-privilege process.	1	Host Server Administration Test Case
5.1.2.5	The voting system SHALL NOT require its execution as an operating system privileged account and SHALL NOT require the use of an operating system privileged account for its operation.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.1.2.6	The voting system SHALL log the identification of all personnel accessing or attempting to access the voting system to the system event lo g.	7	Recovery form hardware error Test Case
		1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case
5.1.2.7	The *(voting system)* SHALL provide tools for monitoring access to the system. These tools SHALL provide specific users real time display of persons accessing the system as well as reports from logs.	1	Host Server Administration Test Case
5.1.2.8	Vote capture device located at the remote voting location and the central server SHALL have the capability to restrict access to the voting system after a preset number of login failures. a. The lockout threshold SHALL be configurable by appropriate administrators/operators b. The voting system SHALL log the event c. The voting system SHALL immediately send a notification to appropriate administrators/operators of the event. d. The voting system SHALL provide a mechanism for the appropriate administrators/operators to reactivate the account after appropriate confirmation.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.1.2.9	The voting system SHALL log a notification when any account has been locked out.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.1.2.10	Authenticated sessions on critical processes SHALL have an inactivity time-out control that will require personnel re-authentication when reached. This time-out SHALL be implemented for administration and monitor consoles on all voting system devices.	1	Host Server Administration Test Case
		5	Discovery Penetration Test Case
5.1.2.11	Authenticated sessions on critical processes SHALL have a screen-lock functionality that can be manually invoked.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.2	**Identification and Authentication**		
	Authentication mechanisms and their associated strength may vary from one voting system capability and architecture to another but all must meet the minimum requirement to maintain integrity and trust. It is important to consider a range of roles individuals may assume when operating different components in the voting system and each may require different authentication mechanisms. The requirements described in this section vary from role to role. For instance, a kiosk worker will have different identification and authentication characteristics than a voter. Also, for selected critical functions there may be cases where split knowledge or dual authorization is necessary to ensure security. This is especially relevant for critical cryptographic key management functions.		
5.2.1	**Authentication**		
5.2.1.1	Authentication mechanisms supported by the voting system SHALL support authentication strength of at least 1/1,000,000.	11	Host Server Security Test Case
5.2.1.2	The voting system SHALL authenticate users per the minimum authentication methods outlined below. Refer to document for the table layout: http://www.eac.gov/assets/1/AssetManager/UOCAVA_Pilot_Program_Requirements-03.24.10.pdf Table 5-1 Roles : Section 5 | Page 59	11	Host Server Security Test Case
5.2.1.3	The voting system SHALL provide multiple authentication methods to support multi-factor authentication.	1	Host Server Administration Test Case
5.2.1.4	When private or secret authentication data is stored by the voting system, it SHALL be protected to ensure that the confidentiality and integrity of the data are not violated.	11	Host Server Security Test Case
5.2.1.5	The voting system SHALL provide a mechanism to reset a password if it is forgotten, in accordance with the system access/security policy.	1	Host Server Administration Test Case
5.2.1.6	The voting system SHALL allow the administrator group or role to specify password strength for all accounts including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters per NIST 800-63 Electronic Authentication Guideline Standards.	1	Host Server Administration Test Case
5.2.1.7	The voting system SHALL enforce password histories and allow the administrator to configure the history length when passwords are stored by the system.	1	Host Server Administration Test Case
5.2.1.8	The voting system SHALL ensure that the user name is not used in the password.	1	Host Server Administration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.2.1.9	The voting system SHALL provide a means to automatically expire passwords.	1	Host Server Administration Test Case
5.2.1.10	The voting system servers and vote capture devices SHALL identify and authenticate one another using NIST - approved cryptographic authentication methods at the 112 bits of security.	3	Cryptography Test Case
5.2.1.11	Remote voting location site Virtual Private Network (VPN) connections (i.e., vote capture devices) to voting servers SHALL be authenticated using strong mutual cryptographic authentication at the 112 bits of security.	N/A	
5.2.1.12	Message authentication SHALL be used for applications to protect the integrity of the message content using a schema with 112 bits of security.	11	Host Server Security Test Case
5.2.1.13	IPsec, SSL, or TLS and MAC mechanisms SHALL all be configured to be compliant with FIPS 140-2 using approved algorithm suites and protocols.	3	Cryptography Test Case
5.3	**Cryptography**		
	Cryptography serves several purposes in voting systems. They include: Confidentiality: where necessary the confidentiality of voting records can be provided by encryption; Authentication: data and programs can be authenticated by a digital signature or message authentication codes (MAC), or by comparison of the cryptographic hashes of programs or data with the reliably known hash values of the program or data. If the program or data are altered, then that alteration is detected when the signature or MAC is verified, or the hash on the data or program is compared to the known hash value. Typically the programs loaded on voting systems and the ballot definitions used by voting systems are verified by the systems, while systems apply digital signatures to authenticate the critical audit data that they output. For remote connections cryptographic user authentication mechanism SHALL be based on strong authentication methods; and Random number generation: random numbers are used for several purposes including the creation of cryptographic keys for cryptographic algorithms and methods to provide the services listed above, and as identifiers for voting records that can be used to identify or correlate the records without providing any information that could identify the voter.		
5.3.1	**General Cryptography Requirements**		
5.3.1.1	All cryptographic functionality SHALL be implemented using NIST-approved cryptographic algorithms/schemas, or use published and credible cryptographic algorithms/schemas/protocols.	3	Cryptography Test Case
5.3.1.2	Cryptographic algorithms and schemas SHALL be implemented with a security strength equivalent to at least 112 bits of security to protect sensitive voting information and election records.	3	Cryptography Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.3.1.3	Cryptography used to protect information in-transit over public telecommunication networks SHALL use NIST-approved algorithms and cipher suites. In addition the implementations of these algorithms SHALL be NIST-approved (Cryptographic Algorithm Validation Program).	3	Cryptography Test Case
5.3.2	**Key Management**		
	The following requirements apply to voting systems that generate cryptographic keys internally.		
5.3.2.1	Cryptographic keys generated by the voting system SHALL use a NIST-approved key generation method, or a published and credible key generation method.	3	Cryptography Test Case
5.3.2.2	Compromising the security of the key generation method (e.g., guessing the seed value to initialize the deterministic random number generator (RNG)) SHALL require as least as many operations as determining the value of the generated key.	N/T	
5.3.2.3	If a seed key is entered during the key generation process, entry of the key SHALL meet the key entry requirements in 5.3.3.1. If intermediate key generation values are output from the cryptographic module, the values SHALL be output either in encrypted form or under split knowledge procedures.	3	Cryptography Test Case
5.3.2.4	Cryptographic keys used to protect information in-transit over public telecommunication networks SHALL use NIST-approved key generation methods. If the approved key generation method requires input from a random number generator, then an approved (FIPS 140-2) random number generator SHALL be used.	3	Cryptography Test Case
5.3.2.5	Random number generators used to generate cryptographic keys SHALL implement one or more health tests that provide assurance that the random number generator continues to operate as intended (e.g., the entropy source is not stuck).	3	Cryptography Test Case
5.3.3	**Key Establishment**		
	Key establishment may be performed by automated methods (e.g., use of a public key algorithm), manual methods (use of a manually transported key loading device), or a combination of automated and manual methods.		
5.3.3.1	Secret and private keys established using automated methods SHALL be entered into and output from a voting system in encrypted form. Secret and private keys established using manual methods may be entered into or output from a system in plaintext form.	3	Cryptography Test Case
5.3.4.1	Cryptographic keys stored within the voting system SHALL NOT be stored in plaintext. Keys stored outside the voting system SHALL be protected from disclosure or modification.	3	Cryptography Test Case
5.3.4.2	The voting system SHALL provide methods to zeroize all plaintext secret and private cryptographic keys within the system.	3	Cryptography Test Case
5.3.4.3	The voting system SHALL support the capability to reset cryptographic keys to new values.	3	Cryptography Test Case
5.4	**Voting System Integrity Management**		
	This section addresses the secure deployment and operation of the voting system, including the protection of removable media and protection against malicious software.		

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.4.1	**Protecting the Integrity of the Voting System**		
5.4.1.1	The integrity and authenticity of each individual cast vote SHALL be protected from any tampering or modification during transmission.	N/A	
5.4.1.2	The integrity and authenticity of each individual cast vote SHALL be preserved by means of a digital signature during storage.	N/A	
5.4.1.3	Cast vote data SHALL NOT be permanently stored on the vote capture device.	4	Normal Ballot Delivery Test Case
5.4.1.4	The integrity and authenticity of the electronic ballot box SHALL be protected by means of a digital signature.	N/A	
5.4.1.5	The voting system SHALL use malware detection software to protect against known malware that targets the operating system, services, and applications.	5	Discovery Penetration Test Case
5.4.1.6	The voting system SHALL provide a mechanism for updating malware detection signatures.	5	Discovery Penetration Test Case
5.4.1.7	The voting system SHALL provide the capability for kiosk workers to validate the software used on the vote capture devices as part of the daily initiation of kiosk operations.	N/A	
5.5	**Communications Security**		
	This section provides requirements for communications security. These requirements address ensuring the integrity of transmitted information and protecting the voting system from external communications-based threats.		
5.5.1	**Data Transmission Security**		
5.5.1.1	Voting systems that transmit data over communications links SHALL provide integrity protection for data in transit through the generation of integrity data (digital signatures and/or message authentication codes) for outbound traffic and verification of the integrity data for inbound traffic.	11	Host Server Security Test Case
5.5.1.2	Voting systems SHALL use at a minimum TLS 1.0, SSL 3.1 or equivalent protocols, including all updates to both protocols and implementations as of the date of the submission (e.g., RFC 5746 for TLS 1.0).	11	Host Server Security Test Case
5.5.1.3	Voting systems deploying VPNs SHALL configure them to only allow FIPS-compliant cryptographic algorithms and cipher suites.	N/A	
5.5.1.4	Each communicating device SHALL have a unique system identifier.	11	Host Server Security Test Case
5.5.1.5	Each device SHALL mutually strongly authenticate using the system identifier before additional network data packets are processed.	11	Host Server Security Test Case
5.5.1.6	Data transmission SHALL preserve the secrecy of voters' ballot selections and SHALL prevent the violation of ballot secrecy and integrity.	5	Discovery Penetration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.5.2	**External Threats**		
	Voting systems SHALL implement protections against external threats to which the system may be susceptible.	1	Host Server Administration Test Case
		6	Remote Terminal Security Test Case
		5	Discovery Penetration Test Case
5.5.2.1	Voting system components SHALL have the ability to enable or disable physical network interfaces.	1	Host Server Administration Test Case
5.5.2.2	The number of active ports and associated network services and protocols SHALL be restricted to the minimum required for the voting system to function.	11	Host Server Security Test Case
5.5.2.3	The voting system SHALL block all network connections that are not over a mutually authenticated channel.	11	Host Server Security Test Case
5.6	**Logging**		
5.6.1	**Log Management**		
5.6.1.1	The voting system SHALL implement default settings for secure log management activities, including log generation, transmission, storage, analysis, and disposal.	1	Host Server Administration Test Case
5.6.1.2	Logs SHALL only be accessible to authorized roles.	1	Host Server Administration Test Case
5.6.1.3	The voting system SHALL restrict log access to append-only for privileged logging processes and read-only for authorized roles.	1	Host Server Administration Test Case
5.6.1.4	The voting system SHALL log logging failures, log clearing, and log rotation.	1	Host Server Administration Test Case
5.6.1.5	The voting system SHALL store log data in a publicly documented format, such as XML, or include a utility to export log data into a publicly documented format.	1	Host Server Administration Test Case
5.6.1.6	The voting system SHALL ensure that each jurisdiction's event logs and each component's logs are separable from each other.	N/A	
5.6.1.7	The voting system SHALL include an application or program to view, analyze, and search event logs.	1	Host Server Administration Test Case
5.6.1.8	All logs SHALL be preserved in a useable manner prior to voting system decommissioning.	1	Host Server Administration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.6.1.9	Logs SHALL NOT contain any data that could violate the privacy of the voter's identity.	4	Normal Ballot Delivery Test Case
		13	Registration Processing Test Case
5.6.1.10	Timekeeping mechanisms SHALL generate time and date values, including hours, minutes, and seconds.	4	Normal Ballot Delivery Test Case
		1	Host Server Administration Test Case
		13	Registration Processing Test Case
5.6.1.11	The precision of the timekeeping mechanism SHALL be able to distinguish and properly order all log events.	4	Normal Ballot Delivery Test Case
		13	Registration Processing Test Case
5.6.1.12	Only the system administrator SHALL be permitted to set the system clock.	N/A	
5.6.2	**Communication Logging**		
5.6.2.1	All communications actions SHALL be logged.	4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case
		13	Registration Processing Test Case
5.6.2.2	The communications log SHALL contain at least the following entries: Times when the communications are activated and deactivated; Services accessed; Identification of the device which data was transmitted to or received from; Identification of authorized entity; and Successful and unsuccessful attempts to access communications or services.	4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.6.3	**System Event Logging**		
	This section describes requirements for the voting system to perform event logging for system maintenance troubleshooting, recording the history of system activity, and detecting unauthorized or malicious activity. The operating system, and/or applications software may perform the actual event logging. There may be multiple logs in use for any system component.		
5.6.3.1	The voting system SHALL log the following data for each event: a. System ID; b. Unique event ID and/or type; c. Timestamp; d. Success or failure of event, if applicable; e. User ID triggering the event, if applicable; and f. Jurisdiction, if applicable.	1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
		7	Recovery form hardware error Test Case
		5	Discovery Penetration Test Case
5.6.3.2	All critical events SHALL be recorded in the system event log.	5	Discovery Penetration Test Case
		4	Normal Ballot Delivery Test Case
		7	Recovery form hardware error Test Case
		13	Registration Processing Test Case
5.6.3.3	At a minimum the voting system SHALL log the events described in the table below. NOTE: See "Table 5-2 System Events" in document - page 71	1	Host Server Administration Test Case
		4	Normal Ballot Delivery Test Case
		5	Discovery Penetration Test Case
		7	Recovery form hardware error Test Case
5.7	**Incident Response**		
5.7.1	**Incident Response Support**		
5.7.1.1	Manufacturers SHALL document what types of system operations or security events (e.g., failure of critical component, detection of malicious code, unauthorized access to restricted data) are classified as critical.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.7.1.2	An alarm that notifies appropriate personnel SHALL be generated on the vote capture device, system server, or tabulation device, depending upon which device has the error, if a critical event is detected.	N/A	
5.8	**Physical and Environmental Security**		
5.8.1	**Physical Access**		
5.8.1.1	Any unauthorized physical access SHALL leave physical evidence that an unauthorized event has taken place.	N/A	
5.8.2.1	The voting system SHALL disable physical ports and access points that are not essential to voting operations, testing, and auditing.	11	Host Server Security Test Case
5.8.3.1	If a physical connection between the vote capture device and a component is broken, the affected vote capture device port SHALL be automatically disabled.	N/A	
5.8.3.2	The voting system SHALL produce a visual alarm if a connected component is physically disconnected.	N/A	
5.8.3.3	An event log entry that identifies the name of the affected device SHALL be generated if a vote capture device component is disconnected.	7	Recovery form hardware error Test Case
5.8.3.4	Disabled ports SHALL only be re-enabled by authorized administrators.	1	Host Server Administration Test Case
5.8.3.5	Vote capture devices SHALL be designed with the capability to restrict physical access to voting device ports that accommodate removable media with the exception of ports used to activate a voting session.	N/A	
5.8.3.6	Vote capture devices SHALL be designed to give a physical indication of tampering or unauthorized access to ports and all other access points, if used as described in the manufacturer's documentation.	N/A	
5.8.3.7	Vote capture devices SHALL be designed such that physical ports can be manually disabled by an authorized administrator.	N/A	
5.8.4	**Door Cover and Panel Security**		
5.8.4.1	Access points such as covers and panels SHALL be secured by locks or tamper evident or tamper resistant countermeasures and SHALL be implemented so that kiosk workers can monitor access to vote capture device components through these points.	N/A	
5.8.5	**Secure Paper Record Receptacle**		
	If the voting system provides paper record containers then they SHALL be designed such that any unauthorized physical access results in physical evidence that an unauthorized event has taken place.	N/A	
5.8.6	**Secure Physical Lock and Key**		
5.8.6.1	Voting equipment SHALL be designed with countermeasures that provide physical indication that unauthorized attempts have been made to access locks installed for security purposes.	N/A	
5.8.6.2	Manufacturers SHALL provide locking systems for securing vote capture devices that can make use of keys that are unique to each owner.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.8.7	**Media Protection**		
	These requirements apply to all media, both paper and digital, that contain personal privacy related data or other protected or sensitive types of information.		
5.8.7.1	The voting system SHALL meet the following requirements: a. All paper records (including rejected ones) printed at the kiosk locations SHALL be deposited in a secure container; b. Vote capture device hardware, software and sensitive information (e.g., electoral roll) SHALL be physically protected to prevent unauthorized modification or disclosure; and c. Vote capture device hardware components, peripherals and removable media SHALL be identified and registered by means of a unique serial number or other identifier.	N/A	
5.9	**Penetration Resistance**		
5.9.1	**Resistance to Penetration Attempts**		
5.9.1.1	The voting system SHALL be resistant to attempts to penetrate the system by any remote unauthorized entity.	5	Discovery Penetration Test Case
		11	Host Server Security Test Case
5.9.1.2	The voting system SHALL be configured to minimize ports, responses and information disclosure about the system while still providing appropriate functionality.	5	Discovery Penetration Test Case
		11	Host Server Security Test Case
5.9.1.3	The voting system SHALL provide no access, information or services to unauthorized entities.	5	Discovery Penetration Test Case
		1	Host Server Administration Test Case
5.9.1.4	All interfaces SHALL be penetration resistant including TCP/IP, wireless, and modems from any point in the system.	11	Host Server Security Test Case
5.9.1.5	The configuration and setup to attain penetration resistance SHALL be clearly and completely documented.	N/A	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements [redacted] Functional Requirements Matrix	Test Case No.	Test Case Description
5.9.2.1	The scope of penetration testing SHALL include all the voting system components. The scope of penetration testing includes but is not limited to the following: System server; Vote capture devices; Tabulation device; All items setup and configured per Technical Data Package (TDP) recommendations; Local wired and wireless networks; and03/09/2011 Internet connections.	5	Discovery Penetration Test Case
5.9.2.2	Penetration testing SHALL be conducted on a voting system set up in a controlled lab environment. Setup and configuration SHALL be conducted in accordance with the TDP, and SHALL replicate the real world environment in which the voting system will be used.	N/A	
5.9.2.3	The penetration testing team SHALL conduct white box testing using manufacturer supplied documentation and voting system architecture information. Documentation includes the TDP and user documentation. The testing team SHALL have access to any relevant information regarding the voting system configuration. This includes, but is not limited to, network layout and Internet Protocol addresses for system devices and components. The testing team SHALL be provided any source code included in the TDP.	N/A	
5.9.2.04	Penetration testing seeks out vulnerabilities in the voting system that might be used to change the outcome of an election, interfere with voter ability to cast ballots, ballot counting, or compromise ballot secrecy. The penetration testing team SHALL prioritize testing efforts based on the following: a. Threat scenarios for the voting system under investigation; b. Remote attacks SHALL be prioritized over in-person attacks; c. Attacks with a large impact SHALL be prioritized over attacks with a more narrow impact; and d. Attacks that can change the outcome of an election SHALL be prioritized over attacks that compromise ballot secrecy or cause non-selective denial of service.	5	Discovery Penetration Test Case

APPENDIX B
FUNCTIONAL TEST CASES
(Submitted under separate cover)

APPENDIX C
CRYPTOGRAPHIC TEST CASES
(Submitted under separate cover)

APPENDIX D
DISCOVERY PHASE PENTRATION TEST CASES
(Submitted under separate cover)

wyle laboratories

Wyle Laboratories, Inc.
7800 Highway 20 West
Huntsville, Alabama 35806
Phone (256) 837-4411 • Fax (256) 721-0144
www.wyle.com

TEST REPORT

REPORT NO.: T58371.01-06
WYLE JOB NO.: T58371.01
CLIENT P.O. NO.: N/A
CONTRACT: N/A
TOTAL PAGES (INCLUDING COVER): 84
DATE: July 18, 2011

SECURITY TEST REVIEW OF THE UOCAVA OVERSEAS VOTING PILOT PROGRAM ELECTRONIC VOTING SUPPORT WIZARDS (EVSW)

for

Calibre
6354 Walker Lane
Alexandria, Virginia 22310-3252

STATE OF ALABAMA
COUNTY OF MADISON }

Robert D. Hardy, Department Manager, being duly sworn, deposes and says: The information contained in this report is the result of complete and carefully conducted testing and is to the best of his knowledge true and correct in all respects.

Robert Hardy

SUBSCRIBED and sworn to before me this 19 day of July 2011

Sandra A. Daniel

Notary Public in and for the State of Alabama at Large

My Commission expires June 2, 2015

Wyle shall have no liability for damages of any kind to person or property, including special or consequential damages, resulting from Wyle's providing the services covered by this report.

PREPARED BY: Jack Cobb 7-18-11
Jack Cobb, Senior Project Engineer Date

APPROVED BY: Frank Padilla 7-18-11
Frank Padilla, Voting Systems Manager Date

WYLE Q. A.: FOR Raul Terceno 7/19/11
Raul Terceno, Q. A. Manager Date

NVLAP LAB CODE 200771-0

VSTL
EAC Lab Code 0704

TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 Objective

This report documents the procedures followed and the results obtained during testing performed by Wyle on five independent (different Manufacturer's) Electronic Voting Support Wizard (EVSW) systems. The primary purpose of this testing was to demonstrate that the submitted systems conformed to Section 5 "Security" of the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements.

1.2 Scope

The scope of testing for this test campaign was limited to Section 5 "Security" of the UOCAVA Pilot Program Testing Requirements. These requirements were written for a remote electronic Kiosk. The EVSW systems submitted for the test campaign were each designed and deployed prior to the development of these standards. During this test campaign, all applicable requirements were attempted to be tested by Wyle for each EVSW system.

This test campaign included testing in the following areas:

Functional Tests

The functional test area focused on inspection, review and execution as the primary test methods. The functional tests were designed to cover the requirements in the following sections of the UOCAVA Pilot Program Testing Requirements:

5.1 Access Control

5.2 Identification and Authentication

5.4 Voting System Integrity Management

5.5 Communication Security

5.6 Logging

5.7 Incident Response

Cryptographic Tests

The cryptographic test area focused on inspection, review and execution as the primary test methods. The cryptographic tests were designed to cover the requirements in the following section:

5.3 Cryptography

Penetration Tests

The penetration test area was broken into two phases: discovery and exploratory. The penetration tests were designed to cover the requirements in the following sections:

5.8 Physical and Environmental Security

5.9 Penetration Resistance

1.0 INTRODUCTION (CONTINUED)

1.3 Customer

Calibre
6354 Walker Lane
Alexandria, Virginia 22310-3252

1.4 References

The documents listed were utilized to perform testing.

- Wyle Laboratories Quotation No. 545/052353-R1/DB, dated December 22, 2010
- National Voluntary Laboratory Accreditation Program NIST Handbook 150, 2006 Edition, "NVLAP Procedures and General Requirements (NIST Handbook 150)", dated February 2006
- National Voluntary Laboratory Accreditation Program NIST Handbook 150-22, 2008 Edition, "Voting System Testing (NIST Handbook 150-22)", dated May 2008
- Wyle Laboratories' Quality Assurance Program Manual, Revision 3
- ANSI/NCSL Z540-1, "Calibration Laboratories and Measuring and Test Equipment, General Requirements"
- ISO 10012-1, "Quality Assurance Requirements for Measuring Equipment"
- Election Assistance Commission, "Uniform and Overseas Citizens Absentee Voting Act Pilot Program Testing Requirements", August 25, 2010
- NIST 800-63 Electronic Authentication Guideline Standards
- NIST SP800-57 Computer Security
- FIPS 140-2 Security Requirements for Cryptographic Modules
- Manufacturer's submitted documentation – may have included any of the following types of documentation: overview, design or architecture, functional, user manual, hardware, setup, registration, or help.

1.5 Summary

The EVSW systems were subjected to the tests required per the scope of this test campaign. Testing was performed at Wyle Laboratories, Huntsville, Alabama Test Facility from March 2 through June 24, 2011. All hard copy data generated by the performance of these tests was retained by Wyle as raw data.

Details of the systems tested and the tests performed are provided in redacted format in the following sections.

2.0 TEST EQUIPMENT DESCRIPTION

2.1 System Overview

The systems submitted for this test campaign ranged from web based online ballot delivery systems to web based online internet voting systems. Each system was accessible from any internet capable computing device via a vendor chosen host web server.

A generic / redacted description of the EVSW systems submitted for testing follows.

System A: [redacted] The administration website allows for management and general administrative tasks. The voter website allows for identity verification, voting, and reviewing of ballots.

System B: [redacted] Voter data, candidates, contests, and election information is uploaded through an administrative website that provides:

- Tiered access based on user location, permission, and role;
- Interfaces to upload mass voter and election data;
- The capability to associate ballots with styles and precincts; and
- Usage metrics, ballot tracking and alerts.

Voters are able to access the uploaded information via a separate voter website.

System C: [redacted]. The back-end (administrative) website allows for request and elector management and general administrative tasks. The front-end (elector) website allows for registration and voting options.

System D: [redacted]. Voter data, candidates, contests, and election information is uploaded through an administrative website that provides:

- Tiered access based on user location, permission, and role;
- Interfaces to upload mass voter and election data;
- The capability to associate ballots with styles and precincts; and
- Usage metrics, ballot tracking and alerts.

Voters are able to access the uploaded information via a separate voter website.

System E: [redacted]. Voter data, candidates, contests, and election information is uploaded through an administrative website that provides:

- Tiered access based on user location, permission, and role;
- Interfaces to upload mass voter and election data;
- The capability to associate ballots with styles and precincts; and
- Usage metrics, ballot tracking and alerts.

Voters are able to access the uploaded information via a separate voter website.

2.0 TEST EQUIPMENT DESCRIPTION (CONTINUED)

2.2 Software

Each EVSW system was tested with software as submitted by the manufacturer.

2.3 Hardware

The manufacturer's applications were each web-based and therefore did not have locally available hardware.

2.4 Test Tools/Materials

This subsection enumerates any and all test materials needed to perform functional testing. The equipment was used to implement the test cases on each EVSW system evaluated.

Table 2-3 Test Materials

Test Material	Quantity
Dell OptiPlex 780	1
Windows 7	1
IE (Internet Explorer) 8	1

3.0 TEST PROCEDURES AND RESULTS

The methodology utilized to perform testing differed from that from a typical test campaign in three primary ways: control and possession of the system hardware, technical documentation and source code. During the course of a typical certification test campaign, manufacturers' provide the hardware and a Technical Data Package (TDP) for each system being tested. For this test campaign, Wyle was not provided a full TDP for the systems tested. The absence of technical documentation limited the requirements that could be evaluated due to a lack of information for defining test cases. Additionally, in typical certification efforts, a source code review will be performed on all proprietary software. Source code reviews were not required during this effort; therefore, the execution of the penetration testing was limited and "white-box" level testing could not be performed.

Each EVSW system was subjected to all tests as required for the scope of the test campaign. For testing purposes, test cases were developed using the manufacturer's documentation, architectural documents, and security specifications, as well as "Use Case" and verification methods. These test cases were then mapped to the applicable requirements of Section 5 "Security" of the UOCAVA Pilot Program Testing Requirements. This test campaign included the following core test cases: Functional, Penetration and Cryptography. The UOCAVA Functional Requirements Matrix, contained in Appendix A of this report, presents the requirements tested, test cases utilized to test each applicable requirement, and designates all non-applicable requirements (marked "N/A").

3.1 Functional Tests

Functional tests were performed by Wyle qualified personnel (henceforth referred to as Wyle) to validate compliance to the applicable UOCAVA requirements. The following test methods were used during functional tests: inspection, review, and execution. Wyle executed some combination of the following set of test cases that were specifically designed for each EVSW system.

3.0 TEST PROCEDURES AND RESULTS (CONTINUED)

3.1 Functional Tests (continued)

Below is a brief description of each of the test cases utilized:

- TC01HostAdmin (Host Server Administration) – A test to verify the roles of the system administrator and the ability to maintain user roles, passwords, logs and other voting system administrative functions.

- TC04BallotDelivery (Normal Ballot Delivery) – A test to verify accurately ballot delivery, implementation of authentication prior to allowing voter access to the ballot, and logging of events.

- TC10BallotDelivery (Local Ballot Delivery) – A test to verify accurate ballot delivery, implementation of authentication prior to allowing voter access to the ballot, and logging of events.

- TC12VoterRegReq (Voter Registration Request) – A test to verify a voter can securely register to vote on-line. The test includes authentication of voter credentials.

- TC13RegProcess (Registration Processing) – A test to verify the ability of an election administrator to view voter requests and accept or reject the request based on successful comparison of the voter's credentials.

- TC14NormalVoting (Normal Voting) – A test to verify accurate ballot delivery, implementation of authentication prior to allowing voter access to the ballot, and logging of events.

The functional test cases executed for each system under test are listed in the table below.

Table 3-1 Functional Test Cases

System	Test Cases
A	TC01HostAdmin (Host Server Administration) TC10BallotDelivery (Local Ballot Delivery)
B	TC01HostAdmin (Host Server Administration) TC04BallotDelivery (Normal Ballot Delivery)
C	TC01HostAdmin (Host Server Administration) TC12VoterRegReq (Voter Registration Request) TC13RegProcess (Registration Processing) TC14NormalVoting (Normal Voting)
D	TC01HostAdmin (Host Server Administration) TC04BallotDelivery (Normal Ballot Delivery)
E	TC01HostAdmin (Host Server Administration) TC12VoterRegReq (Voter Registration Request) TC13RegProcess (Registration Processing) TC04BallotDelivery (Normal Ballot Delivery)

3.0 TEST PROCEDURES AND RESULTS (CONTINUED)

3.1 Functional Tests (continued)

The findings from the performance of each test case are detailed in the following paragraphs.

Summary Findings

For Systems A, B, D, and E, the following paragraph applies:

TC01HostAdmin

During the Host Admin test case Wyle logged in with the administrative account provided by the vendor. An attempt was made to dump logs and manipulate any stored data. Data from the logs was analyzed to determine compliance with the UOCAVA requirements. Wyle then attempted to modify the user data and login credentials. Validation was performed to validate that all requirements for voter security were met per the UOCAVA requirements. Wyle then attempted to create administration accounts and validate security of administration accounts. Admin accounts were used to validate roles and responsibilities of each administrator. Attempts were made to access administration functionality without use of the administration login.

System A specifics for TC01HostAdmin:

During the performance of the test case, the following issues were noted:

- Admin page functionality was very limited.
- Admin account management is system based
- There is nothing implemented to limit incorrect login attempts.
- System does not have a lock out function.
- System does not have a time out control.
- Passwords would need to be reset by a system administrator.
- Log files must be generated by the admin on local system. They will then be in the format selected by the admin.
- Many requirements could not be tested do to the architecture requiring physical access to the server.

System B specifics for TC01HostAdmin:

During the performance of the test case, it was noted that the following core functions were untestable:

- User functionality was very limited.
- Logs were not tested. Only a voter's log was available.
- No reporting was available.
- Admin account management was not functional.

3.0 TEST PROCEDURES AND RESULTS (CONTINUED)

3.1 Functional Tests (continued)

System D specifics for TC01HostAdmin:

During the performance of the test case, the following issues were noted:

- There is only one login for each election.
- Incorrect login attempts are not limited.
- The administrator of the election can send a new password for that user. At which point, the author can then customize his/her own password if they so choose. For the <redacted>, the password is set by the system administrator and the user cannot reset it.
- An administrator does not configure the password strength configuration.
- There is nothing in place to limit the use of historically used passwords.
- There is not a restriction on user password matching the user name.
- There is not a password expiration option.
- The log remains continuous and cannot be cleared.

System E specifics for TC01HostAdmin:

During the performance of the test case, the following issues were noted:

- Nothing is implemented to limit incorrect login attempts.
- System does not have a lock out function.
- Administrator cannot set the password strength configuration
- There is not anything in place to limit the use of historically used passwords.
- There is not a restriction on user password matching the user name.
- Passwords do not expire.
- Logs are retained and do not get cleared.
- Member login log is not exportable

For System C, the following paragraph applies for TC01HostAdmin:

During performance of testing, Wyle was able to verify the system contained segregation of duties and those duties were maintainable. The system does require passwords and provides an event log, but not all requirements were met for these functions.

3.0 TEST PROCEDURES AND RESULTS (CONTINUED)

3.1 Functional Tests (continued)

System C specifics for TC01HostAdmin:

During the performance of the test case, the following issues were noted:

- Upon creation of a new user and default role is the administrator role.
- No ability for the user to reset their password. This function is handled by requesting a password change.
- No limit on incorrect login attempts.
- No password expiration.
- The current system logging is not as detailed per the requirements.

TC01HostAdmin – Synopsis of Summary Findings – All Tested Systems:

Per the UOCAVA requirements tested by test case TC01HostAdmin, Wyle deduced from the above summary findings that the primary areas of deficiency of the systems tested can be categorized into one of the following areas.

- Login functions.
- Password functions.
- Log generation functions.

TC04BallotDelivery

For Systems A, B, D, and E, the following paragraph applies:

During the Ballot Delivery test case Wyle logged in with the voter accounts provided by the vendor. Attempts were made to access multiple ballots using a single voter. Analysis was done to determine the level of security of data as a result of the ballot delivery process. Wyle attempted to gain access to a ballot by an unauthorized voter. Wyle attempted to gain access to administration information utilizing voter credentials.

System A specifics for TC04BallotDelivery:

During the performance of the test case, it the following issues were noted:

- There is nothing implemented to limit incorrect login attempts.
- System does not have a lock out function.
- System does not have a time out control.
- Passwords would need to be reset by a system administrator.

3.0 TEST PROCEDURES AND RESULTS (CONTINUED)

3.1 Functional Tests (continued)

System B specifics for TC04BallotDelivery:

During the performance of the test case, it was noted that the following core functions were untestable:

- Blank Ballot delivery

System D specifics for TC04BallotDelivery:

During the performance of the test case, the following issues were noted:

- There is not a restriction on user password matching the user name.
- There is not a password expiration option.
- It was noted that the pages are being cached and would give a hacker the ability to return to pages that should be secure.

System E specifics for TC04BallotDelivery:

- No issues noted.

TC04HostAdmin – Synopsis of Summary Findings – All Tested Systems:

Per the UOCAVA requirements tested by test case TC04HostAdmin, Wyle deduced from the above summary findings that the primary areas of deficiency of the systems tested can be categorized into one of the following areas.

- Login functions.
- Password functions.

TC12 Registration Request Test Case

System C specifics for TC12 Registration Request Test Case:

During performance of testing, Wyle was able to verify a voter could successfully and securely submit information and request an online registration. The test also verified authentication of a registered voter with credential from the system. There were no discrepancies to report.

System E specifics for TC12 Registration Request Test Case:

During performance of the test case, Wyle logged in with the voter credentials provided by the vendor. Analysis was done to determine the level of security of data as a result of the registration request process. Wyle attempted to gain access to a ballot by registering unauthorized voter. Wyle attempted to gain access to administration information utilizing voter credentials.

3.0 TEST PROCEDURES AND RESULTS (CONTINUED)

3.1 Functional Tests (continued)

During the performance of the test case, the following issues were noted:

- It was noticed that after the registration is completed, a user can use the back button and still see the registration information.

TC12 Registration Request Test Case – Synopsis of Summary Findings – Tested Systems:

For the two systems supporting these areas of the UOCAVA requirements, the one area of deficiency has to do with limiting web page caching and session storage of user input information that might be miss-used to compromise privacy or security.

TC13 Registration Processing Test Case

System C specifics for TC13 Registration Processing Test Case:

During performance of testing, Wyle was able to verify a user logged in with administrative duties could approve and reject requests submitted by on online voter. Wyle was also able to authenticate voter credential against an approved UOCAVA registered voter list.

- There were no discrepancies to report.

System E specifics for TC13 Registration Processing Test Case:

During performance of the test case, Wyle logged in with the administrative accounts provided by the vendor. Analysis was done to determine the level of security of data as a result of the registration request process. Validation was made that admins do validation of voter credentials.

- There were no discrepancies to report.

TC13HostAdmin – Synopsis of Summary Findings – Tested Systems:

For the two systems supporting these areas of the UOCAVA requirements, there were no discrepancies to report.

TC14 Normal Voting

During performance of testing, Wyle was able to submit an accurate online ballot. Wyle also verified that a voter must be a registered and approved to gain access to a ballot. Voters are also only able to vote one time. The system does log some events for the voting process, but the log function does not meet all requirements.

A summary of discrepancies are listed below:

- No ability for the user to reset their password. This function is handled by requesting a password change.
- No limit on incorrect login attempts.

3.0 TEST PROCEDURES AND RESULTS (CONTINUED)

3.1 Functional Tests (continued)

- No password expiration.
- The current system logging is not as detailed per the requirements.

TC14 Normal Voting – Synopsis of Summary Findings – Tested Systems:

Per the UOCAVA requirements tested by test case TC14 Normal Voting, Wyle deduced from the above summary findings that the primary areas of deficiency of the system tested can be categorized into one of the following areas.

- Login functions.
- Password functions.
- Log generation functions.

3.2 Cryptographic Tests

Cryptographic Tests were performed to validate compliance to the applicable UOCAVA requirements.

Three test methods were used during performance of the cryptographic tests: inspection, review, and execution. Wyle executed some combination of the following set of test cases that were specifically designed for each EVSW system. Below is a brief description of each of the test cases utilized:

- TC03CryptoTestSheet (Manufacturer) – A test to verify the functionality, strength and NIST compliance of the system, no matter which one of the three purposes it serves in the voting system (Confidentiality, Authentication or Random Number Generation (RNG)).

Summary Findings

The following summary applied to all systems tested in this campaign:

During performance of testing, Wyle was able to verify portions of the cryptographic requirements. Key management and key establishment could not be tested due to lack of documentation in this area as well as physical access to the system necessary to complete these two areas of cryptographic testing. Wyle only had access to the client side functionality; therefore, no administrator credentialed cryptographic testing could be performed. The test cases and results obtained are presented in Appendix B of this document.

3.0 TEST PROCEDURES AND RESULTS (CONTINUED)

3.3 Penetration Tests

Penetration tests were performed to determine the security of each EVSW system and to validate compliance to the applicable UOCAVA requirements.

The penetration test area was broken into two phases: discovery and exploratory. The discovery phase consisted of performing scans while the system was running with leveraged and unleveraged credentials. These scans provided information about the ports, protocols, and hardware configurations as well as simulated certain portions of an attack on vulnerable areas of the system. The information gathered was provided to a certified security professional, who analyzed the results and determined the best method and types of attacks to be performed during the exploratory phase of testing. Specific test cases were then designed and executed during the exploratory phase of the penetration tests. These test cases were based on all information gathered during discovery, any subsequent observations made during the exploratory phase and any Rules Of Engagement (ROE) previously agreed upon by Wyle and the manufacturer.

Below is a brief description of each of the test cases utilized:

- TC05DiscoveryPenetration (Manufacturer) – A test to seek out vulnerabilities in the voting system and to verify the system's resistance to any remote unauthorized entity.

Summary Findings

NOTE: Information redacted. In general, all vulnerabilities discovered and their level (high, medium, low) were reported to each manufacturer. However, any discovered vulnerabilities could not be exploited in the time constraint set for the exploratory phase of the penetration test. Details of this test case can be found in Appendix B of this document. NOTE: Appendix B information redacted in this report.

TC05DiscoveryPenetration

During performance of testing, Wyle sought to discover vulnerabilities that fall into risk levels of "High", "Medium", or "Low".

System A specifics for **TC05DiscoveryPenetration**:

A summary of risk levels are listed below:

- Low risk area – 11 found.

System B specifics for **TC05DiscoveryPenetration**:

A summary of risk levels are listed below:

- SQL attempts exposed some information that could be useful to an attacker.

3.0 TEST PROCEDURES AND RESULTS (CONTINUED)

3.3 Penetration Tests

System C specifics for **TC05DiscoveryPenetration**:

A summary of risk levels are listed below:

- Low risk area – 22 found.

System D specifics for **TC05DiscoveryPenetration**:

A summary of risk levels are listed below:

- Low risk area – 42 found.
- Medium risk area – 8 found.

System E specifics for **TC05DiscoveryPenetration**:

- No risk areas were located in the time constraint set for penetration testing.

TC05DiscoveryPenetration – Synopsis of Summary Findings – Tested Systems:

Penetration testing discovered primarily "low" risk areas of vulnerability in the systems tested in this test campaign. Regardless of the risk level/areas located, none of these could be exploited in the time constraint set for the exploratory phase of the penetration testing.

3.4 Test Summary

For the specific test cases executed, and the results for each system, refer to Attachment B "Test Cases". Overall assessment of the test results for each system tested and the specific requirement by system "Pass/Fail" are presented in Attachment C "Statistical Analysis of the UOCAVA EVSW's". As for the ability of the EVSW's tested to meet the requirements, the results observed during testing is provided below:

Table 3-1 Test Result Summary

Average Summary	Pass	Fail	Not Tested	N/A
	24%	22%	24%	30%

ATTACHMENT A

REQUIREMENT MATRIX

Overall, during the execution of this test campaign, Wyle did not encounter any major problems working with the requirements. However, Wyle feels that some of the requirements can be clearer and better defined to make them more testable. The following table contains comments and recommendations per requirement. As for the Non-Applicable requirements, Wyle did not attempt to test them; therefore, recommendations are not provided. Additionally, the Not Tested requirements were attempted to be applied but could not be tested under this test campaign due to the current configuration of the systems tested. The major areas that Wyle is unable to comment on are the Communication Security, Penetration Resistance, and Cryptography sections.

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix	Test Case Description	Wyle Comment
Section 5	**Security**		
5.1	**Access Control**		
	This section states requirements for the identification of authorized system users, processes and devices and the authentication or verification of those identities as a prerequisite to granting access to system processes and data. It also includes requirements to limit and control access to critical system components to protect system and data integrity, availability, confidentiality, and accountability. This section applies to all entities attempting to physically enter voting system facilities or to request services or data from the voting system.		
5.1.1	**Separation of Duties**		
5.1.1.1	The voting system SHALL allow the definition of personnel roles with segregated duties and responsibilities on critical processes to prevent a single person from compromising the integrity of the system.	Administration Test Case	Specific roles should be defined to facilitate true segregation of duties.
5.1.1.2	The voting system SHALL ensure that only authorized roles, groups, or individuals have access to election data.	Administration Test Case	
5.1.1.3	The voting system SHALL require at least two persons from a predefined group for validating the election configuration information, accessing the cast vote records, and starting the tabulation process.	N/A	Current web based system do not do tabulation so this requirement was not applicable to our testing. The majority of election configuration is done independent of the Web application and is therefore not a critical function of our testing.
5.1.2	**Voting System Access**		
	The voting system SHALL provide access control mechanisms designed to permit authorized access and to prevent unauthorized access to the system.	Penetration Test Case Administration Test Case	This requirement does not define at what minimum level this security should be implemented.
5.1.2.1	The voting system SHALL identify and authenticate each person, to whom access is granted, and the specific functions and data to which each person holds authorized access.	Administration Test Case Ballot Delivery Test Case	This requirement does not define at what minimum level this security should be implemented.
5.1.2.2	The voting system SHALL allow the administrator group or role to configure permissions and functionality for each identity, group or role to include account and group/role creation, modification, and deletion.	Administration Test Case	This requirement does not state whether this should be a system OS level or at a web based administration application level.
5.1.2.3	The voting system's default access control permissions SHALL implement the least privileged role or group needed.	Administration Test Case	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix	Test Case Description	Wyle Comment
5.1.2.4	The voting system SHALL prevent a lower-privilege process from modifying a higher-privilege process.	Administration Test Case	
5.1.2.5	The voting system SHALL NOT require its execution as an operating system privileged account and SHALL NOT require the use of an operating system privileged account for its operation.	N/A	Wyle's testing was based on utilization of a web based application. Therefore this did not apply directly. But, it was noted that in some systems tested the OS administration privileges were required to configure election information.
5.1.2.6	The voting system SHALL log the identification of all personnel accessing or attempting to access the voting system to the system event log.	Administration Test Case Ballot Delivery Test Case Penetration Test Case	This requirement does not define what information should be logged. Some systems only log Administration functions while others only log Voter information.
5.1.2.7	The *(voting system)* SHALL provide tools for monitoring access to the system. These tools SHALL provide specific users real time display of persons accessing the system as well as reports from logs.	Administration Test Case	This requirement does not define what information should be logged. This requirement also does not state if the tool is to be accessible via the Web based administration application or at an OS Level.
5.1.2.8	Vote capture device located at the remote voting location and the central server SHALL have the capability to restrict access to the voting system after a preset number of login failures. a. The lockout threshold SHALL be configurable by appropriate administrators/operators b. The voting system SHALL log the event c. The voting system SHALL immediately send a notification to appropriate administrators/operators of the event. d. The voting system SHALL provide a mechanism for the appropriate administrators/operators to reactivate the account after appropriate confirmation.	Administration Test Case Penetration Test Case	This requirement does not define if this needs to be at a Web application level or at OS level. Reactivation of an account should not require utilization of anything but the Web based application.
5.1.2.9	The voting system SHALL log a notification when any account has been locked out.	Administration Test Case Penetration Test Case	This requirement does not define what information should be logged.

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix	Test Case Description	Wyle Comment
5.1.2.10	Authenticated sessions on critical processes SHALL have an inactivity time-out control that will require personnel re-authentication when reached. This time-out SHALL be implemented for administration and monitor consoles on all voting system devices.	Administration Test Case Penetration Test Case	This requirement does not define how this function should be configured.
5.1.2.11	Authenticated sessions on critical processes SHALL have a screen-lock functionality that can be manually invoked.	N/A	This requirement was deemed N/A due to the web based application being accessible from a privately controlled PC and not a public Voting site.
5.2	**Identification and Authentication**		
	Authentication mechanisms and their associated strength may vary from one voting system capability and architecture to another but all must meet the minimum requirement to maintain integrity and trust. It is important to consider a range of roles individuals may assume when operating different components in the voting system and each may require different authentication mechanisms. The requirements described in this section vary from role to role. For instance, a kiosk worker will have different identification and authentication characteristics than a voter. Also, for selected critical functions there may be cases where split knowledge or dual authorization is necessary to ensure security. This is especially relevant for critical cryptographic key management functions.		
5.2.1	**Authentication**		
5.2.1.1	Authentication mechanisms supported by the voting system SHALL support authentication strength of at least 1/1,000,000.	Administration Test Case	
5.2.1.2	The voting system SHALL authenticate users per the minimum authentication methods outlined below. Refer to document for the table layout: http://www.eac.gov/assets/1/AssetManager/UOCAVA_Pilot_Program_Requirments-03.24.10.pdf Table 5-1 Roles : Section 5 | Page 59	Administration Test Case	Since these systems do not tabulate and are not located in a polling location, the groups for Election Judge and Kiosk Worker do not really apply. (See Table 5-1 Roles : Section 5 | Page 59.)
5.2.1.3	The voting system SHALL provide multiple authentication methods to support multi-factor authentication.	Administration Test Case	This requirement does not define what minimum level is required.

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix	Test Case Description	Wyle Comment
5.2.1.4	When private or secret authentication data is stored by the voting system, it SHALL be protected to ensure that the confidentiality and integrity of the data are not violated.	Administration Test Case	
5.2.1.5	The voting system SHALL provide a mechanism to reset a password if it is forgotten, in accordance with the system access/security policy.	Administration Test Case	This requirement does not define if this function is to be Web Based.
5.2.1.6	The voting system SHALL allow the administrator group or role to specify password strength for all accounts including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters per NIST 800-63 Electronic Authentication Guideline Standards.	Administration Test Case	This requirement does not define if this configuration is to be Web Based or OS configurable.
5.2.1.7	The voting system SHALL enforce password histories and allow the administrator to configure the history length when passwords are stored by the system.	Administration Test Case	This requirement does not define if this configuration is to be Web Based or OS configurable.
5.2.1.8	The voting system SHALL ensure that the user name is not used in the password.	Administration Test Case	
5.2.1.9	The voting system SHALL provide a means to automatically expire passwords.	Administration Test Case	
5.2.1.10	The voting system servers and vote capture devices SHALL identify and authenticate one another using NIST - approved cryptographic authentication methods at the 112 bits of security.	Cryptography Test Case	This requirement does not define which NIST standard or level to use.
5.2.1.11	Remote voting location site Virtual Private Network (VPN) connections (i.e., vote capture devices) to voting servers SHALL be authenticated using strong mutual cryptographic authentication at the 112 bits of security.	N/A	Wyle deems this requirement N/A due to the Web Based architecture. VPN systems will only be utilized at a system server level.
5.2.1.12	Message authentication SHALL be used for applications to protect the integrity of the message content using a schema with 112 bits of security.	Cryptography Test Case	
5.2.1.13	IPsec, SSL, or TLS and MAC mechanisms SHALL all be configured to be compliant with FIPS 140-2 using approved algorithm suites and protocols.	Cryptography Test Case	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix	Test Case Description	Wyle Comment
5.3	**Cryptography**		
	Cryptography serves several purposes in voting systems. They include: Confidentiality: where necessary the confidentiality of voting records can be provided by encryption; Authentication: data and programs can be authenticated by a digital signature or message authentication codes (MAC), or by comparison of the cryptographic hashes of programs or data with the reliably known hash values of the program or data. If the program or data are altered, then that alteration is detected when the signature or MAC is verified, or the hash on the data or program is compared to the known hash value. Typically the programs loaded on voting systems and the ballot definitions used by voting systems are verified by the systems, while systems apply digital signatures to authenticate the critical audit data that they output. For remote connections cryptographic user authentication mechanism SHALL be based on strong authentication methods; and Random number generation: random numbers are used for several purposes including the creation of cryptographic keys for cryptographic algorithms and methods to provide the services listed above, and as identifiers for voting records that can be used to identify or correlate the records without providing any information that could identify the voter.		
5.3.1	**General Cryptography Requirements**		
5.3.1.1	All cryptographic functionality SHALL be implemented using NIST-approved cryptographic algorithms/schemas, or use published and credible cryptographic algorithms/schemas/protocols.	Cryptography Test Case	This requirement does not define what minimum NIST level is required.
5.3.1.2	Cryptographic algorithms and schemas SHALL be implemented with a security strength equivalent to at least 112 bits of security to protect sensitive voting information and election records.	Cryptography Test Case	
5.3.1.3	Cryptography used to protect information in-transit over public telecommunication networks SHALL use NIST-approved algorithms and cipher suites. In addition the implementations of these algorithms SHALL be NIST-approved (Cryptographic Algorithm Validation Program).	Cryptography Test Case	This requirement does not define which NIST standard or level to use.

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix	Test Case Description	Wyle Comment
5.3.2	**Key Management**		
	The following requirements apply to voting systems that generate cryptographic keys internally.		
5.3.2.1	Cryptographic keys generated by the voting system SHALL use a NIST-approved key generation method, or a published and credible key generation method.	Cryptography Test Case	This requirement does not define which NIST standard or level to use.
5.3.2.2	Compromising the security of the key generation method (e.g., guessing the seed value to initialize the deterministic random number generator (RNG)) SHALL require as least as many operations as determining the value of the generated key.	Cryptography Test Case	
5.3.2.3	If a seed key is entered during the key generation process, entry of the key SHALL meet the key entry requirements in 5.3.3.1. If intermediate key generation values are output from the cryptographic module, the values SHALL be output either in encrypted form or under split knowledge procedures.	Cryptography Test Case	
5.3.2.4	Cryptographic keys used to protect information in-transit over public telecommunication networks SHALL use NIST-approved key generation methods. If the approved key generation method requires input from a random number generator, then an approved (FIPS 140-2) random number generator SHALL be used.	Cryptography Test Case	This requirement does not define which NIST standard or level to use.
5.3.2.5	Random number generators used to generate cryptographic keys SHALL implement one or more health tests that provide assurance that the random number generator continues to operate as intended (e.g., the entropy source is not stuck).	Cryptography Test Case	
5.3.3	**Key Establishment**		
	Key establishment may be performed by automated methods (e.g., use of a public key algorithm), manual methods (use of a manually transported key loading device), or a combination of automated and manual methods.		
5.3.3.1	Secret and private keys established using automated methods SHALL be entered into and output from a voting system in encrypted form. Secret and private keys established using manual methods may be entered into or output from a system in plaintext form.	Cryptography Test Case	
5.3.4.1	Cryptographic keys stored within the voting system SHALL NOT be stored in plaintext. Keys stored outside the voting system SHALL be protected from disclosure or modification.	Cryptography Test Case	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix	Test Case Description	Wyle Comment
5.3.4.2	The voting system SHALL provide methods to zeroize all plaintext secret and private cryptographic keys within the system.	Cryptography Test Case	
5.3.4.3	The voting system SHALL support the capability to reset cryptographic keys to new values.	Cryptography Test Case	
5.4	**Voting System Integrity Management**		
	This section addresses the secure deployment and operation of the voting system, including the protection of removable media and protection against malicious software.		
5.4.1	**Protecting the Integrity of the Voting System**		
5.4.1.1	The integrity and authenticity of each individual cast vote SHALL be protected from any tampering or modification during transmission.	Ballot Delivery Test Case	
5.4.1.2	The integrity and authenticity of each individual cast vote SHALL be preserved by means of a digital signature during storage.	Ballot Delivery Test Case	
5.4.1.3	Cast vote data SHALL NOT be permanently stored on the vote capture device.	Ballot Delivery Test Case	
5.4.1.4	The integrity and authenticity of the electronic ballot box SHALL be protected by means of a digital signature.	Ballot Delivery Test Case	
5.4.1.5	The voting system SHALL use malware detection software to protect against known malware that targets the operating system, services, and applications.	Penetration Test Case	
5.4.1.6	The voting system SHALL provide a mechanism for updating malware detection signatures.	Penetration Test Case	
5.4.1.7	The voting system SHALL provide the capability for kiosk workers to validate the software used on the vote capture devices as part of the daily initiation of kiosk operations.	N/A	Wyle deems this requirement N/A due to the Web Based architecture.
5.5	**Communications Security**		
	This section provides requirements for communications security. These requirements address ensuring the integrity of transmitted information and protecting the voting system from external communications-based threats.		
5.5.1	**Data Transmission Security**		
5.5.1.1	Voting systems that transmit data over communications links SHALL provide integrity protection for data in transit through the generation of integrity data (digital signatures and/or message authentication codes) for outbound traffic and verification of the integrity data for inbound traffic.	Host Server Security Test Case	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix	Test Case Description	Wyle Comment
5.5.1.2	Voting systems SHALL use at a minimum TLS 1.0, SSL 3.1 or equivalent protocols, including all updates to both protocols and implementations as of the date of the submission (e.g., RFC 5746 for TLS 1.0).	Host Server Security Test Case	
5.5.1.3	Voting systems deploying VPNs SHALL configure them to only allow FIPS-compliant cryptographic algorithms and cipher suites.	N/A	Wyle deems this requirement N/A due to the Web Based architecture. VPN systems will only be utilized at a system server level.
5.5.1.4	Each communicating device SHALL have a unique system identifier.	Host Server Security Test Case	
5.5.1.5	Each device SHALL mutually strongly authenticate using the system identifier before additional network data packets are processed.	Host Server Security Test Case	
5.5.1.6	Data transmission SHALL preserve the secrecy of voters' ballot selections and SHALL prevent the violation of ballot secrecy and integrity.	Penetration Test Case	
5.5.2	**External Threats**		
	Voting systems SHALL implement protections against external threats to which the system may be susceptible.	Penetration Test Case	
5.5.2.1	Voting system components SHALL have the ability to enable or disable physical network interfaces.	Administration Test Case	
5.5.2.2	The number of active ports and associated network services and protocols SHALL be restricted to the minimum required for the voting system to function.	Penetration Test Case	
5.5.2.3	The voting system SHALL block all network connections that are not over a mutually authenticated channel.	Penetration Test Case	
5.6	**Logging**		
5.6.1	**Log Management**		
5.6.1.1	The voting system SHALL implement default settings for secure log management activities, including log generation, transmission, storage, analysis, and disposal.	Administration Test Case	
5.6.1.2	Logs SHALL only be accessible to authorized roles.	Administration Test Case	
5.6.1.3	The voting system SHALL restrict log access to append-only for privileged logging processes and read-only for authorized roles.	Administration Test Case	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix	Test Case Description	Wyle Comment
5.6.1.4	The voting system SHALL log logging failures, log clearing, and log rotation.	Administration Test Case	This requirement does not specify if these logs should contain both voter and administration information.
5.6.1.5	The voting system SHALL store log data in a publicly documented format, such as XML, or include a utility to export log data into a publicly documented format.	Administration Test Case	This requirement does not determine if these functions should be part of an administration web based application or at an OS level administration function.
5.6.1.6	The voting system SHALL ensure that each jurisdiction's event logs and each component's logs are separable from each other.	Administration Test Case	
5.6.1.7	The voting system SHALL include an application or program to view, analyze, and search event logs.	Administration Test Case	This requirement does not determine if these functions should be part of an administration web based application or at an OS level administration function.
5.6.1.8	All logs SHALL be preserved in a useable manner prior to voting system decommissioning.	Administration Test Case	
5.6.1.9	Logs SHALL NOT contain any data that could violate the privacy of the voter's identity.	Ballot Delivery Test Case Registration Processing Test Case	This requirement does not outline what information is deemed to violate a voter's identity. These systems utilize several voter specific credentials that are required for proper identification of voters.
5.6.1.10	Timekeeping mechanisms SHALL generate time and date values, including hours, minutes, and seconds.	Ballot Delivery Test Case Administration Test Case Registration Processing Test Case	
5.6.1.11	The precision of the timekeeping mechanism SHALL be able to distinguish and properly order all log events.	Ballot Delivery Test Case Registration Processing Test Case	This requirement must meet 5.6.1.10

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix	Test Case Description	Wyle Comment
5.6.1.12	Only the system administrator SHALL be permitted to set the system clock.	N/A	Wyle determined that this requirement is N/A due to this function being a system administration function.
5.6.2	**Communication Logging**		
5.6.2.1	All communications actions SHALL be logged.	Penetration Test Case	This requirement does not define what all communications encompasses.
5.6.2.2	The communications log SHALL contain at least the following entries: Times when the communications are activated and deactivated; Services accessed; Identification of the device which data was transmitted to or received from; Identification of authorized entity; and Successful and unsuccessful attempts to access communications or services.	Ballot Delivery Test Case Penetration Test Case	
5.6.3	**System Event Logging**		
	This section describes requirements for the voting system to perform event logging for system maintenance troubleshooting, recording the history of system activity, and detecting unauthorized or malicious activity. The operating system, and/or applications software may perform the actual event logging. There may be multiple logs in use for any system component.		
5.6.3.1	The voting system SHALL log the following data for each event: a. System ID; b. Unique event ID and/or type; c. Timestamp; d. Success or failure of event, if applicable; e. User ID triggering the event, if applicable; and f. Jurisdiction, if applicable.	Administration Test Case Ballot Delivery Test Case Recovery form hardware error Test Case Penetration Test Case	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix	Test Case Description	Wyle Comment
5.6.3.2	All critical events SHALL be recorded in the system event log.	Penetration Test Case Ballot Delivery Test Case Recovery form hardware error Test Case Registration Processing Test Case	This requirement does not define what a critical event might be.
5.6.3.3	At a minimum the voting system SHALL log the events described in the table below. NOTE: See "Table 5-2 System Events" in document - page 71	Administration Test Case Ballot Delivery Test Case Penetration Test Case Recovery form hardware error Test Case	Wyle was unable to completely validate this requirement due to limited access to physical hardware. The majority of the events defined are from a server OS level and not a web based application level.
5.7	**Incident Response**		
5.7.1	**Incident Response Support**		
5.7.1.1	Manufacturers SHALL document what types of system operations or security events (e.g., failure of critical component, detection of malicious code, unauthorized access to restricted data) are classified as critical.	N/A	Wyle determined that this requirement is not applicable to a web based application. But it is a requirement for a web server and therefore could not be tested at this time.
5.7.1.2	An alarm that notifies appropriate personnel SHALL be generated on the vote capture device, system server, or tabulation device, depending upon which device has the error, if a critical event is detected.	N/A	Wyle determined that this requirement is not applicable to a web based application. A system server notification should be sent to administrators when issues arise with the web server.
5.8	**Physical and Environmental Security**		
5.8.1	**Physical Access**		

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix	Test Case Description	Wyle Comment
5.8.1.1	Any unauthorized physical access SHALL leave physical evidence that an unauthorized event has taken place.	N/A	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.
5.8.2.1	The voting system SHALL disable physical ports and access points that are not essential to voting operations, testing, and auditing.	Host Server Security Test Case	
5.8.3.1	If a physical connection between the vote capture device and a component is broken, the affected vote capture device port SHALL be automatically disabled.	N/A	Wyle determined that this requirement is not applicable to a web based application. A physical connection will only be made during a single instance of vote casting.
5.8.3.2	The voting system SHALL produce a visual alarm if a connected component is physically disconnected.	N/A	Wyle determined that this requirement is not applicable to a web based application.
5.8.3.3	An event log entry that identifies the name of the affected device SHALL be generated if a vote capture device component is disconnected.	N/A	Wyle determined that this requirement is not applicable to a web based application.
5.8.3.4	Disabled ports SHALL only be re-enabled by authorized administrators.	Administration Test Case	
5.8.3.5	Vote capture devices SHALL be designed with the capability to restrict physical access to voting device ports that accommodate removable media with the exception of ports used to activate a voting session.	N/A	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.
5.8.3.6	Vote capture devices SHALL be designed to give a physical indication of tampering or unauthorized access to ports and all other access points, if used as described in the manufacturer's documentation.	N/A	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.
5.8.3.7	Vote capture devices SHALL be designed such that physical ports can be manually disabled by an authorized administrator.	N/A	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.
5.8.4	**Door Cover and Panel Security**		
5.8.4.1	Access points such as covers and panels SHALL be secured by locks or tamper evident or tamper resistant countermeasures and SHALL be implemented so that kiosk workers can monitor access to vote capture device components through these points.	N/A	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix	Test Case Description	Wyle Comment
5.8.5	**Secure Paper Record Receptacle**		
	If the voting system provides paper record containers then they SHALL be designed such that any unauthorized physical access results in physical evidence that an unauthorized event has taken place.	N/A	Wyle determined that this requirement is not applicable to a web based application
5.8.6	**Secure Physical Lock and Key**		
5.8.6.1	Voting equipment SHALL be designed with countermeasures that provide physical indication that unauthorized attempts have been made to access locks installed for security purposes.	N/A	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.
5.8.6.2	Manufacturers SHALL provide locking systems for securing vote capture devices that can make use of keys that are unique to each owner.	N/A	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.
5.8.7	**Media Protection**		
	These requirements apply to all media, both paper and digital, that contain personal privacy related data or other protected or sensitive types of information.		
5.8.7.1	The voting system SHALL meet the following requirements: a. All paper records (including rejected ones) printed at the kiosk locations SHALL be deposited in a secure container; b. Vote capture device hardware, software and sensitive information (e.g., electoral roll) SHALL be physically protected to prevent unauthorized modification or disclosure; and c. Vote capture device hardware components, peripherals and removable media SHALL be identified and registered by means of a unique serial number or other identifier.	N/A	Wyle determined that this requirement is not applicable to a web based application.
5.9	**Penetration Resistance**		
5.9.1	**Resistance to Penetration Attempts**		
5.9.1.1	The voting system SHALL be resistant to attempts to penetrate the system by any remote unauthorized entity.	Penetration Test Case Host Server Security Test Case	
5.9.1.2	The voting system SHALL be configured to minimize ports, responses and information disclosure about the system while still providing appropriate functionality.	Penetration Test Case Host Server Security Test Case	

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix	Test Case Description	Wyle Comment
5.9.1.3	The voting system SHALL provide no access, information or services to unauthorized entities.	Penetration Test Case Administration Test Case	
5.9.1.4	All interfaces SHALL be penetration resistant including TCP/IP, wireless, and modems from any point in the system.	Penetration Test Case	
5.9.1.5	The configuration and setup to attain penetration resistance SHALL be clearly and completely documented.	Penetration Test Case	Based on the system documentation provided by the participants in this test campaign, Wyle was unable to validate this requirement. However, Wyle deems it necessary for future testing.
5.9.2.1	The scope of penetration testing SHALL include all the voting system components. The scope of penetration testing includes but is not limited to the following: System server; Vote capture devices; Tabulation device; All items setup and configured per Technical Data Package (TDP) recommendations; Local wired and wireless networks; and03/09/2011 Internet connections.	Penetration Test Case	
5.9.2.2	Penetration testing SHALL be conducted on a voting system set up in a controlled lab environment. Setup and configuration SHALL be conducted in accordance with the TDP, and SHALL replicate the real world environment in which the voting system will be used.	Penetration Test Case	Wyle was unable to validate this requirement, but deems it necessary for future testing.
5.9.2.3	The penetration testing team SHALL conduct white box testing using manufacturer supplied documentation and voting system architecture information. Documentation includes the TDP and user documentation. The testing team SHALL have access to any relevant information regarding the voting system configuration. This includes, but is not limited to, network layout and Internet Protocol addresses for system devices and components. The testing team SHALL be provided any source code included in the TDP.	Penetration Test Case	Wyle was unable to validate this requirement, but deems it necessary for future testing.

UOCAVA Req. No.	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements Functional Requirements Matrix	Test Case Description	Wyle Comment
5.9.2.4	Penetration testing seeks out vulnerabilities in the voting system that might be used to change the outcome of an election, interfere with voter ability to cast ballots, ballot counting, or compromise ballot secrecy. The penetration testing team SHALL prioritize testing efforts based on the following: a. Threat scenarios for the voting system under investigation; b. Remote attacks SHALL be prioritized over in-person attacks; c. Attacks with a large impact SHALL be prioritized over attacks with a more narrow impact; and d. Attacks that can change the outcome of an election SHALL be prioritized over attacks that compromise ballot secrecy or cause non-selective denial of service.	Penetration Test Case	

ATTACHMENT B

TEST CASES

Test Case:	Test Case 10 Local Ballot Delivery System A	
Test Objective:		**Test Configuration:**
Verify functional operation and basic security of the system with the client and server residing on the same device.		The client and server software are located on the same PC
Devices Utilized:	Server: Apple PowerPC G4 CPU, OS X 10.5.8 Client: Safari 5.0.4	

Step	Procedure	Notes
0	Record start time and date, hardware models and serial numbers, software versions for system test. Record physical location of equipment (remote / local). Get voter names and credentials from the list provided by Vendor.	
10000	Log on by starting the Safari Browser and clicking on the '[redacted]' user button and log in as the first user available on the list.	[redacted]
30000	Perform authentication necessary to access ballot distribution pages.	Images saved.
40000	Complete forms, options required by server to download a ballot. Record your inputs.	Ballot received.
45000	Verify that the system's ballot summary screen matches the election for your location.	N/A
50000	Download the ballot.	Ballot saved as pdf.
65000	Close the window (click on red button) and log off the voting system -- do not exit safari.	Exited.
70000	Attempt to print a second ballot - attempt to vote the ballot and then print. Attempt to reprint the ballot using a different delivery option (mail, email, fax).	Only one ballot option is available. Ballot can have unlimited modifications and unlimited copies.
90000	Sign out or log off the voting system.	N/A
100000	Attempt to view all temporary files to verify no sensitive information is left on the voting device. (cookies, history pages)	Using browser back button reveals all log in information.
110000	Log in as the same voter.	There is not limit on the number of times that a voter can log in and download a ballot.
120000	Attempt to print or cast a second ballot.	There is not limit on the number of times that a voter can log in and download a ballot.
130000	Log out as this user.	N/A
135000	Use "Preview" by double-clicking on the file in the finder and then fill out the ballot and associated forms and print them.	N/A
140000	Log in as administrator. View and dump all reports. Verify that all events for all users that voted are logged.	Logs retained.
150000	Dump all logs and collect screen prints, etc. Record end time.	Logs retained.
160000	END	

1

Test Case: Test Case 01 Host Server Administration (System A)	
Test Objective:	**Test Configuration:**
This test case verifies the roles of system administrator and the ability to maintain user roles, passwords, logs and other voting system administrative functions.	Host server with two terminals.
Devices Utilized:	Server: Apple PowerPC G4 CPU, OS X 10.5.8, Desktop PC with IE browser (for admin access to server), Client PC: Safari 5.0.4 (for simulating voter activity)

Step	Procedure	Notes
0	Record time and date of test, record hardware models, serial numbers and software versions	
10000	Log in as a non-administrative (operating system) account but as a voting system administrator. (BTA/chang3m3)	Log in successful.
20000	Exercise every option to view the logs, errors, activity reports, admin users.	Only has log information.
30000	View user list and attempt to add user, assign role, delete user, and reassign roles to existing user.	N/A - not possible on this system
40000	Log in as voting system super-user role, create new user and verify default role is the least privileged	N/A - not possible on this system
50000	Log in as user just created (low privileges) user and attempt to change higher priority role and / or privileges.	N/A - not possible on this system
60000	Log out and log in as super user and attempt to view storage in server such that unencrypted passwords, etc. are detected??/	N/A - not possible on this system
70000	Reset password for existing user, perform password administration such as setting minimum required password length, type of characters, capitals, etc. per NIST 800-63. (user name cannot be part of password)	N/A - not possible on this system
80000	If possible, attempt to disable/ enable the network interface.	N/A - not possible on this system
90000	Verify password histories are maintained and that user cannot reuse passwords according to the password length requirement.	N/A - not possible on this system
100000	Verify that passwords automatically expire at a specified length of time and attempt to use a password containing the user name and verify that it is rejected. (may need to set expiration date on next day and then verify after that date)	N/A - not possible on this system
110000	As administrator (super user), record default settings for log control (rqmt 5.6.1.1) verify logs are append only and read-only for authorized roles ____ verify it is not possible to alter the log..	Logs are in order by date and time.
120000	Attempt to create log failure and verify that log events, such as errors or rotation are recorded. Attempt to clear log and verify that action is	Clearing log and exporting logs are not accessible at a non-system level.

	logged. Then export the log for storage (5.6.1.8)	
130000	View log and verify it is in a publicly documented format, such as XML, or include a utility to export log data into a publicly documented format and that it has not data violating privacy. Search log and exercise any analysis tools	N/A - not possible on this system
140000	Attempt to monitor real-time reporting of system events. Log in as super admin and view any logs / reports that may provide real-time monitoring of the system activity - especially of logged on users (Check for OS capability external to voting system.)	Login attempts are logged.
150000	Attempt to log in with an invalid administrator user ID Re-attempt until sufficient attempts cause the terminal to be locked out.(Login never locks)	There does not appear to be a limit on incorrect log in attempts.
155000	Log in, change the number of attempts threshold for locking out the terminal and then repeat the process.	N/A - not possible on this system
160000	Log in as a valid administrator and don't do anything - allow the system to time out. Then log back in and verity it requires reentry of the password.	Logged in 5/5/2011 8:47:51 AM. Admin is never logged out.
170000	Record date and time of test end, collect logs and all output records. Verify events are recorded with proper order and times verify entry includes system id, timestamp, event id, success/fail, and if applicable, user id and jurisdiction id	
180000	End of test – record time and date	

Result Test Sheet

Test Case: TC03 Crypto Test Sheet System A	
Test Objective:	**Test Configuration:**
This test case verifies that the cryptographic functionality implemented by the system meets/is NIST-approved and/or FIPS 140-2 compliant.	Full test System setup, fully functional and under normal operating conditions. Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link.
Devices Utilized:	Client: Dell optima Desktop at Wyle Laboratories. Server: make and model unknown

Step	Procedure	Notes
1000	Record time and date of test, record hardware models, serial numbers and software versions.	6/1/201, Win 7, IE 8 URL:
2000	Review System documentation for cryptographic algorithms and protocols implemented by the system and record them. **Note:** If keys are put into the voting system manually, read step 7 before continuing.	Could not perform. No documentation provided.
3000	Check to ensure that algorithms and protocols used have gone through the Cryptographic Algorithm Validation Program or FIPS 140-2 approved. If not, that the appropriate waiver has been applied for from NIST. Additionally, check tables in SP 800-57 and ensure algorithms are at 112 bit level.	Could only check protocols used on client browser side, due to not having access to the system. Connection: TLS 1.0 AES 128 bit, RSA 2048 bit Cert: Issuer – Go Daddy, class 2, sign algorithm Sha1RSA, hash Sha1
4000	Log into system with administrative privileges. Manually verify or pull using script the permissions on appropriate cryptographic applications and files.	Could not perform. No administrative credentials provided. Only application admin credentials provided.
4100	Verify that permissions are restricted and not writable by voting system application. Record and document all observations.	Could not perform. No access to system other than client side browser connection.
5000	Pull the hash values for the cryptographic keys from the system.	Could not perform. No access to system.
6000	Check hash lengths to ensure the crypto modules are using a correct strength algorithm.	Not performed, see step 5.
7000	If keys are input manually into system, vary the key by only changing one value slightly. (e.g. Key starts with a "T" use a "t" on second entry.) Follow any system instructions to load key before starting to pull logs and data.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
7100	If system only holds and allows one key/hash; pull hash; then re-log into system reenter key following system instructions; then re-pull hash.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
7200	If the system allows more than one hash; then follow systems instruction for a specific key set then re-enter same key set changing the key as described in main step; then pull hashes.	Not performed, see step 7.
7300	Compare the hashes with the slight change; there should be significant change in hash value. Record observations.	Not performed, see step 7.

Result Test Sheet

8000	Review voting system software source code. Verify that crypto modules are being called in the correct manner to meet NIST requirements and 112 bit encryption. **Note:** The application doing the encryption maybe FIPS 140-2 compliant but, the voting application (i.e. Java code call to crypto module.) could use wrong method to encrypt at proper strength.	Not performed, code not provided.
9000	Key Management, Perform this step if cryptographic keys are generated internally. Review voting system documentation to see what type encryption methods is deployed.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
9100	Review source code and take note to ensure that methods used comply with FIPS 140-2. This should be done by referring to annex A, C or D of 140-2. Record all observations and discrepancies.	Not performed, code not provided.
9200	Pull file permissions of those executable and library files in the system. Ensure they have restricted access and are properly controlled. Record all observations.	No access to system other than application usage. This step Not performed.
10000	Perform key entry procedures following voting system documentation. Verify that input and output are NIST compliant.	No access to system other than application usage. This step Not performed.
10100	If automated method is used input and output from system must be encrypted. Record observations.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
10200	If a manual method is used input and output from system maybe plaintext. Record observations. **Note:** Transportation and any other processes dealing with the input and output data should reviewed to verify proper security measures are being applied.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
11000	Perform Key zeroization procedures following voting system documentation. Verify that the key no longer exist on the system after completion of procedure. Record all observations.	Not performed, see step 10.
12000	Perform rekeying procedures following voting system documentation. Verify the system performs as documented and is compliant. Record all observations.	Not performed, see step 10.
13000	During Operational tests, ensure that the voting system supports rekeying during communications. This should be done by verifying protocols used and/or sniffing network traffic and examining the packets. **Note:** System documentation should but may not state the amount or limit of data encrypted with the same key. The key could change on a daily basis, when a pre-set volume of data has been transmitted or a given period of time has elapsed.	Verified protocols being used but, did not monitor traffic due to the whole system not being in Wyle testing lab.

Result Test Sheet

	Most systems, implement rekeying by forcing a new key exchange, typically through a separate protocol like Internet key exchange (IKE). (e.g. Wi-Fi Protected Access (WPA), does this by frequently replacing session keys through the Temporal Key Integrity Protocol (TKIP))	
14000	During Operational tests, ensure that the voting system uses NIST or FIPS approved protocols for communications. Record all observations. **Note:** This should be done by sniffing network traffic (i.e. Wireshark) and examining the packets.	Verified protocols being used from client side browser.
15000	End of test – record time and date	6/1/2011

Additional Notes:

- Only IE browser tested.
- Side issues – web browser can be any type and Adobe any version. This can lead to issues surrounding a compromised machine being used on client side. Should be further tested (possibly as part of pen test).

Result Test Sheet

Test Case: 05 Discovery Penetration System A	
Test Objective:	**Test Configuration:**
This test seeks out vulnerabilities in the voting system, verifies the system's resistance to any remote unauthorized entity. That the system provides no access, information or services to unauthorized entities and is configured to minimize ports and information disclosure about the system.	Full System with host, remote terminal and communication devices. Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link. Full test System setup, fully functional and under normal operating conditions.
Devices Utilized:	BackTrack OS with Nessus Laptop

Step	Procedure	Notes
1000	Record time and date of test start, model and serial number of hardware, software with version numbers.	12:30 6/8/2011 HP Pavilion dv6 laptop running Backtrack 4 R2 as OS with Nessus installed. Nessus version : 4.4.1 feed ver. : 201105041534 Scanner MAC : 00:0f:00:3a:3b:c7 Scanner IP : 10.10.13.124 Metasploit v3.7.0 svn r12540
2000	Record IP and URL addresses to be tested.	[redacted]
3000	Scan IP and URL ranges with Nmap, unobtrusive.	Port 80, 443 open. Apple Mac OS X 10.6.X|10.5.X (86%) file: [redacted]
4000	Scan from inside target/s netmask range. Save results to file.	N/A
5000	Scan target/s from outside interfaces. Save results to file.	See step 3.
6000	If needed and applicable, scan IP and URL ranges with Nmap, aggressive. Save results to file.	Not required.
7000	Scan IP and URL ranges with Nessus, unleveraged "no credentials". Save scan result, in file name indicate unleveraged.	Scanned with Nessus polices (see files); Web Apps- [redacted] External- [redacted]
8000	Scan from inside target/s netmask range. Save results, indicating "inside" (e.g. system_noC_in.xml)	N/A
9000	If applicable, scan target/s from outside interfaces. Save results, indicating "outside" (e.g. system_noC_out.xml)	See step 7.
10000	Scan IP and URL ranges with Nessus, leveraged "with credentials". Save scan result, in file name indicating leveraged. Note: This type scan is usually done from "inside" only.	Not done, no credentials were provided.
11000	Probe target URL for further information. (i.e. URL manipulation, input/form field manipulation, SQL injection, etc.) Record all observations and displayed information.	Simple SQL injection not effective.
12000	Review all scan results and recorded information.	2 open ports, 11 low vulnerabilities, scans hung no OS detection
13000	Annotate record and organize all pertinent information (e.g. Ports, Protocols, Services, versioning, etc.) from	Done.

Result Test Sheet

	the results for second phase of Pen test.	
14000	From review of pertinent information, setup/develop and additional discovery scans/tests as needed.	Not needed.
15000	Perform any additional discovery scans or tests as needed. Save and record these results.	N/A
16000	Review all results, notes and finalize exploratory tests for second phase of testing.	With time restrictions went with port exploits as primary attack method. Also, attempt login with application credentials.
17000	End of test – record time and date	14:20 6/8/2011

Additional Notes:

- Nessus web scan hung at 90%. Restarted but due to time restrictions had to stop before completion.
- Metasploit port attacks were used (examples; webdav_upload_upload_asp, hagent_untrusted_hsdata, RealServer describe Buffer Overflow).
- None of attempted exploits succeeded. More detailed attempts against the OS or more detailed SQL attempts maybe successful but, require more time than was currently allocated.

Test Case:	Test Case 01 Host Server Administration System B	
Test Objective:		**Test Configuration:**
This test case verifies the roles of system administrator and the ability to maintain user roles, passwords, logs and other voting system administrative functions.		Host server accessed through a secure link via the internet to URL (TBS)
Devices Utilized:	Client: Dell Optiplex 780, Server: provided by Microsoft Azure Cloud Service	

Step	Procedure	
0	Record time and date of test, record hardware models, serial numbers and software versions	
10000	Log in with the administrative account provided by the vendor. (this is an "administrator" role with full privileges)	"wyle@[redacted]" pass: "wyle"
20000	Dump system Logs. Then view the logs and save. Attempt to change and/or reset the log. Verify they cannot be altered.	Only log available is for voter log in . Other logs are not developed.
30000	View user list and attempt to add user, assign role, delete user, and reassign roles to existing user.	Add User page currently does not function.
40000	Log in as voting system administrator (full privileges) role, create a new user and verify default role is the least privileged. Note information entered for this user and add one more user for each administrator role.	Add User page currently does not function.
50000	Perform a series of log-ins, one for each role, and attempt to exercise privileges not allowed for that role, verify each role can only view/modify the items there are authorized..	Only have one admin user. Add user function currently not working.
60000	Log out and log in as super user and attempt to view storage in server such that unencrypted passwords, etc are detected??/	User information can not currently be edited.
70000	Reset password for existing user, perform password administration such as setting minimum required password length, type of characters, capitals, etc. per NIST 800-63. (user name cannot be part of password)	Currently a password of one character is acceptable. No history of passwords is retained and password can match log in.
90000	Verify password histories are maintained and that user cannot reuse passwords according to the password length requirement. Attempt to use a password containing the user name and verify that it is rejected.	No history of passwords is retained and password can match log in.
100000	Verify that passwords automatically expire at a specified length of time. (may need to set expiration date on next day and then verify after that date)	There is not expiration for passwords.
110000	As administrator (super user), record default settings for log control (rqmt 5.6.1.1) verify logs are append only and read-only for authorized roles ____ verify it is not possible to alter the log..	Only log is for voter log in information. This log is appended.

120000	Attempt to create log failure and verify that log events, such as errors or rotation are recorded. Attempt to clear log and verify that action is logged. Then export the log for storage (5.6.1.8)	Log has recorded an attempted login failure.
130000	View log and verify it is in a publicly documented format, such as XML, or include a utility to export log data into a publicly documented format and that it has not data violating privacy. Search log and exercise any analysis tools	Log is not exportable.
140000	Attempt to monitor real-time reporting of system events. Log in as super admin and view any logs / reports that may provide real-time monitoring of the system activity - especially of logged on users (Check for OS capability external to voting system.)	Voter log is real time.
150000	Attempt to log in with an invalid administrator user ID Re-attempt until sufficient attempts cause the terminal to be locked out.	System does not lock out an admin.
155000	Log in, change the number of attempts threshold for locking out the terminal and then repeat the process.	System does not support this from an admin page.
160000	Log in as a valid administrator and don't do anything - allow the system to time out. Then log back in and verity it requires reentry of the password.	No timeout after an hour.
165000	Export the voting system log to external device for archiving	No export option.
170000	Record date and time of test end, collect logs and all output records. Verify events are recorded with proper order and times verify entry includes system id, timestamp, event id, success/fail, and if applicable, user id and jurisdiction id	No logs to record.
180000	End of test – record time and date	

Result Test Sheet

Test Case: 03 Crypto Test Sheet System B	
Test Objective:	**Test Configuration:**
This test case verifies that the cryptographic functionality implemented by the system meets/is NIST-approved and/or FIPS 140-2 compliant.	Full test System setup, fully functional and under normal operating conditions. Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link.
Devices Utilized:	Client: Dell optima Desktop at Wyle Laboratories. Server: make and model unknown

Step	Procedure	Notes
1000	Record time and date of test, record hardware models, serial numbers and software versions.	17:50 6/14/2011. Win 7. IE 8 URL: [redacted]
2000	Review System documentation for cryptographic algorithms and protocols implemented by the system and record them. **Note:** If keys are put into the voting system manually, read step 7 before continuing.	Could not perform. No documentation provided.
3000	Check to ensure that algorithms and protocols used have gone through the Cryptographic Algorithm Validation Program or FIPS 140-2 approved. If not, that the appropriate waiver has been applied for from NIST. Additionally, check tables in SP 800-57 and ensure algorithms are at 112 bit level.	Could only check protocols used on client browser side, due to not having access to the system. Admin account page had NO cert! Connection: TLS 1.0 AES 128 bit, RSA 2048 bit Cert: Issuer – Go Daddy, class 3, sign algorithm Sha1RSA, hash Sha1
4000	Log into system with administrative privileges. Manually verify or pull using script the permissions on appropriate cryptographic applications and files.	Could not perform. No administrative credentials provided. Only application admin credentials provided.
4100	Verify that permissions are restricted and not writable by voting system application. Record and document all observations.	Could not perform. No access to system other than client side browser connection.
5000	Pull the hash values for the cryptographic keys from the system.	Could not perform. No access to system.
6000	Check hash lengths to ensure the crypto modules are using a correct strength algorithm.	Could not perform. No access to system.
7000	If keys are input manually into system, vary the key by only changing one value slightly. (e.g. Key starts with a "T" use a "t" on second entry.) Follow any system instructions to load key before starting to pull logs and data.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
7100	If system only holds and allows one key/hash; pull hash; then re-log into system reenter key following system instructions; then re-pull hash.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
7200	If the system allows more than one hash; then follow systems instruction for a specific key set then re-enter same key set changing the key as described in main step; then pull hashes.	Not performed, see step 7.
7300	Compare the hashes with the slight change; there should be significant change in hash value. Record observations.	Not performed, see step 7.

Result Test Sheet

8000	Review voting system software source code. Verify that crypto modules are being called in the correct manner to meet NIST requirements and 112 bit encryption. **Note:** The application doing the encryption maybe FIPS 140-2 compliant but, the voting application (i.e. Java code call to crypto module.) could use wrong method to encrypt at proper strength.	Not performed, code not provided.
9000	Key Management, Perform this step if cryptographic keys are generated internally. Review voting system documentation to see what type encryption methods is deployed.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
9100	Review source code and take note to ensure that methods used comply with FIPS 140-2. This should be done by referring to annex A, C or D of 140-2. Record all observations and discrepancies.	Not performed, code not provided.
9200	Pull file permissions of those executable and library files in the system. Ensure they have restricted access and are properly controlled. Record all observations.	No access to system other than application usage. This step Not performed.
10000	Perform key entry procedures following voting system documentation. Verify that input and output are NIST compliant.	No access to system other than application usage. This step Not performed.
10100	If automated method is used input and output from system must be encrypted. Record observations.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
10200	If a manual method is used input and output from system maybe plaintext. Record observations. Note: Transportation and any other processes dealing with the input and output data should reviewed to verify proper security measures are being applied.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
11000	Perform Key zeroization procedures following voting system documentation. Verify that the key no longer exist on the system after completion of procedure. Record all observations.	No access to system other than application usage. This step Not performed.
12000	Perform rekeying procedures following voting system documentation. Verify the system performs as documented and is compliant. Record all observations.	No access to system other than application usage. This step Not performed.
13000	During Operational tests, ensure that the voting system supports rekeying during communications. This should be done by verifying protocols used and/or sniffing network traffic and examining the packets. Note: System documentation should but may not state the amount or limit of data encrypted with the same key. The key could change on a daily basis, when a pre-set volume of data has been transmitted or a given period of time has elapsed.	Verified protocols being used but, did not monitor traffic due to the whole system not being in Wyle testing lab.

Result Test Sheet

	Most systems, implement rekeying by forcing a new key exchange, typically through a separate protocol like Internet key exchange (IKE). (e.g. Wi-Fi Protected Access (WPA), does this by frequently replacing session keys through the Temporal Key Integrity Protocol (TKIP))	
14000	During Operational tests, ensure that the voting system uses NIST or FIPS approved protocols for communications. Record all observations. **Note:** This should be done by sniffing network traffic (i.e. Wireshark) and examining the packets.	Verified protocols being used from client side browser.
15000	End of test – record time and date	18:48 6/14/2011

Additional Notes:

- Only IE browser tested.

Test Case: Test Case 04 Normal Ballot Delivery System B	
Test Objective:	**Test Configuration:**
One ballot will be delivered to the terminal and displayed and/or printed to exercise the normal processing path for delivery of ballot. The test will verify that: 1. The system delivers that ballot to the voter 2. The system implements authentication prior to allowing the voter access to the ballot. 3. The system adequately logs the event of transferring the ballot. 4. The ballot that is delivered is identical to the ballot that was provided by the Election Management System.	Host server accessed through a secure link via the internet to URL (TBS)
Devices Utilized:	Client: Dell Optiplex 780, Server: provided by Microsoft Azure Cloud Service

Step	Procedure	
0	Record start time and date, hardware models and serial numbers, software versions for system test. Record physical location of equipment (remote / local) :::HOT KEYS;<ctrl ;> for current date, <ctrl shift ;> for time.	
10000	Log on as a voter to the system (a non-administrator account on this terminal) .(during the following steps, record each action and response by the system so that at the end, we can verify that all significant events were logged)	Sample Voter (NP) 123 Sample Drive, Springfield 12345
30000	Perform authentication necessary to access ballot distribution pages.	Only requires a 5 digit pin.
40000	Select ballot from list and note which one you selected. Select Mail as delivery option.	Sample Voter (NP) 123 Sample Drive, Springfield 12345 received error message for coding error.
50000	Download the ballot package	Download ballots do not contain all the information necessary for returning the ballot.
60000	If voting is an option, then do NOT vote at this time and print the ballot.	Ballot not voted
70000	Attempt to print a second ballot - attempt to vote the ballot and then print. Attempt to reprint the ballot using a different delivery option (mail, email, fax) (Attempt to use browser back button to return to options)	No limit on reprints.
80000	Repeat step selection mark and print option	Same voter can vote again.
90000	Sign out or log off as this voter. Repeat step using mark and save option with new voter. (using email option)	Ballot marked and saved
100000	View all temporary files to verify no voting information is left on the voting device.	The browser back button allows someone to return to the previous ballot.
110000	Log in as the same voter	No limit in place to stop voters from voting multiple times.

120000	Attempt to print or cast a second ballot	Can get unlimited ballots.
140000	Log off -- and log in as administrator. View and dump logs. Verify that all events for all users that voted are logged. If on the same terminal as voter, then search for files/temporary storage that contains any voter information.	Log records voter actions.
150000	Examine and Dump all logs and collect screen prints, etc. On both the server and the client.	No other logs available.
160000	End of test – record time and date	

Result Test Sheet

Test Case: 05 Discovery Penetration System B	
Test Objective:	**Test Configuration:**
This test seeks out vulnerabilities in the voting system, verifies the system's resistance to any remote unauthorized entity. That the system provides no access, information or services to unauthorized entities and is configured to minimize ports and information disclosure about the system.	Full System with host, remote terminal and communication devices. Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link. Full test System setup, fully functional and under normal operating conditions.
Devices Utilized:	BackTrack OS with Nessus Laptop

Step	Procedure	Notes
1000	Record time and date of test start, model and serial number of hardware, software with version numbers.	16:35 6/14/2011 HP Pavilion dv6 laptop running Backtrack 4 R2 as OS with Nessus installed. Nessus version : 4.4.1 feed ver. : 201105041534 Scanner MAC : 00:0c:43:78:6e:ca Scanner IP : 10.10.13.124 Metasploit v3.7.0 svn r12540
2000	Record IP and URL addresses to be tested.	[redacted]
3000	Scan IP and URL ranges with Nmap, unobtrusive.	Port 21, 22, 80 and 443 open. Linux 2.6.18 (93%) file: [redacted]
4000	Scan from inside target/s netmask range. Save results to file.	N/A
5000	Scan target/s from outside interfaces. Save results to file.	See step 3.
6000	If needed and applicable, scan IP and URL ranges with Nmap, aggressive. Save results to file.	Not required.
7000	Scan IP and URL ranges with Nessus, unleveraged "no credentials". Save scan result, in file name indicate unleveraged.	Scanned with Nessus polices (see files); Web Apps- [redacted] External- [redacted]
8000	Scan from inside target/s netmask range. Save results, indicating "inside" (e.g. system_noC_in.xml)	N/A
9000	If applicable, scan target/s from outside interfaces. Save results, indicating "outside" (e.g. system_noC_out.xml)	See step 7.
10000	Scan IP and URL ranges with Nessus, leveraged "with credentials". Save scan result, in file name indicating leveraged. Note: This type scan is usually done from "inside" only.	Not done, no credentials were provided.
11000	Probe target URL for further information. (i.e. URL manipulation, input/form field manipulation, SQL injection, etc.) Record all observations and displayed information.	Simple SQL injection not effective. Did however gather good information, with more time could have possible gained access. See file error_withInfo.png for example.
12000	Review all scan results and recorded information.	4 open ports, 1 medium and 45 low vulnerabilities, Linux 2.6
13000	Annotate record and organize all pertinent information (e.g. Ports, Protocols, Services, versioning, etc.) from	Done.

Result Test Sheet

	the results for second phase of Pen test.	
14000	From review of pertinent information, setup/develop and additional discovery scans/tests as needed.	Not needed.
15000	Perform any additional discovery scans or tests as needed. Save and record these results.	N/A
16000	Review all results, notes and finalize exploratory tests for second phase of testing.	With time restrictions went with port exploits as primary attack method. Also, attempt login with application credentials.
17000	End of test – record time and date	18:37 6/14/2011

Additional Notes:

- More time on pen test or closer to the parameters of requirement to white box testing and access to system would most likely occur.
- Metasploit port attacks were used (examples; webdav_upload_upload_asp, hagent_untrusted_hsdata, RealServer describe Buffer Overflow).
- None of attempted exploits succeeded. More detailed attempts against the OS or more detailed SQL attempts maybe successful but, require more time than was currently allocated.

Test Case: Test Case 01 Host Server Administration System C	
Test Objective:	**Test Configuration:**
This test case verifies the roles of system administrator and the ability to maintain user roles, passwords, logs and other voting system administrative functions.	Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link.
Devices Utilized:	Client: Dell optima Desktop at Wyle Laboratories. Server: make and model unknown

Step	Procedure	Notes
1000	Record time and date of test, record hardware models, serial numbers and software versions	
2000	Log in with the administrative account provided by the vendor. (This is an "administrator" role vs. the less privileged "operator" role.	Login admin Wyleadmin / #20wyle11#
3000	Dump system logs. Then view the logs and compare them to the report listed in the "audit" screen.	The Audit screen showed events that are not in the event log.
4000	View user list and add one user with "administrator" privileges and two with "operator" privileges. Note the name, password and role for each user. Verify default role is "operator". Create one password containing the user name.	Entered name "Wyle Tester", username "Wyletester", password "wyle", no role selected. It responded with "password strength not correct" tried "wyle11" and still not good, tried "Wyle11" - no, tried "wylelabs" no, tried "wylelab11" - it took that and gave me administrator role as default. Entered Wyle operator, user name "wyleoperator", password "wyleoperator". got "password strength not correct" entered password of "wyleoperator11" same result, tried "wyleoperator1A" Password strength not correct, tried "Wyleoperator11" not good enough, tried "WWyleoperator 11" tried changed last name to "Wyleoperator", password to "Wyleoperator" and it failed again. Tried password "WWyleoperator11", no; tried "wylelab11" - it took it. Apparently it does not allow "user name" in the password. Added wyle "operatortwo", username "operatortwo", password "wylelab12" as operator role.
5000	Exercise the search options on the "user management" screen. Search for "user name", for "role", for all and for combination of user name and role.	Searched on name "Wyle" and it found the correct users. It found users ok when I selected "administrator role" and for "operator role". Selected name of "Wyle testers" with no role criteria and it did not find it. Selected "tester" and it found it. Selected "operator" and it found the two with last names containing "operator".
6000	Edit an administrator with "operator" role by changing all fields, note the changes and save them. Select a user with "administrator" privilege and modify the username and save	Changed entry for "wyle operatortwo", to "replace1 replace2", replaceusername, "Twylelab11", "Twylelab11" and role change to administrator. It accepted the changes.
7000	Log in as user just created (operator) user and attempt to change higher priority role and / or privileges.	Logged out and logged back in as "operatortwo", "wylelab11". It did not allow access to "user management". Could not change roles or any information about "operatortwo".

8000	As operator, attempt to perform each administrator function and note which ones are allowed to take on "operator" role.	Attempted to access the "security question" - was logged out. Tried two more times and was logged out each time. Could not perform any of the functions on the bottom of the administrative screen where a administrator password is required.
9000	Log out and log back in as an administrator with "administrator" role.	Logged in.
10000	Reset password for existing user, perform password administration such as setting minimum required password length, type of characters, capitals, etc. per NIST 800-63. (user name cannot be part of password)	Password is not configurable from admin screen.
11000	If possible, attempt to disable/ enable the network interface.	Not possible from here.
12000	Verify password histories are maintained and that user cannot reuse passwords according to the password length requirement.	There is nothing in place to limit reusing historical passwords.
13000	Verify that passwords automatically expire at a specified length of time and attempt to use a password containing the user name and verify that it is rejected. (may need to set expiration date on next day and then verify after that date)	Passwords containing the user names are not accepted. Need to verify what the password timeout period is.
14000	As administrator (super user), record default settings for log control (rqmt 5.6.1.1) verify logs are append only and read-only for authorized roles ____ verify it is not possible to alter the log. (do this for both the "audit" and "export" logs)	Audit log is not exportable. Exporting log contains admin log functions.
15000	Attempt to create log failure and verify that log events, such as errors or rotation are recorded. Attempt to clear log and verify that action is logged. Then export the log for storage (5.6.1.8) (do for both "audit" and "export" logs.	Logs only admin functions.
16000	Export log data into a publicly documented format and verify that it contains no data violating voter privacy. Search log -- do for both "audit" and "export" logs.	Audit log is not exportable. Exporting log contains admin log functions.
17000	Monitor real-time reporting of system events. View logs and if necessary, log in as a voter and verify that log is updated with voter actions.	Logs only admin functions and successful login attempts. No voter logins are recorded.
18000	Log out and then attempt to log in with an invalid administrator user ID Re-attempt until sufficient attempts cause the terminal to be locked out.	Attempted to log in as "wyle". Logged in 12 times with incorrect password. User was never locked out.
19000	Log in, change the number of attempts threshold for locking out the terminal and then repeat the process.	This function not configurable.
20000	Log in as a valid administrator and don't do anything - allow the system to time out. Then log back in and verity it requires reentry of the password.	System logs out after 5 minutes.

21000	Log in, allow the time to drop to 1 minute and then select an action or click on a button, anything that causes the system to reset the time.	Select another page - restarts counter at 5 minutes
22000	Record date and time of test end, collect logs and all output records. Verify events are recorded with proper order and times verify entry includes system id, timestamp, event id, success/fail, and if applicable, user id and jurisdiction id	Logs recorded and reviewed
23000	End of test – record time and date	

Result Test Sheet

Test Case: 03 Crypto Test Sheet System C	
Test Objective:	**Test Configuration:**
This test case verifies that the cryptographic functionality implemented by the system meets/is NIST-approved and/or FIPS 140-2 compliant.	Full test System setup, fully functional and under normal operating conditions. Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link.
Devices Utilized:	Client: Dell optima Desktop at Wyle Laboratories. Server: make and model unknown

Step	Procedure	Notes
1000	Record time and date of test, record hardware models, serial numbers and software versions.	6/1/2011, Win 7, IE 8 URL:
2000	Review System documentation for cryptographic algorithms and protocols implemented by the system and record them. **Note:** If keys are put into the voting system manually, read step 7 before continuing.	Could not perform. No documentation provided.
3000	Check to ensure that algorithms and protocols used have gone through the Cryptographic Algorithm Validation Program or FIPS 140-2 approved. If not, that the appropriate waiver has been applied for from NIST. Additionally, check tables in SP 800-57 and ensure algorithms are at 112 bit level.	Could only check protocols used on client browser side, due to not having access to the system. Connection: TLS 1.0 AES 128 bit, RSA 1024 bit Cert: Issuer – VeriSign, class 3, sign algorithm Sha1RSA, hash Sha1
4000	Log into system with administrative privileges. Manually verify or pull using script the permissions on appropriate cryptographic applications and files.	Could not perform. No administrative credentials provided. Only application admin credentials provided.
4100	Verify that permissions are restricted and not writable by voting system application. Record and document all observations.	Could not perform. No access to system other than client side browser connection.
5000	Pull the hash values for the cryptographic keys from the system.	Could not perform. No access to system.
6000	Check hash lengths to ensure the crypto modules are using a correct strength algorithm.	Could not perform. No access to system.
7000	If keys are input manually into system, vary the key by only changing one value slightly. (e.g. Key starts with a "T" use a "t" on second entry.) Follow any system instructions to load key before starting to pull logs and data.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
7100	If system only holds and allows one key/hash; pull hash; then re-log into system reenter key following system instructions; then re-pull hash.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
7200	If the system allows more than one hash; then follow systems instruction for a specific key set then re-enter same key set changing the key as described in main step; then pull hashes.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
7300	Compare the hashes with the slight change; there should be significant change in hash value. Record observations.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.

1

Result Test Sheet

8000	Review voting system software source code. Verify that crypto modules are being called in the correct manner to meet NIST requirements and 112 bit encryption. **Note:** The application doing the encryption maybe FIPS 140-2 compliant but, the voting application (i.e. Java code call to crypto module.) could use wrong method to encrypt at proper strength.	Not performed, code not provided.
9000	Key Management, Perform this step if cryptographic keys are generated internally. Review voting system documentation to see what type encryption methods is deployed.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
9100	Review source code and take note to ensure that methods used comply with FIPS 140-2. This should be done by referring to annex A, C or D of 140-2. Record all observations and discrepancies.	Not performed, code not provided.
9200	Pull file permissions of those executable and library files in the system. Ensure they have restricted access and are properly controlled. Record all observations.	No access to system other than application usage. This step Not performed.
10000	Perform key entry procedures following voting system documentation. Verify that input and output are NIST compliant.	No access to system other than application usage. This step Not performed.
10100	If automated method is used input and output from system must be encrypted. Record observations.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
10200	If a manual method is used input and output from system maybe plaintext. Record observations. **Note:** Transportation and any other processes dealing with the input and output data should reviewed to verify proper security measures are being applied.	Unknown, system documentation not provided. No access to system other than application usage. This step Not performed.
11000	Perform Key zeroization procedures following voting system documentation. Verify that the key no longer exist on the system after completion of procedure. Record all observations.	No access to system other than application usage. This step Not performed.
12000	Perform rekeying procedures following voting system documentation. Verify the system performs as documented and is compliant. Record all observations.	No access to system other than application usage. This step Not performed.
13000	During Operational tests, ensure that the voting system supports rekeying during communications. This should be done by verifying protocols used and/or sniffing network traffic and examining the packets. **Note:** System documentation should but may not state the amount or limit of data encrypted with the same key. The key could change on a daily basis, when a pre-set volume of data has been transmitted or a given period of time has elapsed.	Verified protocols being used but, did not monitor traffic due to the whole system not being in Wyle testing lab.

Result Test Sheet

	Most systems, implement rekeying by forcing a new key exchange, typically through a separate protocol like Internet key exchange (IKE). (e.g. Wi-Fi Protected Access (WPA), does this by frequently replacing session keys through the Temporal Key Integrity Protocol (TKIP))	
14000	During Operational tests, ensure that the voting system uses NIST or FIPS approved protocols for communications. Record all observations. **Note:** This should be done by sniffing network traffic (i.e. Wireshark) and examining the packets.	Verified protocols being used from client side browser.
15000	End of test – record time and date	6/1/2011

Additional Notes:

- Only IE browser tested.
- Side issue – No browser restriction, web browser can be any type. This can lead to issues surrounding a compromised machine being used on client side.

Result Test Sheet

Test Case: 05 Discovery Penetration System C	
Test Objective:	**Test Configuration:**
This test seeks out vulnerabilities in the voting system, verifies the system's resistance to any remote unauthorized entity. That the system provides no access, information or services to unauthorized entities and is configured to minimize ports and information disclosure about the system.	Full System with host, remote terminal and communication devices. Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link. Full test System setup, fully functional and under normal operating conditions.
Devices Utilized:	BackTrack OS with Nessus Laptop

Step	Procedure	Notes
1000	Record time and date of test start, model and serial number of hardware, software with version numbers.	15:10 6/1/2011 HP Pavilion dv6 laptop running Backtrack 4 R2 as OS with Nessus installed. Nessus version : 4.4.1 feed ver. : 201105041534 Scanner MAC : 00:02:16:09:de:66 Scanner IP : 10.10.13.123 Metasploit v3.7.0 svn r12540
2000	Record IP and URL addresses to be tested.	[redacted]
3000	Scan IP and URL ranges with Nmap, unobtrusive.	Port 80, 443 open. Server 2008 (90%) file: [redacted]
4000	Scan from inside target/s netmask range. Save results to file.	N/A
5000	Scan target/s from outside interfaces. Save results to file.	See step 3.
6000	If needed and applicable, scan IP and URL ranges with Nmap, aggressive. Save results to file.	Not required.
7000	Scan IP and URL ranges with Nessus, unleveraged "no credentials". Save scan result, in file name indicate unleveraged.	Scanned with Nessus polices (see files); Web Apps- [redacted] External- [redacted]
8000	Scan from inside target/s netmask range. Save results, indicating "inside" (e.g. system_noC_in.xml)	N/A
9000	If applicable, scan target/s from outside interfaces. Save results, indicating "outside" (e.g. system_noC_out.xml)	See step 7.
10000	Scan IP and URL ranges with Nessus, leveraged "with credentials". Save scan result, in file name indicating leveraged. Note: This type scan is usually done from "inside" only.	Not done, no credentials were provided.
11000	Probe target URL for further information. (i.e. URL manipulation, input/form field manipulation, SQL injection, etc.) Record all observations and displayed information.	Simple SQL injection not effective.
12000	Review all scan results and recorded information.	2 open ports, 22 low vulnerabilities, Windows Server 2008 R2
13000	Annotate record and organize all pertinent information (e.g. Ports, Protocols, Services, versioning, etc.) from	Done.

Result Test Sheet

	the results for second phase of Pen test.	
14000	From review of pertinent information, setup/develop and additional discovery scans/tests as needed.	Not needed.
15000	Perform any additional discovery scans or tests as needed. Save and record these results.	N/A
16000	Review all results, notes and finalize exploratory tests for second phase of testing.	With time restrictions went with port exploits as primary attack method. Also, attempt login with application credentials.
17000	End of test – record time and date	17:40 6/1/2011

Additional Notes:

- Metasploit port attacks were used (examples; webdav_upload_upload_asp, hagent_untrusted_hsdata, RealServer describe Buffer Overflow).
- None of attempted exploits succeeded. More detailed attempts against the OS or more detailed SQL attempts maybe successful but, require more time than was currently allocated.

Test Case:	Test Case 12 Voter Registration Request System C	
Test Objective:		**Test Configuration:**
This test case verifies that a voter can securely register to vote on-line. The test includes authentication that the voter is the voter that he/she claims to be and that the request is queued for processing by an election administrator.		The client connects to the ******* server via the Wyle LAN and internet connection using Internet Explorer. The port for access as a voting administrator is *****
Devices Utilized:	Client located at Wyle: Dell Desktop - OptiPlex 780, 2.0GB RAM, Windows 7 Professional, Internet Explorer 8.0.7600.16385, Wyle domain ai-engsvcs.com to internet connection. Server: make and model unknown, provided by [redacted] at their site.	

Step	Procedure	Notes
0	Record date and time, equipment with model numbers, server software versions.	-
10000	Log into the administrator screen, record statistics on screen (take a screen print) and select an unregistered voter for testing. (you will be selecting a number of voters from the list) Set "registration" voting on by clicking on the button to start it)	Logged in to admin screen as Wyleadmin/#20wyle11#, Dumped log to get initial content. Searched on "rejected voters" and stored snip of a list of available voters.
20000	Go to the voter registration screen -- ([redacted]) and using the voter credentials log in with the correct name, voter ID	At that screen, selected "vote" -- then went back and selected "Register".
27500	Select a voter that has not yet registered by searching on a name in the "electors" search screen.	Using [redacted] logged onto registration screen.
30000	Complete the registration screen by providing a valid email (yours) that you can access and a secret question with answer and the correct birth year for this voter. Submit that form. And click finish on the review screen -- close the browser.	Saved screen shot.
40000	Repeat the registration process with the same voter on each screen	Attempted to use the browser back button to re-enter registration information, but it gave me a "webpage has expired" message. I attempted to login under the "register" option, it gave the "Request with given NRC Id is already created" message. I then went back to the initial screen and selected the "voting" option. It rejected my log on with "Elector with given ID in not an eligible voter."
50000	Select a different voter from the unregistered voters in the database.	Selected unregistered voter [redacted]
60000	Using this voter, enter the ID, voter name correctly but enter an incorrect year.	Entered with year 2000. The vote request was accepted.
70000	Select a different voter from the unregistered voters in the database	Selected [redacted]
80000	Using this voter, enter the ID and Year correctly, but misspell the first name. Complete the registration process.	The previous screen was up, I pressed the browser back button and got the "web page expired" message. So then hit the browser "reload" button and it brought up the login

		screen - blank, no information from the previous voter. Entered voter as specified above - system rejected registration with a wrong first name -- "There is no elector with given parameters".
85000	Select a non-registered voter with no birth date in the database and do a valid registration.	Selected voter [redacted] no birth date. I entered a birth date of [redacted]. It confirmed that it has received the request.
90000	Select a different voter from the unregistered voters in the database	Selected [redacted]
100000	Using this voter, enter the ID and year correctly but misspell the last name and complete the registration process.	It rejected the request -- "there is no elector with given parameters"
110000	Select a different voter from the unregistered voters in the database	Selected [redacted]
120000	Enter invalid data into the login screen, click on Reset form	Entered invalid ID number -- it required me to enter the correct number of digits before it would give the green check mark. Selected "Reset" - form cleared all of the fields.
130000	Enter valid login information -- and proceed to the next screen.	Done.
140000	Enter information in the next form and use the reset button to clear the fields.	Done.
150000	Press the submit button with all fields clear	All fields lit up with red indicating they were required.
160000	Complete the form correctly except for year of birth and submit the form	It would not accept input. System required me to enter date in order to accept it
170000	Complete the form correctly except for the secret question / answer	Entered a valid date and removed the question -- it would not accept the form and highlighted the missing question box.
180000	Select the email option, complete the form but do not enter an email address	System would not accept the form without an email address.
190000	Select the email option, complete the form, but incorrectly enter the email confirmation address	System flagged the confirmation address and did not accept the form.
200000	Complete the form enter an incorrect year, do not enter an email address and select the "regular mail" option and submit the form but when the review screen appears, select "go back".	PM Erased the email addresses and clicked on the regular mail button. The email address remained in red with the notation that "this information is mandatory, please enter your email address". Scrolled up and it appeared. Clicked "extend" but it timed out while attempting to write the exception. Picked regular mail submitted it and selected "go back". The system went all the way back to the login screen and cleared all fields.
210000	Revise the year so that all data is correct and submit the registration request.	Re-enter log data. For voter [redacted] regular mail, selected "finish" on review screen and got confirmation message.

220000	Log off as a voter.	Done.
225000	From the list of unregistered voters, logon and enter requests for 8 more voters. Enter valid requests with matching information on at least 5 and incorrect dates on 3. Use a variety of email addresses - one of them with only one voter associated.	Enter voters -- [redacted]
230000	Log in as administrator, record statistics and view logs and verify that the requests have been queued. -- view pending requests and verify content of each request entered in this test.	Stored images of statistics screen and pending voters screen. Unable to view log requests on-line. The pending voters and the information for each one was correct.
250000	End of test record date and time of end.	

Test Case:	Test Case 13 Registration Processing System C
Test Objective:	**Test Configuration:**
This test case verifies the ability of the election administrator to view voter requests and accept or reject them based on successful comparison of the voter's credentials that were supplied by the voter to those that are known in the system database. The test will verify the acceptance/ rejection process and the notification to the voter. It will verify that all voter identification transmitted to the voter is protected against unauthorized access.	The client connects to the [redacted] server via the Wyle LAN and internet connection using Internet Explorer. The port for access as a voting administrator is [redacted]
Devices Utilized:	Client located at Wyle: Dell Desktop - OptiPlex 780, 2.0GB RAM, Windows 7 Professional, Internet Explorer 8.0.7600.16385, Wyle domain ai-engsvcs.com to internet connection. Server: make and model unknown, provided by supplier at their site.

Step	Procedure	Notes
	Record date and time, hardware and software model and versions.	Client located at Wyle: server - make and model unknown
10000	Log in as an administrator with full privileges.	Logged in Wyleadmin/#20wyle11#.
20000	Record statistics on registration page (screen print), export log file and results file. Click on the "Voting" button if necessary to be sure voting has started.	Entered password and clicked on export logs. Exported results and clicked on the "voting button" which it accepted - at that point it cleared the password (voting was now stopped). Had to reenter the password and then started voting by clicking on that button.
30000	Select "Voters Requests" from the menu bar and search for voters in "pending" status. Note the voters with correctly matching information.	Verified.
40000	Return to voting administration screen and click on Automatic Accept.	Pop up message indicated 6 voters were accepted. The number of pending and accepted correctly changed in those boxes on the administration screen.
50000	Go to voters request screen and search on pending voters, only those with some mismatch should remain.	Only saw those with mismatch dates and the one with no date in the database - 4 voters total.
60000	Reject one mismatched voter -- that has a working email	Rejected voter 1208100573263 with email address david.jakobsen@wyle.com. It would not let me close the detail info box until saving it (the "send" button was NOT enabled). Upon saving, the pop up message "Voter request updated" was displayed. On returning to the pending list, he had been removed. Verified his name appeared on the "rejected" list and the information was correct.
70000	Change the email address in for one voter.	Changed voter [redacted] to [redacted] and saved and closed (Clicked on save and got the message confirming it was saved. Then clicked on close and got the message "changes you made require sending Information to the voter. Please send info and then close form." The SEND button

		was not enabled, but you can only exit by hitting the "cancel" button. Apparently when it "cancels" it does not update the Pending voter list because that list still had the old address. It was updated when edit was clicked again. Closed the detail box by clicking on "close". The new address now correctly appeared.
80000	Accept that same voter as a registered voter.	Changed his status to Accepted. The system enabled the "send" button and required saving and sending the information.
90000	For that same voter change the status to "rejected".	Searched on his Id number in accepted and found him. Clicked on edit and it brought up his "voter Request" detail info box with the "send" button enabled. Changed the status to rejected and it disabled the "send" button. Clicked on "save" and it acknowledged successful save. It allowed selecting close ok and did not require a send.
100000	Manual review and accept remaining voters.	Done.
105000	Click on the "sent mail" item in the menu bar and verify the accuracy of the sent mails.	Viewed the sent mail list and it appeared ok
110000	Search for accepted voters with today's date and record the list (screen print)	Done.
120000	View and screen print or print logs and reports. Collect pins created for all voters -- save emails and archive all information collected. Printed duplicate email report.	Done.
130000	End of test -- record time and date	Completed test...

Test Case:	Test Case 14 Normal Voting System C
Test Objective:	**Test Configuration:**
One ballot will be delivered to the terminal and voted and cast on-line. 1. The system accurately delivers the content for that ballot to the voter 2. The system implements authentication prior to allowing the voter access to the ballot. 3. The system adequately logs the event of transferring the ballot information 4. The system records the voters choices accurately and securely 5. The system only records the vote after the voter has performed the action to "cast" it 6. The system protects the cast vote against any viewing or access by anyone until the day that the jurisdiction has authorized for the voting to be opened. 7. The browser does not allow access to sensitive data through storage in cookies or temporary files. 8. The voter is protected from inadvertently exposing sensitive information.	The client connects to the *****server via the Wyle LAN and internet connection using Internet Explorer. The port for access as a voting administrator is ******
Devices Utilized:	Client located at Wyle: Dell Desktop - OptiPlex 780, 2.0GB RAM, Windows 7 Professional, Internet Explorer 8.0.7600.16385, Wyle domain ai-engsvcs.com to internet connection. Server: make and model unknown, provided by supplier at their site.

Step	Procedure	Notes
0	Locate the PIN(s) provided by email / standard mail. For email user verify that the PIN is securely wrapped in a PDF lock and requires a key (vote rid) to open	1208100538567 pin 134502.
10000	Record start time and date, hardware models and serial numbers, software versions for system test. Record physical location of equipment (remote / local).	Client located at Wyle: Dell Desktop - OptiPlex 780, 2.0GB RAM, Windows 7 Professional, Internet Explorer 8.0.7600.16385, [redacted] server - make and model unknown.
20000	If necessary, log into the system as an administrator and search for "accepted" voters within the dates that "Registration Processing Test Case" was used to accept registration requests. (screen print of the list)	Step completed in previous testing. Using list registeredvVotersListforTest.xls.
30000	Login with a valid voter ID number and PIN.	[redacted]
40000	Click on the "Accept" button to accept the voter oath.	Selected "I agree" Selected "No, I do not want audio ballot".
50000	Click on the "help" button in the top right hand corner.	Selected Help screen.
60000	Return to the contest screen and vote for one (or as many as specified for the contest) continue through all the contests and vote according to the instructions for each contest.	First contest Voted for Neil R. ELLIS. Second contest voted for first 6 candidates. Third contest for first 2 candidates. Selected Review Ballot.
70000	From the review screen go back and change one	Selected go back and original candidate is

1

	vote. Record the final review screen(s) content and "cast" the ballot.	missing. Must revote complete ballot.
80000	Try to use the browser "back" button to vote again. Then attempt to vote a second ballot with the same id and PIN numbers.	Selecting back after voting returns you to the login selection page.
90000	Log in with a different PIN and voter ID. Go to the first contest and over vote (vote for more than instructed). If possible, leave the over vote and move to the next contest	[redacted] Over-voted first contest.
100000	Under vote a contest, leave it under voted and proceed to the next contest. Vote remaining contests with valid vote	Under-voted second contest.
110000	Record the votes as they appear on the review screen and verify they are as voted. Then cast the ballot	Reviewed and cast under and over vote ballot.
120000	Log in as the same voter	[redacted]
130000	Attempt to print or cast a second ballot	User already voted.
140000	Log out as this user	Selecting Continue will log user out.
160000	Log in as administrator. View and dump all reports. Verify that all events for all users that voted are logged.	Upon checking the log, no information was logged regarding this activity.
170000	Dump all logs and collect screen prints, etc.	All files recorded.
180000	End of test – record time and date	

Test Case:	Test Case 01 Host Server Administration System D	
Test Objective:		**Test Configuration:**
This test case verifies the roles of system administrator and the ability to maintain user roles, passwords, logs and other voting system administrative functions.		Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link via (Link TBS) and uses the voter page accessed at URL
Devices Utilized:	Client: Dell Optiplex 780, Server: Vendor supplied, make and model TBS.	

Step	Procedure	
0	Record time and date of test, record hardware models, serial numbers and software versions	
10000	Log in with the administrative account provided by the vendor. (this is an "administrator" role with full privileges)	Demo /Demo
20000	Dump system Logs. Then view the logs and save. Attempt to change and/or reset the log. Verify they cannot be altered.	Logs can be exported and imported into excel.
30000	View user list and attempt to add user, assign role, delete user, and re-assign roles to existing user.	Admin can modify all user information.
40000	Log in as voting system administrator (full privileges) role, create a new user and verify default role is the least privileged. Note information entered for this user and adds one more user for each administrator role.	Created "Wylelabs" with the password "wylelab".
50000	Perform a series of log-ins, one for each role, and attempt to exercise privileges not allowed for that role, verify each role can only view/modify the items there are authorized..	Was unable to log in as "Wylelabs".
60000	Log out and log in as super user and attempt to view storage in server such that unencrypted passwords, etc are detected??/	Passwords are encrypted.
70000	Reset password for existing user, perform password administration such as setting minimum required password length, type of characters, capitals, etc. per NIST 800-63. (user name cannot be part of password)	Changed password for 33W44 to "wyle".
90000	Verify password histories are maintained and that user cannot reuse passwords according to the password length requirement. Attempt to use a password containing the user name and verify that it is rejected.	Does not appear to be a limit on historical passwords.
100000	Verify that passwords automatically expire at a specified length of time. Need to set expiration date on next day and then verify after that date.	Passwords do not expire.
110000	As administrator (super user), record default settings for log control (rqmt 5.6.1.1) verify logs are append only and read-only for authorized roles ____ verify it is not possible to alter the log..	Logs are exported into an excel format.
120000	Attempt to create log failure and verify that log	Log in failures do not appear in the logs.

1

	events, such as errors or rotation are recorded. Attempt to clear log and verify that action is logged. Then export the log for storage (5.6.1.8)	
130000	View log and verify it is in a publicly documented format, such as XML, or include a utility to export log data into a publicly documented format and that it has no data violating voter privacy. Search log and exercise any analysis tools	Logs are in an excel format.
140000	Attempt to monitor real-time reporting of system events. Log in as super admin and view any logs / reports that may provide real-time monitoring of the system activity - especially of logged on users (Check for OS capability external to voting system.)	N/A
150000	Attempt to log in with an invalid administrator user ID Re-attempt until sufficient attempts cause the terminal to be locked out.	There does not appear to be a limit on invalid logins.
155000	Log in, change the number of attempts threshold for locking out the terminal and then repeat the process.	This function is not configurable using the admin screen.
160000	Log in as a valid administrator and don't do anything - allow the system to time out. Then log back in and verity it requires reentry of the password.	Logged in to author tools. NO ADMIN TIMEOUT.
165000	Export the voting system log to external device for archiving.	Logs export into excel format.
170000	Record date and time of test end, collect logs and all output records. Verify events are recorded with proper order and times verify entry includes system id, timestamp, event id, success/fail, and if applicable, user id and jurisdiction id	Logs recorded.
180000	End of test – record time and date	

Result Test Sheet

Test Case: 03 Crypto Test Sheet System D	
Test Objective:	**Test Configuration:**
This test case verifies that the cryptographic functionality implemented by the system meets/is NIST-approved and/or FIPS 140-2 compliant.	Full test System setup, fully functional and under normal operating conditions. Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link.
Devices Utilized:	Client: Dell optima Desktop at Wyle Laboratories. Server: make and model unknown

Step	Procedure	Notes
1000	Record time and date of test, record hardware models, serial numbers and software versions.	6/1/2011 Win 7, IE 8, System VM running CentOS 5.4 URL: [redacted]
2000	Review System documentation for cryptographic algorithms and protocols implemented by the system and record them. **Note:** If keys are put into the voting system manually, read step 7 before continuing.	System documentation reviewed, listed: HTTPS AES-256-bit (2048-bit keyed) SSL - Ballot Transmission Salted MD5, SHA256 Hashes (256-bit) - Credential Storage PKCS#7, 2048-bit RSA (3DES symmetric ephemeral ciphers) - Ballot Encryption
3000	Check to ensure that algorithms and protocols used have gone through the Cryptographic Algorithm Validation Program or FIPS 140-2 approved. If not, that the appropriate waiver has been applied for from NIST. Additionally, check tables in SP 800-57 and ensure algorithms are at 112 bit level.	Check protocols used on client browser side. Connection: Local intranet / Not protected Cert: Non-Registered, version 1, Sha1RSA, RSA 1024 bit
4000	Log into system with administrative privileges. Manually verify or pull using script the permissions on appropriate cryptographic applications and files.	Due to issues with VM this step not performed.
4100	Verify that permissions are restricted and not writable by voting system application. Record and document all observations.	Not performed, see step 4.
5000	Pull the hash values for the cryptographic keys from the system.	Not performed, see step 4.
6000	Check hash lengths to ensure the crypto modules are using a correct strength algorithm.	Not performed, see step 4.
7000	If keys are input manually into system, vary the key by only changing one value slightly. (e.g. Key starts with a "T" use a "t" on second entry.) Follow any system instructions to load key before starting to pull logs and data.	Documentation supports this process however, due to issues with VM this could not be tested and verified.
7100	If system only holds and allows one key/hash; pull hash; then re-log into system reenter key following system instructions; then re-pull hash.	Documentation did not provide any information on this process.
7200	If the system allows more than one hash; then follow systems instruction for a specific key set then re-enter same key set changing the key as described in main step; then pull hashes.	Documentation did not provide any information on this process.

I

Result Test Sheet

7300	Compare the hashes with the slight change; there should be significant change in hash value. Record observations.	Due to issues with VM this step not performed.
8000	Review voting system software source code. Verify that crypto modules are being called in the correct manner to meet NIST requirements and 112 bit encryption. **Note:** The application doing the encryption maybe FIPS 140-2 compliant but, the voting application (i.e. Java code call to crypto module.) could use wrong method to encrypt at proper strength.	Not performed, code not provided.
9000	Key Management, Perform this step if cryptographic keys are generated internally. Review voting system documentation to see what type encryption methods is deployed.	Reviewed documentation see step 2. Additional information; key lengths for: Ballot Transmission - HTTPS AES-256-bit (2048-bit keyed) SSL Credential Storage - Salted MD5, SHA256 Hashes (256-bit) Ballot Encryption - PKCS#7, 2048-bit RSA (3DES symmetric ephemeral ciphers)
9100	Review source code and take note to ensure that methods used comply with FIPS 140-2. This should be done by referring to annex A, C or D of 140-2. Record all observations and discrepancies.	Not performed, code not provided.
9200	Pull file permissions of those executable and library files in the system. Ensure they have restricted access and are properly controlled. Record all observations.	Due to issues with VM this could not be tested.
10000	Perform key entry procedures following voting system documentation. Verify that input and output are NIST compliant.	Due to issues with VM and lack of detail in the documentation this could not be tested and verified.
10100	If automated method is used input and output from system must be encrypted. Record observations.	The documentation states that '[redacted] This process was not clearly defined and was not tested.
10200	If a manual method is used input and output from system maybe plaintext. Record observations. **Note:** Transportation and any other processes dealing with the input and output data should reviewed to verify proper security measures are being applied.	Not performed, see step 7for explanation.
11000	Perform Key zeroization procedures following voting system documentation. Verify that the key no longer exist on the system after completion of procedure. Record all observations.	Not performed, see step 7for explanation.
12000	Perform rekeying procedures following voting system documentation. Verify the system performs as documented and is compliant. Record all observations.	Due to issues with VM this step not performed.
13000	During Operational tests, ensure that the voting system supports rekeying during communications.	Verified protocols being used.

Result Test Sheet

	This should be done by verifying protocols used and/or sniffing network traffic and examining the packets. **Note:** System documentation should but may not state the amount or limit of data encrypted with the same key. The key could change on a daily basis, when a pre-set volume of data has been transmitted or a given period of time has elapsed. Most systems, implement rekeying by forcing a new key exchange, typically through a separate protocol like Internet key exchange (IKE). (e.g. Wi-Fi Protected Access (WPA), does this by frequently replacing session keys through the Temporal Key Integrity Protocol (TKIP))	
14000	During Operational tests, ensure that the voting system uses NIST or FIPS approved protocols for communications. Record all observations. **Note:** This should be done by sniffing network traffic (i.e. Wireshark) and examining the packets.	Verified protocols being used from client side browser.
15000	End of test – record time and date	6/1/2011

Additional Notes:

- Only IE browser tested.
- Side issues – network configuration of the VM caused issues, as well as initial VM settings/options. These had to be adjusted to run on Lab system. Unexplained issues would happen after some of the adjustments were made to get the system up and running.

Test Case:	Test Case 04 Normal Ballot Delivery System D
Test Objective:	**Test Configuration:**
One ballot will be delivered to the terminal and displayed and/or printed to exercise the normal processing path for delivery of ballot. The test will verify that: 1. The system delivers that ballot to the voter 2. The system implements authentication prior to allowing the voter access to the ballot. 3. The system adequately logs the event of transferring the ballot. 4. The ballot that is delivered is identical to the ballot that was provided by the Election Management System.	Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link via voter page at URL Administrative access required via URL (TBS) to monitor and collect test results.
Devices Utilized:	Client: Dell Optiplex 780, Server: Vendor supplied, make and model TBS.

Step	Procedure	Notes
0	Record start time and date, hardware models and serial numbers, software versions for system test. Record physical location of equipment (remote / local)	
10000	Log on as a voter to the system (a non-administrator account on this terminal) .(during the following steps, record each action and response by the system so that at the end, we can verify that all significant events were logged)	Successful login as non-admin.
30000	Perform authentication necessary to access ballot distribution pages.	Ballot displayed.
60000	Mark the ballot and save the marked ballot.	Ballot marked.
80000	Review the ballot and verify the choices are as intended. , then change a choice and print the marked ballot.	Ballot verified.
90000	Sign out or log off as this voter.	Log off successful.
100000	If a browser is used, attempt to view all temporary files to verify no voting information is left on the voting device.	All screens are cached. Files have been saved.
110000	Log in as the same voter	Ballot already submitted.
120000	Attempt to print or cast a second ballot	Access denied due to already voting.
140000	Log off -- and log in as administrator. View and dump logs. Verify that all events for all users that voted are logged. If on the same terminal as voter, then search for files/temporary storage that contains any voter information.	No user log exists.
150000	Examine and Dump all logs and collect screen prints, etc. On both the server and the client.	Logs do not contain all information.
160000	End of test –record time and date	

1

Result Test Sheet

Test Case: 05 Discovery Penetration System D	
Test Objective:	**Test Configuration:**
This test seeks out vulnerabilities in the voting system, verifies the system's resistance to any remote unauthorized entity. That the system provides no access, information or services to unauthorized entities and is configured to minimize ports and information disclosure about the system.	Full System with host, remote terminal and communication devices. Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link. Full test System setup, fully functional and under normal operating conditions.
Devices Utilized:	BackTrack OS with Nessus Laptop

Step	Procedure	Notes
1000	Record time and date of test start, model and serial number of hardware, software with version numbers.	12:35 6/3/2011 HP Pavilion dv6 laptop running Backtrack 4 R2 as OS with Nessus installed. Nessus version : 4.4.1 feed ver. : 201105041534 Scanner MAC : 00:e0:6a:3c:fc:68 Scanner IP : 10.10.13.124 Metasploit v3.7.0 svn r12540
2000	Record IP and URL addresses to be tested.	10.10.13.10 (Need URL)
3000	Scan IP and URL ranges with Nmap, unobtrusive.	Port 22, 80 and 443 open. Linux 2.6.x (100%) VM running file: [redacted]
4000	Scan from inside target/s netmask range. Save results to file.	N/A
5000	Scan target/s from outside interfaces. Save results to file.	See step 3.
6000	If needed and applicable, scan IP and URL ranges with Nmap, aggressive. Save results to file.	Not required.
7000	Scan IP and URL ranges with Nessus, unleveraged "no credentials". Save scan result, in file name indicate unleveraged.	Scanned with Nessus polices (see files); External- [redacted]
8000	Scan from inside target/s netmask range. Save results, indicating "inside" (e.g. system_noC_in.xml)	N/A
9000	If applicable, scan target/s from outside interfaces. Save results, indicating "outside" (e.g. system_noC_out.xml)	See step 7.
10000	Scan IP and URL ranges with Nessus, leveraged "with credentials". Save scan result, in file name indicating leveraged. Note: This type scan is usually done from "inside" only.	Not done, with time restrictions, 8 medium vulnerabilities found unleveraged and remote access by root successful decided vendor had enough to address major problems.
11000	Probe target URL for further information. (i.e. URL manipulation, input/form field manipulation, SQL injection, etc.) Record all observations and displayed information.	Simple SQL injection not effective.
12000	Review all scan results and recorded information.	3 open ports, 8 medium and 42 low vulnerabilities, Linux Kernel 2.6 on CentOS 5, VM machine (00:0c:29:9d:38:86 : VMware, Inc.)

1

Result Test Sheet

13000	Annotate record and organize all pertinent information (e.g. Ports, Protocols, Services, versioning, etc.) from the results for second phase of Pen test.	Done.
14000	From review of pertinent information, setup/develop and additional discovery scans/tests as needed.	Not needed.
15000	Perform any additional discovery scans or tests as needed. Save and record these results.	N/A
16000	Review all results, notes and finalize exploratory tests for second phase of testing.	With time restrictions went with port exploits as primary attack method. Also, attempt login with application credentials. **NOTE:** Login with Root successful, deposited Hacker.txt in root directory.
17000	End of test – record time and date	15:31 6/3/2011

Additional Notes:

- Was able to login with Root remotely. Opened command shell from 10.10.13.124:56693 to 10.10.13.10:22 at 14:25 6/3/2011. Root should never have remote access.
- Metasploit port attacks were used (examples; webdav_upload_upload_asp, hagent_untrusted_hsdata, RealServer describe Buffer Overflow).
- None of attempted exploits succeeded. More detailed attempts against the OS or more detailed SQL attempts maybe successful but, require more time than was currently allocated.

Test Case:	Test Case 01 Host Server Administration System E
Test Objective:	**Test Configuration:**
This test case verifies the roles of system administrator and the ability to maintain user roles, passwords, logs and other voting system administrative functions.	Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link via (Link TBS) and uses the voter page accessed at URL
Devices Utilized:	Client: Dell Optiplex 780, Server: Vendor supplied, make and model TBS.

Step	Procedure	Notes
0	Record time and date of test, record hardware models, serial numbers and software versions	
10000	Log in with the administrative account provided by the vendor. (this is an "administrator" role with full privileges)	User Name "*******S" Psw "[redacted]". Login successful.
20000	Dump system Logs. Then view the logs and save. Attempt to change and/or reset the log. Verify they cannot be altered.	Logs cannot be modified using administrator access. Member Login Log is the only log that is not exportable.
30000	View user list and attempt to add user, assign role, delete user, and re-assign roles to existing user.	Admin can modify and add all members.
40000	Log in as voting system administrator (full privileges) role, create a new user and verify default role is the least privileged. Note information entered for this user and add one more user for each administrator role.	Created user "WyleLabs" Psw "wylelab". Note! The only way to validate the field requirements is to enter an invalid value. Role is defined by assigning the new user to a specific precinct.
50000	Perform a series of log-ins, one for each role, and attempt to exercise privileges not allowed for that role, verify each role can only view/modify the items there are authorized..	New Admin can only see specific precinct information. Admin at this level can only add admin's at the same level.
60000	Log out and log in as super user and attempt to view storage in server such that unencrypted passwords, etc. are detected	Login as User Name "*****OS" Psw "[redacted]". Login successful.
70000	Reset password for existing user, perform password administration such as setting minimum required password length, type of characters, capitals, etc. per NIST 800-63. (user name cannot be part of password)	Modified password for admin sale_5713 pwd "wylelabs". Password must be "6-20 bit characters or digits is allowed." Password field accepts special characters. NOTE! Password can match the user name!
90000	Verify password histories are maintained and that user cannot reuse passwords according to the password length requirement. Attempt to use a password containing the user name and verify that it is rejected.	NOTE! Password can match the user name! And there is nothing to stop reuse of old passwords.
100000	Verify that passwords automatically expire at a specified length of time. Need to set expiration date on next day and then verify after that date.	There does not appear to be a function for expiring passwords.

110000	As administrator (super user), record default settings for log control (rqmt 5.6.1.1) verify logs are append only and read-only for authorized roles ____ verify it is not possible to alter the log..	Login logs are appended and non-editable.
120000	Attempt to create log failure and verify that log events, such as errors or rotation are recorded. Attempt to clear log and verify that action is logged. Then export the log for storage (5.6.1.8)	System does not log login failures and the log is not exportable. It could not be determined how long the log information is retained.
130000	View log and verify it is in a publicly documented format, such as XML, or include a utility to export log data into a publicly documented format and that it has no data violating voter privacy. Search log and exercise any analysis tools	The logs that can be exported are in an .XLS format.
140000	Attempt to monitor real-time reporting of system events. Log in as super admin and view any logs / reports that may provide real-time monitoring of the system activity - especially of logged on users (Check for OS capability external to voting system.)	Login access is recorded via Ballot Events and Member login log. It could not be determined how long the log information is retained.
150000	Attempt to log in with an invalid administrator user ID Re-attempt until sufficient attempts cause the terminal to be locked out.	User Name "******OS" Psw "[redacted]". Login successful. It does not appear that there is a limit on the number of incorrect login attempts.
155000	Log in, change the number of attempts threshold for locking out the terminal and then repeat the process.	It does not appear that there is a limit on the number of incorrect login attempts.
160000	Log in as a valid administrator and don't do anything - allow the system to time out. Then log back in and verity it requires reentry of the password.	User Name "*****OS" Psw "[redacted]". Login successful 4/26/2011 2:17:18 PM System has not logged out. 4/26/2011 2:27:18 PM System never logs admin out.
165000	Export the voting system log to external device for archiving.	Members login log is not exportable.
170000	Record date and time of test end, collect logs and all output records. Verify events are recorded with proper order and times verify entry includes system id, timestamp, event id, success/fail, and if applicable, user id and jurisdiction id	All logs retained.
180000	End of test -- record time and date.	

Result Test Sheet

Test Case: 03 Crypto Test Sheet System E	
Test Objective:	**Test Configuration:**
This test case verifies that the cryptographic functionality implemented by the system meets/is NIST-approved and/or FIPS 140-2 compliant.	Full test System setup, fully functional and under normal operating conditions. Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link.
Devices Utilized:	Client: Dell optima Desktop at Wyle Laboratories. Server: make and model unknown

Step	Procedure	Notes
1000	Record time and date of test, record hardware models, serial numbers and software versions.	Win 7, IE 8 URL:
2000	Review System documentation for cryptographic algorithms and protocols implemented by the system and record them. **Note:** If keys are put into the voting system manually, read step 7 before continuing.	Documentation provided did not provide any additional information than what was gathered in step 3.
3000	Check to ensure that algorithms and protocols used have gone through the Cryptographic Algorithm Validation Program or FIPS 140-2 approved. If not, that the appropriate waiver has been applied for from NIST. Additionally, check tables in SP 800-57 and ensure algorithms are at 112 bit level.	Could only check protocols used on client browser side, due to not having access to the system. Connection: TLS 1.0 3DES 168 bit, RSA 2048 bit Cert: Issuer – Go Daddy, class 3, sign algorithm Sha1RSA, hash Sha1
4000	Log into system with administrative privileges. Manually verify or pull using script the permissions on appropriate cryptographic applications and files.	Could not perform. No administrative credentials provided. Only application admin credentials provided.
4100	Verify that permissions are restricted and not writable by voting system application. Record and document all observations.	Could not perform. No access to system other than client side browser connection.
5000	Pull the hash values for the cryptographic keys from the system.	Could not perform. No access to system.
6000	Check hash lengths to ensure the crypto modules are using a correct strength algorithm.	Not performed, see step 5.
7000	If keys are input manually into system, vary the key by only changing one value slightly. (e.g. Key starts with a "T" use a "t" on second entry.) Follow any system instructions to load key before starting to pull logs and data.	Documentation provided did not provide information on this process. No access to system other than application usage. This step Not performed.
7100	If system only holds and allows one key/hash; pull hash; then re-log into system reenter key following system instructions; then re-pull hash.	Documentation provided did not provide information on this process. No access to system other than application usage. This step Not performed.
7200	If the system allows more than one hash; then follow systems instruction for a specific key set then re-enter same key set changing the key as described in main step; then pull hashes.	Not performed, see step 7.
7300	Compare the hashes with the slight change; there	Not performed, see step 7.

1

Result Test Sheet

	should be significant change in hash value. Record observations.	
8000	Review voting system software source code. Verify that crypto modules are being called in the correct manner to meet NIST requirements and 112 bit encryption. **Note:** The application doing the encryption maybe FIPS 140-2 compliant but, the voting application (i.e. Java code call to crypto module.) could use wrong method to encrypt at proper strength.	Not performed, code not provided.
9000	Key Management, Perform this step if cryptographic keys are generated internally. Review voting system documentation to see what type encryption methods is deployed.	Unknown, system documentation provided did not provide information on this process. No access to system other than application usage. This step Not performed.
9100	Review source code and take note to ensure that methods used comply with FIPS 140-2. This should be done by referring to annex A, C or D of 140-2. Record all observations and discrepancies.	Not performed, code not provided.
9200	Pull file permissions of those executable and library files in the system. Ensure they have restricted access and are properly controlled. Record all observations.	No access to system other than application usage. This step Not performed.
10000	Perform key entry procedures following voting system documentation. Verify that input and output are NIST compliant.	No access to system other than application usage. This step Not performed.
10100	If automated method is used input and output from system must be encrypted. Record observations.	Unknown, system documentation provided did not provide information on this process. No access to system other than application usage. This step Not performed.
10200	If a manual method is used input and output from system maybe plaintext. Record observations. Note: Transportation and any other processes dealing with the input and output data should reviewed to verify proper security measures are being applied.	Unknown, system documentation provided did not provide information on this process. No access to system other than application usage. This step Not performed.
11000	Perform Key zeroization procedures following voting system documentation. Verify that the key no longer exist on the system after completion of procedure. Record all observations.	Not performed, see step 10.
12000	Perform rekeying procedures following voting system documentation. Verify the system performs as documented and is compliant. Record all observations.	Not performed, see step 10.
13000	During Operational tests, ensure that the voting system supports rekeying during communications. This should be done by verifying protocols used and/or sniffing network traffic and examining the packets. **Note:** System documentation should but may not state the amount or limit of data encrypted with the same key.	Verified protocols being used but, did not monitor traffic due to the whole system not being in Wyle testing lab.

Result Test Sheet

	The key could change on a daily basis, when a pre-set volume of data has been transmitted or a given period of time has elapsed. Most systems, implement rekeying by forcing a new key exchange, typically through a separate protocol like Internet key exchange (IKE). (e.g. Wi-Fi Protected Access (WPA), does this by frequently replacing session keys through the Temporal Key Integrity Protocol (TKIP))	
14000	During Operational tests, ensure that the voting system uses NIST or FIPS approved protocols for communications. Record all observations. Note: This should be done by sniffing network traffic (i.e. Wireshark) and examining the packets.	Verified protocols being used from client side browser.
15000	End of test – record time and date	6/1/2011

Additional Notes:

- Only IE browser tested.
- Side issues – Web browsers listed in documentation have browser versions with known security issues.

Test Case:	Test Case 04 Normal Ballot Delivery System E
Test Objective:	**Test Configuration:**
One ballot will be delivered to the terminal and displayed and/or printed to exercise the normal processing path for delivery of ballot. The test will verify that: 1. The system delivers that ballot to the voter 2. The system implements authentication prior to allowing the voter access to the ballot. 3. The system adequately logs the event of transferring the ballot. 4. The ballot that is delivered is identical to the ballot that was provided by the Election Management System.	Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link via voter page at URL Administrative access required via URL (TBS) to monitor and collect test results.
Devices Utilized:	Client: Dell Optiplex 780, Server: Vendor supplied, make and model TBS.

Step	Procedure	Notes
0	Record start time and date, hardware models and serial numbers, software versions for system test. Record physical location of equipment (remote / local)	
10000	Log on as a voter to the system (a non-administrator account on this terminal)... (during the following steps, record each action and response by the system so that at the end, we can verify that all significant events were logged)	Login with *PIN: NIPVYVBGINMW7I8*
30000	Perform authentication necessary to access ballot distribution pages.	All information to validate is in unencrypted email.
40000	Log in and Print the blank ballot	Blank ballot saved.
50000	Log in and download another ballot.	Blank ballot saved
60000	Mark the ballot and save the marked ballot.	Marked ballot saved.
80000	Review the ballot and verify the choices are as intended, then change a choice and print the marked ballot.	Validated ballot.
90000	Sign out or log off as this voter.	Browsers closed after finished.
100000	If a browser is used, attempt to view all temporary files to verify no voting information is left on the voting device.	Browsers closed after finished.
105000	Review the printed ballot and saved ballot and verify that the ballot is marked so that multiple copies cannot be submitted.	Each ballot has an identification number.

1

110000	Log in as the same voter	Login with pin: NIPVYVBGINMW7I8.
120000	Attempt to print or cast a second ballot	A voter can vote as many times as they want. A new number is on each ballot.
140000	Log off -- and log in as administrator. View and dump logs. Verify that all events for all users that voted are logged. If on the same terminal as voter, then search for files/temporary storage that contains any voter information.	Ballot log exported.
150000	Examine and Dump all logs and collect screen prints, etc. On both the server and the client. Record end time	Ballot log exported.

Result Test Sheet

Test Case: 05 Discovery Penetration System E	
Test Objective:	**Test Configuration:**
This test seeks out vulnerabilities in the voting system, verifies the system's resistance to any remote unauthorized entity. That the system provides no access, information or services to unauthorized entities and is configured to minimize ports and information disclosure about the system.	Full System with host, remote terminal and communication devices. Server located at Vendor site with Client PC located at Wyle Laboratories. Client running Internet Explorer 8.0 accesses server over secure Internet communication link. Full test System setup, fully functional and under normal operating conditions.
Devices Utilized:	BackTrack OS with Nessus Laptop

Step	Procedure	Notes
1000	Record time and date of test start, model and serial number of hardware, software with version numbers.	09:26 6/2/2011 HP Pavilion dv6 laptop running Backtrack 4 R2 as OS with Nessus installed. Nessus version : 4.4.1 feed ver. : 201105041534 Scanner MAC : 00:0d:ab:ef:a9:2e Scanner IP : 10.10.13.124 Metasploit v3.7.0 svn r12540
2000	Record IP and URL addresses to be tested.	[redacted]
3000	Scan IP and URL ranges with Nmap, unobtrusive.	Port 443 open. Server 2003 (87%) file: kon.xml
4000	Scan from inside target/s netmask range. Save results to file.	N/A
5000	Scan target/s from outside interfaces. Save results to file.	See step 3.
6000	If needed and applicable, scan IP and URL ranges with Nmap, aggressive. Save results to file.	Not required.
7000	Scan IP and URL ranges with Nessus, unleveraged "no credentials". Save scan result, in file name indicate unleveraged.	Scanned with Nessus polices (see files); Web Apps- [redacted] External- [redacted] During scans IP was blocked.
8000	Scan from inside target/s netmask range. Save results, indicating "inside" (e.g. system_noC_in.xml)	N/A
9000	If applicable, scan target/s from outside interfaces. Save results, indicating "outside" (e.g. system_noC_out.xml)	See step 7.
10000	Scan IP and URL ranges with Nessus, leveraged "with credentials". Save scan result, in file name indicating leveraged. Note: This type scan is usually done from "inside" only.	Not done, no credentials were provided.
11000	Probe target URL for further information. (i.e. URL manipulation, input/form field manipulation, SQL injection, etc.) Record all observations and displayed information.	Simple SQL injection not effective.
12000	Review all scan results and recorded information.	1 open ports, 23 low vulnerabilities, Windows Server 2003

Result Test Sheet

13000	Annotate record and organize all pertinent information (e.g. Ports, Protocols, Services, versioning, etc.) from the results for second phase of Pen test.	Done.
14000	From review of pertinent information, setup/develop and additional discovery scans/tests as needed.	Not needed.
15000	Perform any additional discovery scans or tests as needed. Save and record these results.	N/A
16000	Review all results, notes and finalize exploratory tests for second phase of testing.	With time restrictions went with port exploits as primary attack method. Also, attempt login with application credentials.
17000	End of test – record time and date	12:40 6/2/2011

Additional Notes:

- Metasploit port attacks were used (examples; iis, webdav_upload_upload_asp, MS-03_007, MS-10_022, RealServer describe Buffer Overflow).
- During Nessus scans the scanning IP was blocked per security protocol of vendor. However Nmap scans and Metasploit attempts were made without being blocked.
- None of attempted exploits succeeded. More detailed attempts against the OS or more detailed SQL attempts maybe successful but, require more time than was currently allocated.

Test Case:	Test Case 12 Voter Registration Request System E	
Test Objective:		**Test Configuration:**
This test case verifies that a voter can securely register to vote on-line. The test includes authentication that the voter is the voter that he/she claims to be and that the request is queued for processing by an election administrator		The client connects to the [redacted] server via the Wyle LAN and internet connection using Internet Explorer. The port for access as a voting administrator is [redacted] and for access to register as a voter is [redacted].
Devices Utilized:	Client located at Wyle: Dell Desktop - OptiPlex 780, 2.0GB RAM, Windows 7 Professional, Internet Explorer 8.0.7600.16385, Wyle domain ai-engsvcs.com to internet connection. Server: make and model unknown, provided by supplier at their site.	

Step	Procedure	
0	Record date and time, equipment with model numbers, server software versions.	
10000	Log into the administrator screen, record statistics on screen (take a screen print) and Export UOCAVA list.	User Name ******OS Psw [redacted]. Login successful Exported [redacted]
20000	Go to the voter registration screen -- (https://vote4newjersey.us/BallotRequest/Register.aspx) and using the voter credentials log in with the correct name, voter ID	[redacted]
30000	Complete the registration screen by providing a valid email (yours) that you can access and a secret question with answer and the correct birth year for this voter. Submit that form. And click finish on the review screen -- close the browser.	[redacted]
40000	Repeat the registration process with the same voter on each screen	Registration completed - email saved.
50000	Select a different voter from the UOCAVA list.	[redacted]
60000	Using this voter, enter the ID, voter name correctly but enter other incorrect information.	Voter was unable to register. First time due to birthdate not being correct. Re-ran with correct information for name and birthdate. When two people have identical information the system should show both options. I was unable to test this since none of the voters in the supplied list met this requirement.
80000	From the UOCAVA lists, logon and enter requests for 8 more voters. Enter valid requests with matching information on at least 5 and incorrect dates on 3. Use a variety of email addresses - one of them with only one voter associated.	a: [redacted] b: [redacted] c: d: [redacted] f: g: h:
90000	Export the logs and reports.	Logs recorded.
100000	End of test -- record time and date	Note! Pressing the back button on the browser will allow you to see information from a previous applicant.

1

Test Case:	Test Case 13 Registration Processing System E
Test Objective:	**Test Configuration:**
This test case verifies the ability of the election administrator to view voter requests and accept or reject them based on successful comparison of the voter's credentials that were supplied by the voter to those that are known in the system database. The test will verify the acceptance/ rejection process and the notification to the voter. It will verify that all voter identification transmitted to the voter is protected against unauthorized access.	The client connects to the [redacted] server via the Wyle LAN and internet connection using Internet Explorer. The port for access as a voting administrator is C and for access to register as a voter is https://[redacted]
Devices Utilized:	Client located at Wyle: Dell Desktop - OptiPlex 780, 2.0GB RAM, Windows 7 Professional, Internet Explorer 8.0.7600.16385, Wyle domain ai-engsvcs.com to internet connection

Step	Procedure	Notes
0	Record date and time, hardware and software model and versions.	
10000	Log in as an administrator with full privileges.	User Name is "Wyle2011", password is "Wyle2011". Logged in as precinct admin.
20000	Record statistics on registration page (screen print), export log file and results file, Click on the "Voting" button if necessary to be sure voting has started.	Request ballots image saved.
30000	Select "Ballot Requests" from the menu bar and search for voters in "NEW" status. Note the voters with correctly matching information.	Done.
50000	Reject one mismatched voter -- that has a working email address	Rejected [redacted] Email received / [redacted] has invalid information.
60000	Manual review and accept remaining voters.	Changed everyone's precinct from [redacted] to [redacted]. Since [redacted] was not loaded.
70000	Search for accepted voters with today's date and record the list (screen print)	List saved.
80000	View and screen print or print logs and reports. Collect pins created for all voters -- save emails and archive all information collected. Printed duplicate emailed report.	Emails saved.
90000	End of test -- record time and date.	

ATTACHMENT C

STATISTICAL ANALYSIS OF UOCAVA EVSW'S

Note: This Attachment is landscape orientation and requires 11x17 page size.

UOCAVA	Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements		System A	System B	System C	System D	System E	Results								
Req. No.	Functional Requirements Matrix	Wyle Comment														
Section 5	**Security**															
5.1	**Access Control**							29	21	10	15		41.67%	17.50%	15.83%	25.00%
	This section states requirements for the identification of authorized system users, processes and devices and the authentication or verification of those identities as a prerequisite to granting access to system processes and data. It also includes requirements to limit and control access to critical system components to protect system and data integrity, availability, confidentiality, and accountability. This section applies to all entities attempting to physically enter voting system facilities or to request services or data from the voting system.							Pass	Fail	Not Tested	N/A		Pass	Fail	Not Tested	N/A
5.1.1	**Separation of Duties**							7	0	3	5		47%	0%	20%	33%
5.1.1.1	The voting system SHALL allow the definition of personnel roles with segregated duties and responsibilities on critical processes to prevent a single person from compromising the integrity of the system.	Some system's not tested due to not have lab access to hardware for validation.	Not Tested	Not Tested	Pass	Pass	Pass	3	0	2	0		60%	0%	40%	0%
5.1.1.2	The voting system SHALL ensure that only authorized roles, groups, or individuals have access to election data.	Some system's not tested due to not have lab access to hardware for validation.	Not Tested	Pass	Pass	Pass	Pass	4	0	1	0		80%	0%	20%	0%
5.1.1.3	The voting system SHALL require at least two persons from a predefined group for validating the election configuration information, accessing the cast vote records, and starting the tabulation process.	Current web based system do not do tabulation so this requirement was not applicable to our testing. The majority of election configuration is done independent of the Web application and is therefore not a critical function of our testing.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.1.2	**Voting System Access**							22	21	7	10		37%	35%	12%	17%
	The voting system SHALL provide access control mechanisms designed to permit authorized access and to prevent unauthorized access to the system.		Pass	Pass	Pass	Pass	Pass	5	0	0	0		100%	0%	0%	0%
5.1.2.1	The voting system SHALL identify and authenticate each person, to whom access is granted, and the specific functions and data to which each person holds authorized access.	Some system's not tested due to not have lab access to hardware for validation.	Not Tested	Pass	Pass	Pass	Pass	4	0	1	0		80%	0%	20%	0%
5.1.2.2	The voting system SHALL allow the administrator group or role to configure permissions and functionality for each identity, group or role to include account and group/role creation, modification, and deletion.	Some system's not tested due to not have lab access to hardware for validation.	Not Tested	Not Tested	Pass	Pass	Pass	3	0	2	0		60%	0%	40%	0%

5.1.2.3	The voting system’s default access control permissions SHALL implement the least privileged role or group needed.	Some system's not tested due to not have lab access to hardware for validation.	Not Tested	Not Tested	Fail	Pass	Fail	1	2	2	0		20%	40%	40%	0%
5.1.2.4	The voting system SHALL prevent a lower-privilege process from modifying a higher-privilege process.	Some system's not tested due to not have lab access to hardware for validation.	Not Tested	Not Tested	Pass	Pass	Pass	3	0	2	0		60%	0%	40%	0%
5.1.2.5	The voting system SHALL NOT require its execution as an operating system privileged account and SHALL NOT require the use of an operating system privileged account for its operation.	Wyle's testing was based on utilization of a web based application. Therefore this did not apply directly. But, it was noted that in some systems tested the OS administration privileges were required to configure election information.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.1.2.6	The voting system SHALL log the identification of all personnel accessing or attempting to access the voting system to the system event log.		Pass	Fail	Fail	Fail	Pass	2	3	0	0		40%	60%	0%	0%
5.1.2.7	The *(voting system)* SHALL provide tools for monitoring access to the system. These tools SHALL provide specific users real time display of persons accessing the system as well as reports from logs.		Pass	Fail	Fail	Fail	Fail	1	4	0	0		20%	80%	0%	0%
5.1.2.8	Vote capture device located at the remote voting location and the central server SHALL have the capability to restrict access to the voting system after a preset number of login failures.		Fail	Fail	Fail	Fail	Fail	0	5	0	0		0%	100%	0%	0%
5.1.2.9	The voting system SHALL log a notification when any account has been locked out.		Fail	Fail	Fail	Fail	Fail	0	5	0	0		0%	100%	0%	0%
5.1.2.10	Authenticated sessions on critical processes SHALL have an inactivity time-out control that will require personnel re-authentication when reached. This time-out SHALL be implemented for administration and monitor consoles on all voting system devices.		Fail	Fail	Pass	Pass	Pass	3	2	0	0		60%	40%	0%	0%
5.1.2.11	Authenticated sessions on critical processes SHALL have a screen-lock functionality that can be manually invoked.	This requirement was deemed N/A due to the web based application being accessible from a privately controlled PC and not a public Voting site.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.2	**Identification and Authentication**							26	24	9	6		40%	37%	14%	9%
5.2.1	**Authentication**							26	24	9	6		40%	37%	14%	9%
5.2.1.1	Authentication mechanisms supported by the voting system SHALL support authentication strength of at least 1/1,000,000.		Not Tested	Pass	Pass	Fail	Pass	3	1	1	0		60%	20%	20%	0%

5.2.1.2	The voting system SHALL authenticate users per the minimum authentication methods outlined below.	Some system's not tested due to not have lab access to hardware for validation.	Not Tested	Not Tested	Fail	Pass	Fail	1	2	2	0		20%	40%	40%	0%
5.2.1.3	The voting system SHALL provide multiple authentication methods to support multi-factor authentication.		Fail	Fail	Pass	Pass	Pass	3	2	0	0		60%	40%	0%	0%
5.2.1.4	When private or secret authentication data is stored by the voting system, it SHALL be protected to ensure that the confidentiality and integrity of the data are not violated.	Some system's not tested due to not have lab access to hardware for validation.	Not Tested	Pass	Pass	Pass	Pass	4	0	1	0		80%	0%	20%	0%
5.2.1.5	The voting system SHALL provide a mechanism to reset a Password if it is forgotten, in accordance with the system access/security policy.		Fail	Pass	Fail	Fail	Fail	1	4	0	0		20%	80%	0%	0%
5.2.1.6	The voting system SHALL allow the administrator group or role to specify Password strength for all accounts including minimum Password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters per NIST 800-63 Electronic Authentication Guideline Standards.	Some system's not tested due to not have lab access to hardware for validation.	Not Tested	Fail	Fail	Fail	Fail	0	4	1	0		0%	80%	20%	0%
5.2.1.7	The voting system SHALL enforce Password histories and allow the administrator to configure the history length when Passwords are stored by the system.	Some system's not tested due to not have lab access to hardware for validation.	Not Tested	Fail	Fail	Fail	Fail	0	4	1	0		0%	80%	20%	0%
5.2.1.8	The voting system SHALL ensure that the user name is not used in the Password.	Some system's not tested due to not have lab access to hardware for validation.	Not Tested	Not Tested	Pass	Fail	Fail	1	2	2	0		20%	40%	40%	0%
5.2.1.9	The voting system SHALL provide a means to automatically expire Passwords.	Some system's not tested due to not have lab access to hardware for validation.	Not Tested	Fail	Fail	Fail	Fail	0	4	1	0		0%	80%	20%	0%
5.2.1.10	The voting system servers and vote capture devices SHALL identify and authenticate one another using NIST - approved cryptographic authentication methods at the 112 bits of security.		Pass	Fail	Pass	Pass	Pass	4	1	0	0		80%	20%	0%	0%
5.2.1.11	Remote voting location site Virtual Private Network (VPN) connections (i.e., vote capture devices) to voting servers SHALL be authenticated using strong mutual cryptographic authentication at the 112 bits of security.	This requirement was deemed N/A due to the web based application being accessible from a privately controlled PC and not a public Voting site.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.2.1.12	Message authentication SHALL be used for applications to protect the integrity of the message content using a schema with 112 bits of security.		N/A	Pass	Pass	Pass	Pass	4	0	0	1		80%	0%	0%	20%
5.2.1.13	IPsec, SSL, or TLS and MAC mechanisms SHALL all be configured to be compliant with FIPS 140-2 using approved algorithm suites and protocols.		Pass	Pass	Pass	Pass	Pass	5	0	0	0		100%	0%	0%	0%
5.3	**Cryptography**							5	12	18	0		11%	27%	62%	0%
5.3.1	**General Cryptography Requirements**							4	11	0	0		27%	73%	0%	0%
5.3.1.1	All cryptographic functionality SHALL be implemented using NIST-approved cryptographic algorithms/schemas, or use published and credible cryptographic algorithms/schemas/protocols.		Fail	Fail	Fail	Fail	Fail	0	5	0	0		0%	100%	0%	0%
5.3.1.2	Cryptographic algorithms and schemas SHALL be implemented with a security strength equivalent to at least 112 bits of security to protect sensitive voting information and election records.		Fail	Fail	Fail	Fail	Fail	0	5	0	0		0%	100%	0%	0%

5.3.1.3	Cryptography used to protect information in-transit over public telecommunication networks SHALL use NIST-approved algorithms and cipher suites. In addition the implementations of these algorithms SHALL be NIST-approved (Cryptographic Algorithm Validation Program).		Pass	Fail	Pass	Pass	Pass	4	1	0	0		80%	20%	0%	0%
5.3.2	**Key Management**																	
	The following requirements apply to voting systems that generate cryptographic keys internally.							1	2	37	0		0%	4%	96%	0%
5.3.2.1	Cryptographic keys generated by the voting system SHALL use a NIST-approved key generation method, or a published and credible key generation method.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Not Tested	Not Tested	0	0	5	0		0%	0%	100%	0%
5.3.2.2	Compromising the security of the key generation method (e.g., guessing the seed value to initialize the deterministic random number generator (RNG)) SHALL require as least as many operations as determining the value of the generated key.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Not Tested	Not Tested	0	0	5	0		0%	0%	100%	0%
5.3.2.3	If a seed key is entered during the key generation process, entry of the key SHALL meet the key entry requirements in 5.3.3.1. If intermediate key generation values are output from the cryptographic module, the values SHALL be output either in encrypted form or under split knowledge procedures.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Not Tested	Not Tested	0	0	5	0		0%	0%	100%	0%
5.3.2.4	Cryptographic keys used to protect information in-transit over public telecommunication networks SHALL use NIST-approved key generation methods. If the approved key generation method requires input from a random number generator, then an approved (FIPS 140-2) random number generator SHALL be used.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Not Tested	Not Tested	0	0	5	0		0%	0%	100%	0%
5.3.2.5	Random number generators used to generate cryptographic keys SHALL implement one or more health tests that provide assurance that the random number generator continues to operate as intended (e.g., the entropy source is not stuck).	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Fail	Not Tested	0	1	4	0		0%	20%	80%	0%
5.3.3	**Key Establishment**																	
	Key establishment may be performed by automated methods (e.g., use of a public key algorithm), manual methods (use of a manually transported key loading device), or a combination of automated and manual methods.							1	1	18	0		5%	5%	90%	0%
5.3.3.1	Secret and private keys established using automated methods SHALL be entered into and output from a voting system in encrypted form. Secret and private keys established using manual methods may be entered into or output from a system in plaintext form.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Fail	Not Tested	0	1	4	0		0%	20%	80%	0%
5.3.4.1	Cryptographic keys stored within the voting system SHALL NOT be stored in plaintext. Keys stored outside the voting system SHALL be protected from disclosure or modification.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Pass	Not Tested	1	0	4	0		20%	0%	80%	0%
5.3.4.2	The voting system SHALL provide methods to zeroize all plaintext secret and private cryptographic keys within the system.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Not Tested	Not Tested	0	0	5	0		0%	0%	100%	0%
5.3.4.3	The voting system SHALL support the capability to reset cryptographic keys to new values.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Not Tested	Not Tested	0	0	5	0		0%	0%	100%	0%
5.4	**Voting System Integrity Management**																	
	This section addresses the secure deployment and operation of the voting system, including the protection of removable media and protection against malicious software.							3	2	10	20		9%	6%	29%	57%
5.4.1	**Protecting the Integrity of the Voting System**							3	2	10	20		9%	6%	29%	57%

5.4.1.1	The integrity and authenticity of each individual cast vote SHALL be protected from any tampering or modification during transmission.	Current web based system do not do tabulation so this requirement was not applicable to our testing.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.4.1.2	The integrity and authenticity of each individual cast vote SHALL be preserved by means of a digital signature during storage.	Current web based system do not do tabulation so this requirement was not applicable to our testing.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.4.1.3	Cast vote data SHALL NOT be permanently stored on the vote capture device.		Pass	Pass	Pass	Fail	Fail	3	2	0	0		60%	40%	0%	0%
5.4.1.4	The integrity and authenticity of the electronic ballot box SHALL be protected by means of a digital signature.	Current web based system do not do tabulation so this requirement was not applicable to our testing.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.4.1.5	The voting system SHALL use malware detection software to protect against known malware that targets the operating system, services, and applications.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Not Tested	Not Tested	0	0	5	0		0%	0%	100%	0%
5.4.1.6	The voting system SHALL provide a mechanism for updating malware detection signatures.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Not Tested	Not Tested	0	0	5	0		0%	0%	100%	0%
5.4.1.7	The voting system SHALL provide the capability for kiosk workers to validate the software used on the vote capture devices as part of the daily initiation of kiosk operations.	Wyle deems this requirement N/A due to the Web Based architecture.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.5	**Communications Security**																	
	This section provides requirements for communications security. These requirements address ensuring the integrity of transmitted information and protecting the voting system from external communications-based threats.							8	4	33	5		18%	8%	67%	8%
5.5.1	**Data Transmission Security**							3	3	19	5		10%	10%	63%	17%
5.5.1.1	Voting systems that transmit data over communications links SHALL provide integrity protection for data in transit through the generation of integrity data (digital signatures and/or message authentication codes) for outbound traffic and verification of the integrity data for inbound traffic.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Not Tested	Not Tested	0	0	5	0		0%	0%	100%	0%
5.5.1.2	Voting systems SHALL use at a minimum TLS 1.0, SSL 3.1 or equivalent protocols, including all updates to both protocols and implementations as of the date of the submission (e.g., RFC 5746 for TLS 1.0).	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Not Tested	Not Tested	0	0	5	0		0%	0%	100%	0%
5.5.1.3	Voting systems deploying VPNs SHALL configure them to only allow FIPS-compliant cryptographic algorithms and cipher suites.	Wyle deems this requirement N/A due to the Web Based architecture. VPN systems will only be utilized at a system server level.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.5.1.4	Each communicating device SHALL have a unique system identifier.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Pass	Fail	1	1	3	0		20%	20%	60%	0%
5.5.1.5	Each device SHALL mutually strongly authenticate using the system identifier before additional network data packets are processed.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Fail	Fail	0	2	3	0		0%	40%	60%	0%
5.5.1.6	Data transmission SHALL preserve the secrecy of voters' ballot selections and SHALL prevent the violation of ballot secrecy and integrity.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Pass	Pass	2	0	3	0		40%	0%	60%	0%
5.5.2	**External Threats**							5	1	14	0		25%	5%	70%	0%
	Voting systems SHALL implement protections against external threats to which the system may be susceptible.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Pass	Not Tested	1	0	4	0		20%	0%	80%	0%

5.5.2.1	Voting system components SHALL have the ability to enable or disable physical network interfaces.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Pass	Not Tested	Pass	Pass	3	0	2	0		60%	0%	40%	0%
5.5.2.2	The number of active ports and associated network services and protocols SHALL be restricted to the minimum required for the voting system to function.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Pass	Not Tested	1	0	4	0		20%	0%	80%	0%
5.5.2.3	The voting system SHALL block all network connections that are not over a mutually authenticated channel.	Some system's not tested due to not having lab access to hardware for validation or necessary documentation.	Not Tested	Not Tested	Not Tested	Fail	Not Tested	0	1	4	0		0%	20%	80%	0%
5.6	**Logging**							38	36	1	10		29%	65%	1%	6%
5.6.1	**Log Management**							34	15	1	10		57%	25%	2%	17%
5.6.1.1	The voting system SHALL implement default settings for secure log management activities, including log generation, transmission, storage, analysis, and disposal.	Some system's not tested due to not having lab access to hardware for validation.	Not Tested	Pass	Pass	Pass	Pass	4	0	1	0		80%	0%	20%	0%
5.6.1.2	Logs SHALL only be accessible to authorized roles.		Pass	Pass	Pass	Pass	Pass	5	0	0	0		100%	0%	0%	0%
5.6.1.3	The voting system SHALL restrict log access to append-only for privileged logging processes and read-only for authorized roles.		Pass	Pass	Pass	Pass	Pass	5	0	0	0		100%	0%	0%	0%
5.6.1.4	The voting system SHALL log logging failures, log clearing, and log rotation.		Pass	Fail	Fail	Fail	Fail	1	4	0	0		20%	80%	0%	0%
5.6.1.5	The voting system SHALL store log data in a publicly documented format, such as XML, or include a utility to export log data into a publicly documented format.		Fail	Fail	Fail	Pass	Fail	1	4	0	0		20%	80%	0%	0%
5.6.1.6	The voting system SHALL ensure that each jurisdiction’s event logs and each component’s logs are separable from each other.	Some system's not tested due to not having lab access to hardware for validation.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.6.1.7	The voting system SHALL include an application or program to view, analyze, and search event logs.		Fail	Fail	Pass	Pass	Pass	3	2	0	0		60%	40%	0%	0%
5.6.1.8	All logs SHALL be preserved in a useable manner prior to voting system decommissioning.		Pass	Fail	Pass	Pass	Pass	4	1	0	0		80%	20%	0%	0%
5.6.1.9	Logs SHALL NOT contain any data that could violate the privacy of the voter’s identity.		Pass	Fail	Pass	Pass	Pass	4	1	0	0		80%	20%	0%	0%
5.6.1.10	Timekeeping mechanisms SHALL generate time and date values, including hours, minutes, and seconds.		Fail	Fail	Pass	Pass	Pass	3	2	0	0		60%	40%	0%	0%
5.6.1.11	The precision of the timekeeping mechanism SHALL be able to distinguish and properly order all log events.		Fail	Pass	Pass	Pass	Pass	4	1	0	0		80%	20%	0%	0%
5.6.1.12	Only the system administrator SHALL be permitted to set the system clock.	Some system's not tested due to not having lab access to hardware for validation.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.6.2	**Communication Logging**							1	9	0	0		10%	90%	0%	0%
5.6.2.1	All communications actions SHALL be logged.		Fail	Fail	Fail	Fail	Fail	0	5	0	0		0%	100%	0%	0%
5.6.2.2	The communications log SHALL contain at least the following entries:		Fail	Pass	Fail	Fail	Fail	1	4	0	0		20%	80%	0%	0%
5.6.3	**System Event Logging**															
	This section describes requirements for the voting system to perform event logging for system maintenance troubleshooting, recording the history of system activity, and detecting unauthorized or malicious activity. The operating system, and/or applications software may perform the actual event logging. There may be multiple logs in use for any system component.							3	12	0	0		20%	80%	0%	0%
	The voting system SHALL log the following data for each event: a. System ID;															

5.6.3.1	b. Unique event ID and/or type; c. Timestamp; d. Success or failure of event, if applicable;		Pass	Fail	Fail	Pass	Fail	2	3	0	0		40%	60%	0%	0%
5.6.3.2	All critical events SHALL be recorded in the system event log.		Fail	Fail	Fail	Fail	Pass	1	4	0	0		20%	80%	0%	0%
5.6.3.3	At a minimum the voting system SHALL log the events described in the table below.		Fail	Fail	Fail	Fail	Fail	0	5	0	0		0%	100%	0%	0%
5.7	**Incident Response**							0	0	0	10		0	0	0	1
5.7.1	**Incident Response Support**							0	0	0	10		0%	0%	0%	100%
5.7.1.1	Manufacturers SHALL document what types of system operations or security events (e.g., failure of critical component, detection of malicious code, unauthorized access to restricted data) are classified as critical.	Wyle determined that this requirement is not applicable to a web based application. But it is a requirement for a web server and therefore could not be tested at this time.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.7.1.2	An alarm that notifies appropriate personnel SHALL be generated on the vote capture device, system server, or tabulation device, depending upon which device has the error, if a critical event is detected.	Wyle determined that this requirement is not applicable to a web based application. A system server notification should be sent to administrators when issues arise with the web server.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.8	**Physical and Environmental Security**							4	0	6	60		1.8%	0.0%	2.7%	95.6%
5.8.1	**Physical Access**							4	0	6	35		9%	0%	13%	78%
5.8.1.1	Any unauthorized physical access SHALL leave physical evidence that an unauthorized event has taken place.	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.8.2.1	The voting system SHALL disable physical ports and access points that are not essential to voting operations, testing, and auditing.	Some system's not tested due to not having lab access to hardware for validation.	Not Tested	Not Tested	Not Tested	Not Tested	Pass	1	0	4	0		20%	0%	80%	0%
5.8.3.1	If a physical connection between the vote capture device and a component is broken, the affected vote capture device port SHALL be automatically disabled.	Wyle determined that this requirement is not applicable to a web based application. A physical connection will only be made during a single instance of vote casting.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.8.3.2	The voting system SHALL produce a visual alarm if a connected component is physically disconnected.	Wyle determined that this requirement is not applicable to a web based application.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.8.3.3	An event log entry that identifies the name of the affected device SHALL be generated if a vote capture device component is disconnected.	Wyle determined that this requirement is not applicable to a web based application.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.8.3.4	Disabled ports SHALL only be re-enabled by authorized administrators.	Some system's not tested due to not having lab access to hardware for validation.	Not Tested	Not Tested	Pass	Pass	Pass	3	0	2	0		60%	0%	40%	0%

5.8.3.5	Vote capture devices SHALL be designed with the capability to restrict physical access to voting device ports that accommodate removable media with the exception of ports used to activate a voting session.	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.8.3.6	Vote capture devices SHALL be designed to give a physical indication of tampering or unauthorized access to ports and all other access points, if used as described in the manufacturer's documentation.	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.8.3.7	Vote capture devices SHALL be designed such that physical ports can be manually disabled by an authorized administrator.	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.8.4	**Door Cover and Panel Security**							0	0	0	5		0%	0%	0%	100%
5.8.4.1	Access points such as covers and panels SHALL be secured by locks or tamper evident or tamper resistant countermeasures and SHALL be implemented so that kiosk workers can monitor access to vote capture device components through these points.	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.8.5	**Secure Paper Record Receptacle**							0	0	0	5		0%	0%	0%	100%
	If the voting system provides paper record containers then they SHALL be designed such that any unauthorized physical access results in physical evidence that an unauthorized event has taken place.	Wyle determined that this requirement is not applicable to a web based application	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.8.6	**Secure Physical Lock and Key**							0	0	0	10		0	0%	0%	100%
5.8.6.1	Voting equipment SHALL be designed with countermeasures that provide physical indication that unauthorized attempts have been made to access locks installed for security purposes.	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.8.6.2	Manufacturers SHALL provide locking systems for securing vote capture devices that can make use of keys that are unique to each owner.	Wyle determined that this requirement is not applicable to a web based application. Implementation of this requirement would be in a remote server facility.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.8.7	**Media Protection**															
	These requirements apply to all media, both paper and digital, that contain personal privacy related data or other protected or sensitive types of information.							0	0	0	5		0%	0%	0%	100%
5.8.7.1	The voting system SHALL meet the following requirements: a. All paper records (including rejected ones) printed at the kiosk locations SHALL be deposited in a secure container; b. Vote capture device hardware, software and sensitive information (e.g., electoral roll) SHALL be physically protected to prevent unauthorized modification or disclosure; and c. Vote capture device hardware components, peripherals and removable media SHALL be identified and registered by means of a unique serial number or other identifier.	Wyle determined that this requirement is not applicable to a web based application.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.9	**Penetration Resistance**							18	10	8	9		40%	22%	18%	20%
5.9.1	**Resistance to Penetration Attempts**							18	10	8	9		40.0%	22.2%	17.8%	20.0%
5.9.1.1	The voting system SHALL be resistant to attempts to penetrate the system by any remote unauthorized entity.		Pass	Pass	Pass	Fail	Pass	4	1	0	0		80%	20%	0%	0%

5.9.1.2	The voting system SHALL be configured to minimize ports, responses and information disclosure about the system while still providing appropriate functionality.		Pass	Fail	Pass	Pass	Pass	4	1	0	0		80%	20%	0%	0%
5.9.1.3	The voting system SHALL provide no access, information or services to unauthorized entities.		Pass	Fail	Pass	Fail	Pass	3	2	0	0		60%	40%	0%	0%
5.9.1.4	All interfaces SHALL be penetration resistant including TCP/IP, wireless, and modems from any point in the system.		Pass	Pass	Pass	Fail	Pass	4	1	0	0		80%	20%	0%	0%
5.9.1.5	The configuration and setup to attain penetration resistance SHALL be clearly and completely documented.	Based on the system documentation provided by the participants in this test campaign, Wyle was unable to validate this requirement. However, Wyle deems it necessary for future testing.	Not Tested	Not Tested	Not Tested	Fail	Not Tested	0	1	4	0		0%	20%	80%	0%
5.9.2.1	The scope of penetration testing SHALL include all the voting system components. The scope of penetration testing includes but is not limited to the following: System server; Vote capture devices; Tabulation device; All items setup and configured per Technical Data Package (TDP) recommendations; Local wired and wireless networks; and03/09/2011 Internet connections.		Pass	Pass	Pass	Fail	Fail	3	2	0	0		60%	40%	0%	0%
5.9.2.2	Penetration testing SHALL be conducted on a voting system set up in a controlled lab environment. Setup and configuration SHALL be conducted in accordance with the TDP, and SHALL replicate the real world environment in which the voting system will be used.	Wyle was unable to validate this requirement, but deems it necessary for future testing.	N/A	N/A	N/A	Fail	N/A	0	1	0	4		0%	20%	0%	80%
5.9.2.3	The penetration testing team SHALL conduct white box testing using manufacturer supplied documentation and voting system architecture information. Documentation includes the TDP and user documentation. The testing team SHALL have access to any relevant information regarding the voting system configuration. This includes, but is not limited to, network layout and Internet Protocol addresses for system devices and components. The testing team SHALL be provided any source code included in the TDP.	Wyle was unable to validate this requirement, but deems it necessary for future testing.	N/A	N/A	N/A	N/A	N/A	0	0	0	5		0%	0%	0%	100%
5.9.2.4	Penetration testing seeks out vulnerabilities in the voting system that might be used to change the outcome of an election, interfere with voter ability to cast ballots, ballot counting, or compromise ballot secrecy. The penetration testing team SHALL prioritize testing efforts based on the following: a. Threat scenarios for the voting system under investigation; b. Remote attacks SHALL be prioritized over in-person attacks;	Wyle was unable to validate this requirement, but deems it necessary for future testing.	Not Tested	Fail	Not Tested	Not Tested	Not Tested	0	1	4	0		0%	20%	80%	0%

	c. Attacks with a large impact SHALL be prioritized over attacks with a more narrow impact; and d. Attacks that can change the outcome of an election SHALL be prioritized over attacks that compromise ballot secrecy or cause non-selective denial of service.																		

	Pass	Fail	Not Tested	N/A
Average summary	24%	22%	24%	30%

Federal Voting Assistance Program (FVAP) Penetration Testing of a Simulated Election

16 September 2011

Penetration Test of Simulated Election

Delivery Order # DO 80047-0037

Task Order # 5.1.3

Final Report

Version 1

16 September 2011

Executive Summary

The Federal Voting Assistance Program (FVAP) has been mandated to carry out a remote electronic voting demonstration project in which a significant number of uniformed service members could cast ballots in a regularly scheduled election. To address security issues associated with such a project, FVAP collaborated with RedPhone Corporation (RedPhone), a professional information security company and the U.S. Air Force Institute of Technology (AFIT) to carry out penetration testing of three electronic voting systems.

Penetration testing, or PenTesting, is an integral form of security testing which challenges online system security using techniques similar to those used by criminals and other hostile entities intent on inflicting genuine harm. However, in an authorized PenTest, all parties agree to the testing; and the testing is conducted for the benefit, not the harm, of the system vendors and all stakeholders. The findings of the PenTest are evaluated so that mitigation strategies can be developed and applied to manage security risks to acceptable levels.

The PenTest was conducted in August 2011 using online voting systems developed by three major online voting system vendors (who will remain anonymous in this report), whose systems are successfully used by jurisdictions throughout the world to conduct online elections. The intent of this PenTest and subsequent analysis was to provide the FVAP Director with usable information about the security posture of current online voting systems, and to provide data that supports decisions regarding FVAP's future Congressionally-mandated demonstration project. This document presents the findings and recommendations of this PenTest as well as suggestions for future work in this realm.

The most notable overall finding of the PenTest was that none of the vendors' systems were compromised. Neither RedPhone nor AFIT were able to penetrate or exploit the three online voting systems during this testing exercise. Additionally, all evaluated online voting systems passed all of the Penetration Testing requirements enumerated in the Security section of the UOCAVA Pilot Program Testing Requirements (UPPTR). Despite the systems passing this testing, AFIT and RedPhone found areas that each vendor should address to ensure that their systems are as secure as possible. Specific recommendations include:

- improving technical security;
- hardening physical security;
- building a cooperative security relationship;
- assigning security responsibility between the servers and the remote voting stations;
- including personnel training, system certification, and continuous security monitoring from government and industry best practices and guidance;
- undertaking periodic PenTests and other security tests in the future with concurrent development of test cases and requirements; and
- developing operational PenTests during iterative pilot projects conducted in CONUS, OCONUS, Ship Board and Hostile environments, which are intended to lead to the Congressionally-mandated FVAP demonstration project.

Table of Contents

1 Introduction

1.1 Why Penetration Testing Was Done

Perhaps the most cherished right American citizens have is to govern themselves by electing leaders through the voting process. Unarguably, no one is more entitled to this right than the men and women of the United States military who commit themselves to defending this right. Yet, many of military service members, their dependents, and other qualified voters are located throughout the world in places that make it impossible for them to physically report to a polling place to cast their ballot. To accommodate these individuals, a paper-based, absentee voting process is currently utilized by military voters, their dependents, and other overseas voters.

The Federal Voting Assistance Program (FVAP) is exploring the use of current electronic technologies to provide authorized military voters with online voting capability through an electronic network. Meanwhile, election jurisdictions in the U.S. have undertaken their own online voting pilot projects by experimenting with secure electronic ballot delivery, using email/fax/U.S. Postal Service to return marked ballots. The jurisdictions focused on convenience issues, the potential for increased turnout, and the opportunity to streamline the UOCAVA voter absentee voting process to ensure ballots are delivered to their respective voting jurisdictions accurately and in sufficient time to ensure that these absentee ballots are counted.

There are security issues inherent in any electronic or online voting system, just as there are security issues with the current paper-based absentee voting process. Online voting security issues must be individually and collectively addressed in order for online voting to be an acceptable alternative to the current paper-based process. The goal is not perfect security, since perfect security is, and will always be, impossible to attain. Therefore, the standard to reach is security that is at an appropriate level, or provides a high level of assurance. The decision to use online voting involves a balance between the security risks and the benefits to be derived.

One way to measure and improve online voting security is to conduct security testing for systems that are currently available and in use. One such security test is called Penetration Testing, or PenTesting. PenTesting involves attempts to challenge the security capabilities of the system in question. A PenTest is conducted by individuals appropriately trained, experienced, and authorized in this discipline. PenTesting is both an art and a science, and it uses a variety of techniques, including technical, administrative, personnel, physical, and all other methods that can "break" a system. It uses techniques similar to those used by unscrupulous criminals who are intent on inflicting genuine harm to a system. The difference in an authorized PenTest is that all parties agree to the testing, and the test is conducted for the benefit, not the harm, of the system vendors and all stakeholders.

PenTests are conducted according to strict Rules of Engagement, and they include well-defined legal permissions. PenTest results can expose system weaknesses or vulnerabilities that match specific threats—threats that would be posed by malicious sources. The results of a genuine, successful attack by a malicious source can have negative system consequences or impacts, and these factors result in a risk

level (high, medium, low) to the system. The PenTest is designed to simulate a "real" attack to expose vulnerabilities to particular threats, and to provide intelligence that can be used to improve security.

The PenTest findings can be evaluated; and mitigation strategies can be developed and applied to control and reduce risks to acceptable levels. Controls take the form of safeguards and countermeasures designed to prevent, detect, and correct problems; thus reducing security risks to acceptable levels. This process, in theory, "hardens" the system against potential true attackers in a live environment.

During August 2011, a PenTest was performed to expose security risks for online voting based on three products offered in the marketplace. The systems subjected to the PenTest were three companies currently providing online voting capabilities throughout the world. To protect their privacy, in this report, these companies are referred to as Vendor-1, Vendor-2, and Vendor-3. These vendors agreed to participate in a PenTest as a way to improve their system security, with the goal of providing secure online voting capabilities to authorized individuals.

Two organizations conducted the PenTest on the cooperating vendors' systems. One of these organizations, RedPhone (www.redphonecorporation.com), is an experienced information security company. RedPhone is located in the Washington, DC area and specializes in PenTesting and other information security protocols for a wide variety of clients including multinational corporations, the U.S. Air Force, U.S. Army, U.S. Army National Guard, U.S. Navy, U.S. Marine Corps, U.S. Coast Guard, U.S. Customs, Bureau of Alcohol, Tobacco and Firearms, the Department of Justice, and the U.S. Navy Criminal Investigative Service.

The second organization that conducted PenTesting as part of this project was the U.S. Air Force Institute of Technology (AFIT) located at Wright-Patterson Air Force Base in Dayton, Ohio (www.afit.edu). PenTesters in the AFIT organization consisted of highly motivated, well-educated, ROTC college engineering and computer science students on a summer educational internship. The students were participants in the ACE (Academic Center of Excellence) Cyber Security Boot Camp Program. This program is held each summer for a select group of ROTC students studying computer science or cyber security. The curriculum consists of cyber warfare, digital forensics, cryptography, reverse engineering of software and many other subjects. The boot camp lasts for eight weeks and culminates in "Hack Fest." During Hack Fest, the students participate in various exercises where they conduct cyber-attacks, defend against a cyber-attack, and plan attribution strategies. The students were mentored by some of the most skilled experts in the field of cyber security, all having earned their PhDs in cyber security or computer science. These highly trained professionals have direct access to the most modern facilities and equipment in the world.

The mix of PenTesters (the juxtaposition of the professional experts at RedPhone and the academic college students) provided the wisdom and experience of a professional company with the creative ideas and approaches of youthful, competitive, highly skilled and highly motivated military college engineering students, mirroring in many ways the attributes of youthful hackers in the threat environment.

This report provides the results of these two PenTests. Appendix A is the report from the AFIT students and Appendix B provides the report from RedPhone. Appendix C is a Security Gap Analysis of the

UOCAVA Pilot Program Testing Requirements that was conducted by RedPhone for FVAP in February 2011, before the commencement of the PenTest project. The AFIT students' report at Appendix A gives a high-level view of the findings, vulnerabilities, impacts, and recommendations for improvement, while the RedPhone report at Appendix B gives a more detailed, "bit-level" technical evaluation of the vendors' security risks. Both reports have been reviewed and all proprietary information has been removed; however, each vendor did receive a report specific to its own company that can be used to improve system security.

Chapters 2 and 3 of this paper summarize the findings and recommendations, but leave the details to the Appendices, which were written by the individual groups who conducted the actual tests.

1.2 Impact of Results

The results from these two PenTests will inform all online voting system vendors and stakeholders of security vulnerabilities, threats, impacts, and risks, and provide recommended controls (safeguards and countermeasures designed to prevent against, detect, and protect assets), thereby implementing mitigation strategies to reduce the risks associated with online voting to acceptable levels. This research may also assist with general recommendations to the U.S. Election Assistance Commission in the adoption of voting system standards and relevant security standards for internet voting.

1.3 Evolution of the Penetration Test

The 2002 National Defense Authorization Act (NDAA) and the Military and Overseas Voter Empowerment (MOVE) Act of 2009 significantly expanded the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) of 1986, which protects the right of service members to vote in federal elections regardless of where they are stationed and calls for the establishment of a demonstration project to test electronic voting for absentee uniformed services voters in a federal election.

Security of online voting systems has been the subject of much conversation among voting technology providers, academics, and those concerned with online voting security. FVAP has so far conducted three UOCAVA Solutions Working Group (USWG) meetings over the past two years (2010-2011), with the main discussion topic being the security of online voting systems. The need for data providing security information about these systems was the genesis of the PenTesting effort. The NDAA requires consideration of the national level threat. As such, FVAP has engaged in this direct effort to learn the current level of security as established currently in fielded/available systems for procurement.

There have been other types of electronic voting systems (for in-polling place use) subjected to certification testing through the EAC and or various state certification programs that have included a minimum amount of PenTesting, but not on the scale that has been done through this effort and this has not included PenTesting of online voting systems. The FVAP PenTest is of a much larger scope and included three online voting systems that are widely used worldwide. The intent of the PenTest was to provide the FVAP Director usable information about the online voting systems' security posture, and provide data that supports decisions on the electronic voting system way ahead that FVAP must develop and execute.

1.4 The Stakeholders Involved

FVAP could not do this testing alone. Several organizations and commercial enterprises were involved in executing this project. The FVAP Director desired to have as much participation from the voting system vendors as possible, and the three major vendors in particular. The project required setting up voting stations for each vendor's system to allow volunteer voters to cast their ballots. The space for the voting stations required an acceptable level of privacy, yet easy access for the volunteers. Technical expertise was required to set up these systems and to provide the required network connectivity. There also was a need for technical expertise to plan how to best attempt to breach the security of the voting systems.

AFIT volunteered their assistance in this experiment and provided the laboratory space for the "hackers" to use, space for the voting systems and volunteer voters, and specially trained students to serve as one set of "malicious" sources. AFIT also provided all network connectivity needed for the voting systems, the Internet Protocol (IP) addresses needed for the experiment and all of the "hacking" software used in the PenTest including COTS (commercial off the shelf), open source and proprietary tools.

Professional cyber attacking experience is also a critical part of any exercise like this and RedPhone provided all the technical expertise needed in this area. The curriculum at AFIT did not cover cyber hacking to the degree necessary to execute a successful penetration attempt. Therefore, additional training on cyber-attacks was provided to attempt a penetration attack on their voting systems. The vendors' names will not be used in this jointly by FVAP, RedPhone and Mr. John Rossi, a recently retired government employee who taught cyber security to federal employees. The training was comprehensive and laid a firm foundation for the students of AFIT to design and execute their attack plan.

AFIT was a superb venue for the PenTest. The staff was very helpful and cooperative and had a real interest in this project. The PenTesting was mutually beneficial to both AFIT and to FVAP. AFIT enhanced student skills and FVAP gathered useful data about online voting system security. AFIT also expressed interest in working with FVAP on future projects in this area.

None of this would have been possible without the cooperation of the three voting system vendors whose openness and cooperation was key to a successful PenTesting effort that provided much usable data.

1.5 The Penetration Teams

RedPhone is a high profile information security company that provides cyber audits to the federal government, local government and to commercial enterprises. RedPhone developed the cyber security test plan that outlined what specifically the penetration attempts would do and what they would not do. RedPhone also provided one two-person team that performed the PenTest over the 72-hour test period. The AFIT students were also active participants in the PenTesting. The students formed two three-person teams that worked to penetrate the voting systems concurrently with RedPhone.

1.6 The Process

The PenTest was successful due to the cooperation of all the stakeholders. The next step may be to hold a mock election for a local election jurisdiction or for an organization. While the actual voting is being conducted, "hackers" could be attempting to enter and alter the votes being cast. Another option may be to have a "mock" election and have voters from several different locations participating in the election. This would distribute the voters in what would be a more normal pattern. The "hackers" also would need to be more skilled to fully test voting system vulnerabilities. Many different scenarios could be developed to provide even more detailed data on electronic voting security. The bottom line is that FVAP should not stop here, but forge ahead to collect as much data as possible to improve the decision making process for the mandated demonstration project.

2 Test Development and Participants

Multiple vendors were invited to participate in the mock election scenario exercise held at AFIT. Ultimately, three were chosen and participated, agreeing to allow AFIT students and industry professional PenTesters to attempt to breach the security of their remote Internet-based voting systems. Mutual Non-disclosure Agreements (MNDA) and Rules of Engagement were signed by all parties and participants in the PenTesting to ensure that appropriate boundaries were defined. The AFIT students and RedPhone PenTesters were not permitted to use social engineering methods or to interfere with corporate IT systems; only those servers and voting stations used in the mock election exercise were targeted.

RedPhone fully understood the requirements as outlined in the UOCAVA Pilot Program Testing Requirements (UPPTR) for security testing and identified the following requirements as essential:

1. Security test results must be documented and formatted in a way that conveys information to FVAP that can feed the internal risk management processes.

2. Security test reports must contain information sufficient for senior leadership to make informed, risk-based decisions.

3. Experienced tactical information security teams will be required to meet the schedule.

4. Formal project management techniques will be needed for PenTest coordination across multiple locations simultaneously.

RedPhone's approach was based on the National Institute of Standards & Technology (NIST) Special Publication 800-53 rev. 3 and Federal Information Security Management Act (FISMA) requirements. It also leveraged the National Security Agency Information Assurance Methodology (NSA-IAM/IEM) and the Information Systems Security Assessment Framework (ISSAF) approach often used by federal agencies to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels.

The Security Test and Evaluation (ST&E) process directly supports security accreditation by evaluating the security controls in the information system. This evaluation is conducted to determine the effectiveness of those security controls in a particular environment of operation and the vulnerabilities in the information system after the implementation of such controls. The ST&E can include a variety of verification techniques and procedures to demonstrate the effectiveness of the security controls in the information system. These techniques and procedures can include such activities as observations, interviews, exercises, functional testing, PenTesting, regression testing, system design analysis, and test coverage analysis. The level of rigor applied during evaluation is based on the robustness of the security controls employed in the information system—where robustness is defined by the strength of the security controls and the assurance that the controls are effective in their operation. Authorizing officials and their designated representatives are better positioned to make residual risk determinations and the ultimate decisions on the acceptability of such risk after reviewing the results of such evaluations.

ST&E should not be viewed as a static process. An information system is authorized for operation at a specific point in time reflecting the current security state of the system. However, the inevitable changes to the hardware, firmware, and software in the information system, and the potential impact those changes may have on the security of that system, require a more dynamic process—a process capable of monitoring the ongoing effectiveness of the security controls in the information system. Thus, the initial security accreditation of the information system must be supplemented and reinforced by a structured and disciplined process involving: (1) the continuous monitoring of the security controls in the system; and (2) the continuous reporting of the security state of the system to appropriate agency officials.

RedPhone recognizes that detecting vulnerabilities is a specialized security function within the information technology field. Therefore, they developed small, highly skilled teams specifically trained for federal ST&E support. These information assurance Tiger Teams consisting of one Tactical Team Leader, one or more PenTesters, an audit and policy analyst, and one system engineer. Their functions and roles vary depending on the size and scope of the engagement. The purpose of these teams is to use a systematic approach to identifying and reporting vulnerabilities. RedPhone uses the process outlined in Figure 1 below to support penetration testing efforts.

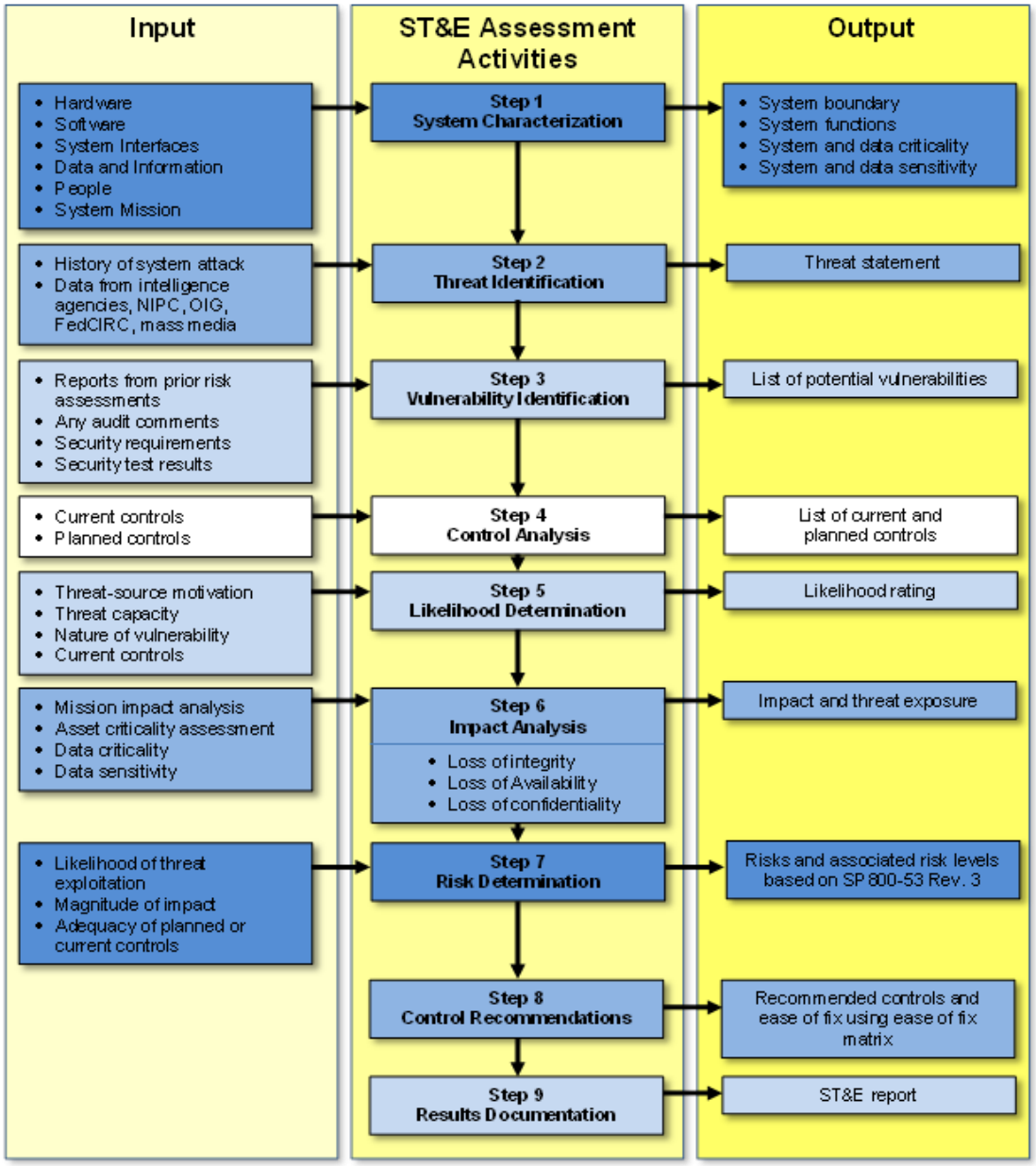


Figure 1. RedPhone Security Test and Evaluation Process

Identifying risk for an IT system requires a keen understanding of the system's processing environment. The ST&E team must therefore collect system-related information first, which is usually classified as follows:

1. Hardware
2. Software
3. Port, protocols and services being used
4. System interfaces (e.g., internal and external connectivity)
5. Data type and classification
6. Persons who support and use the IT system

7. System mission (e.g., the processes performed by the IT system)
8. System and data criticality (e.g., the system's value or importance to an organization)
9. System and data sensitivity

Use of Automated Scanning Tools and other proactive technical methods were used to collect system information efficiently. For example, network mapping tools were used to identify the services that run on a large group of hosts and provide a quick way of building individual profiles of the target IT system(s). RedPhone used at a minimum Nessus, NMAP, and Metasploit for PenTests.

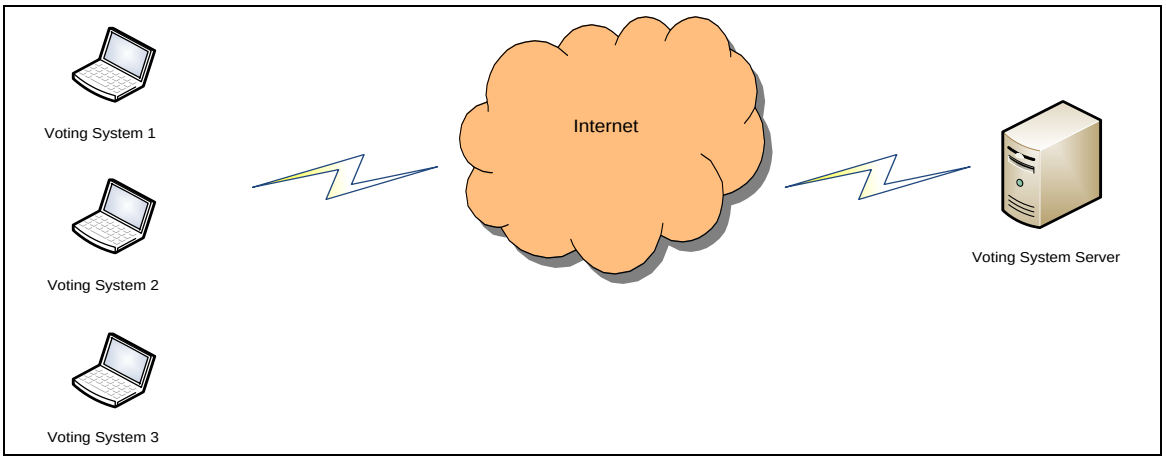
3 Methodology

The following text describes the methodology used to conduct the PenTest and outlines how the experiment was designed, the test environment, the teams involved in the test, and how ballots were cast. Also outlined is what was *not* undertaken for this mock election PenTest.

The AFIT students received training from Mr. Rossi on network security concepts. They also received three separate PenTesting training sessions provided by the RedPhone team. This training provided the students with actionable knowledge on how to construct a test plan, execute the plan, and properly format and report the team's findings. Additionally, the students were provided hands-on training using many "hacker" tools. Examples of these tools include Metasploit, Nessus and NMAP. Each training session provided a logical information progression on each vendor, the tools (and how to use them), and how to build a successful PenTest. The AFIT students also were provided templates for constructing their test plan and the final report format for their findings. The graphic in Figure 3 provides a step-by-step explanation of how the voter cast a ballot and at what point the PenTest teams attempted to penetrate the systems.

A student lounge used by AFIT students served as the polling place for the mock election portion of the PenTest. This area was selected because it was easily accessible by the AFIT students, and they were frequently in the area during breaks and lunch. Since the students were the volunteer voters for the experiment, it was essential that an area be provided that was convenient for them to access. AFIT provided each vendor one laptop computer with only the operating system, Internet Explorer and Firefox installed. The voting computers were inserted into the AFIT network, but were provided Internet access without going through any firewalls or other security devices. Figure 2 below, graphically depicts the AFIT test system environment.

Figure 2. Depiction of Voting Computers used at AFIT



AFIT assigned each computer a static IP address and these IP addresses were given to each hacking team. The systems were left operational for the entire 72-hour period. The student lounge was accessible by the volunteer voters at any time to cast their ballots; however, traffic through the lounge did abate after

normal duty hours, which are 0730–1700 Monday through Friday. Although the AFIT facility is located on a secure military installation, there were no specific physical security precautions taken to protect the machines; no locks or security cables were used to secure the systems to the shelf; and no guards posted to protect the voting machines. The systems did not time out nor did they allow a screen saver to pop up after a certain amount of time.

The volunteer voters walked up to the system of their choice—most voted on all three—and cast their ballots. The three vendors supplied any necessary logon credentials, and the voters used these credentials to access each vendor's Internet voting site. These credentials varied from vendor to vendor, were not complicated, easily used, and allowed the voter to logon to each system's home page. Each vendor's system had a different way to cast an online ballot, but the systems were all intuitive and clear instructions were provided on the screen. Each vendor was given one ballot to load into their system. Every voter had the opportunity to vote on each ballot, and voters were prompted if they had under voted or over voted on a particular ballot. Two of the races on the ballot allowed the choice of a single candidate. One race allowed for the voter to pick up to three of six possible candidates.

Both the AFIT student and the RedPhone penetration teams had direct access to each voting computer, and they did approach each machine and cast ballots. The RedPhone team worked mostly off site, but they did approach the machines in the student lounge and cast ballots. As this was a cooperative test, both the AFIT and RedPhone PenTest teams were provided voting computer and voting system server IP addresses. This allowed more time for penetrating the voting systems without necessarily jeopardizing other AFIT production systems.

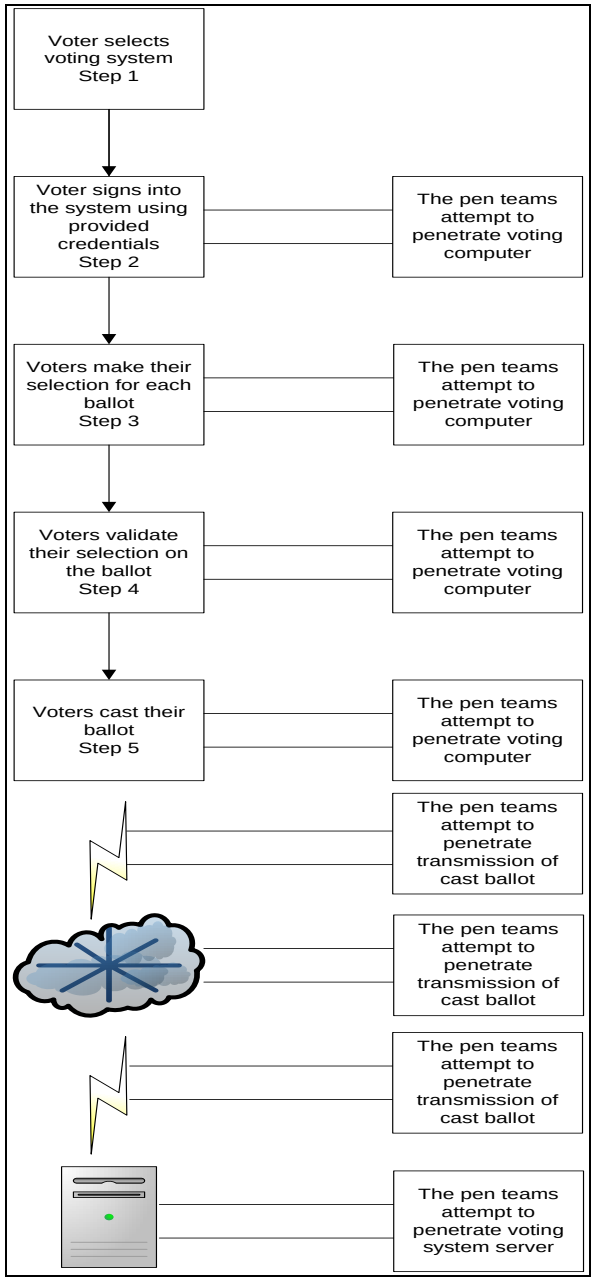


Figure 3. Voter Actions and Penetration Attempts

The PenTest teams were actively attempting to enter the vendor online voting system to change, alter or delete a vote, or votes, beginning at Step 2 and continuing until after the ballot reached the voting system server. These servers were not physically located at AFIT, but were geographically dispersed, with one server located outside the continental United States. Similar to the voting computers, the IP addresses of the voting systems servers were also provided to the penetration testing teams.

4 Results

The PenTest findings included technical, administrative, personnel, and physical vulnerabilities of the online voting systems tested. The table below lists each finding, the importance of each finding, and associated recommendations related to each finding. In general, these findings indicate the presence of system vulnerabilities. These vulnerabilities can be exploited by threats and result in impacts/consequences to system confidentiality, integrity, and availability. Each finding must be addressed; the risks mitigated, accepted or transferred, and the security posture maintained over the life of the voting system in order to remain within acceptable levels.

It is important to note that all vendor systems did not present all of these vulnerabilities. Additionally, some of the vulnerabilities listed below are not vulnerabilities specific to online voting systems, but can be present in polling place voting systems or paper ballot absentee voting systems (i.e. "shoulder surfing"). Also, vulnerabilities associated with access to remote voting machines and kiosk supervision/security could potentially have been addressed by the voting system vendors, but client computer security was not under the control of the vendors and was not part of this official test scenario. Even so, with three days of unrestricted access to the voting stations, the attackers were unable to use this advantage to compromise any aspect of the voting process.

Table 1. Finding/Importance/Recommendation

Finding	Importance	Recommendation
Open Secure Shell (SSH login) was evident.	Anyone having the correct IP address can access the system, whether authorized or not. The login was protected by userid/password, but these can be hacked by a variety of methods. A successful attack can give a hacker control over the vendor's server. The testers were unable to exploit this weakness given the limited time of the test coupled with the requirement to test a variety of weaknesses.	Build stronger authentication. Use either 2-factor (e.g., password and token, smartcard, etc., and/or biometric reader), or strengthen password restrictions such as require upper and lower case alpha characters, require numerals, special characters, etc., and change passwords frequently. Minimize user rights. Follow the recommendation of the U.S. Computer Emergency Response Team (US-CERT) regarding the use of CTR (counter) Mode Encryption.
Testers discovered vendor server information using common hacker tools.	Hackers can use this information to exploit known (or discovered) vulnerabilities, narrow their attack tool choice to focus on the specific vendor system, and use in a social engineering attack. This is a first step in hacking into a system. Once the hack is successful, the system is subject to degraded confidentiality, integrity, and availability.	Use software scanning tools to limit information accessibility; use deception if possible.
Testers breached physical security at the voting	Testers created their own administrator accounts, giving them inappropriate access to	Assign remote terminal security responsibility to the jurisdiction conducting the election. Provide user security training and security

terminal and had easy access to the terminals.	the system and to other voters' activities. Testers were also able to "shoulder surf" other users to obtain sensitive information.	awareness.
SQL injection was able to be performed.	Hackers overflow legitimate computer memory areas and interfere with computer logic and other areas "off limits" to users. This capability puts control into the hands of unauthorized hackers.	Disallow users from entering free-flowing input in database queries. Use prepared statements to limit what a user can enter. Limit the character number and types a user may enter. This limits user control and keeps control with the vendor and the vendor software. This also may assist in mitigating the cross-site scripting vulnerability by controlling user input.
There was use of an SSL cookie.	The application issued a cookie without the secure flag set; therefore, users are not protected from cookies transmitted in unencrypted connections—the cookie is transmitted in clear-text and can be intercepted by hackers.	Set secure flag to prevent transmitting unencrypted cookies.
Script files were unprotected from downloading.	This vulnerability allows hackers to map the site's functionality and expose potential vulnerabilities ripe for attack.	Prevent unauthorized users from downloading scripted files.

Event logging records application, security, and system events for correlation and forensic analysis. Event logging can occur at several places including firewalls, intrusion detection systems, routers and servers, and at the application level. With the event logs, RedPhone obtained information about system hardware, software, and system components, and most importantly security events on both the local and remote servers during the penetration testing. Computers typically record events in the following three logs:

1. Application log

The application log contains events logged by programs. For example, a database program may record a file error in the application log. Events that are written to the application log are determined by the developers of the software program.

2. Security log

The security log records events such as valid and invalid logon attempts, as well as events related to resource use, such as the creating, opening, or deleting of files. For example, when logon auditing is enabled, an event is recorded in the security log each time a user attempts to log on to the computer. You must be logged on as Administrator or as a member of the Administrator group in order to turn on, use, and specify which events are recorded in the security log.

3. System log

The system log contains events logged by the system components. For example, if a driver fails to load during startup, an event is recorded in the system log.

During the mock election PenTesting exercise, RedPhone maintained communication with each of the vendors and their managed security service providers to determine the speed at which events were triaged, communicated, escalated based on severity, and the accuracy of the logging data. Specific information was recorded, including attacking source IP addresses, time, and date. Throughout the penetration test window, accurate and timely responses from all three vendors participating in the PenTest were provided. Attack events were captured, noted, and escalated quickly with a high degree of accuracy.

Voting systems today face a threat landscape that involves stealthy, targeted, and financially motivated attacks that exploit vulnerabilities at both ends and the middle of the communications process. Many of these sophisticated threats can evade traditional security solutions, leaving voting systems vulnerable to data theft and manipulation, disruption of services, and have the potential to irreparably damage the integrity of the voting process. A review of the UOCAVA Pilot Program Testing Requirements (UPPTR), the Security Gap Analysis found in Appendix C, and the findings from the mock election PenTest exercise held during August 2011 confirmed our suspicions regarding the current threat landscape.

In summary, the Security Gap Analysis prepared by RedPhone and located in Appendix C of this report, found a total of 248 requirements that were identified in the UPPTR document from August 2008 and 2010. While many are functional requirements, all were evaluated by RedPhone for their security risk and potential exploit impacts. Risks were rated as low, medium and high relative to confidentially, integrity and availability. A security crosswalk was used to map the UPPTR to multiple industry and federal government security best practices and mandated requirements including NIST, International Standards Organization (ISO), FISMA, the Government Accountability Office (GAO), the Department of Defense (DoD), and Director of Central Intelligence Directive 6/3 Protecting Sensitive Compartmented Information Within Information Systems (DCID 6/3). Security weaknesses can fall into more than one of three categories that include confidentiality, integrity or availability. Security weaknesses and gaps were identified and associated with potential mitigating strategies. Of the 248 requirements evaluated, 144 requirements had an impact on confidentially, 237 had an impact on Integrity, and 178 had an impact on availability. Of the 248 requirements, 39 were categorized as only having a low impact to security. However, 132 were considered to have a medium impact, and 86 were considered to have a high potential risk.

With 218 findings being of medium to high impact, it is clear that voting data has an unusual security posture. Following the mock election scenario exercise, we derived several conclusions. Voting systems, like many DoD systems, handle sensitive data from all locations worldwide, and therefore, the best protection possible would require that both end points—and the transmission medium—be tightly controlled to maintain data integrity, confidentiality and system availability.

Lastly, without endpoint physical security on the voter side of the equation, any operating systems can be corrupted in time. Despite the presence of antivirus and intrusion prevention technology on most end-user systems, most security holes remain completely unplugged because users do not have sufficient knowledge to secure the operating systems adequately.

Only dedicated, well managed, and often out-sourced, hosting providers blend best of breed technologies capable of identifying potential threats, blended attacks, and distributed denial of service attacks, and are able to escalate quickly to shut down these attacks. However, the communications medium remains a considerable threat to the integrity of the data/votes since it is out of the provider's control while in transit. At the present, only dedicated communications solutions, with a tightly controlled security posture, such as the Defense Information Systems Network (DISN) would offer such a secure communications channel. Additionally, only dedicated kiosk-based voting stations that are managed and proctored by voting officials can offer a secure endpoint.

FVAP conducted a series of tests over the past year. One test involved the new EAC's UPPTR dated August 25, 2010. The EAC has the responsibility to develop and implement the certification guidelines to which all voting system manufacturers must adhere. These new EAC UPPTR requirements were developed to serve as a guide to participants in any online pilot voting project. These requirements would provide guidance to pilot project participants regarding what exactly their online pilot project voting system would be required to do. FVAP requested three voting system manufacturers voluntarily subject their system to Voting System Test Lab (VSTL) testing against these new standards. A VSTL is an independent third party accredited as a lab by NIST and certified by the EAC to test voting systems to written standards. The VSTL test was conducted to determine if the requirements were sufficient as written and testable, not to determine if the voting system could pass the new requirements. Section 5.9 of the UPPTR outlines PenTesting and states that systems being tested must be able to pass each portion of section 5.9 in order to pass the VSTL PenTest. The AFIT/RedPhone PenTesting, however, was conducted to determine if the online voting systems could be penetrated to the extent that votes were changed, altered or deleted. The PenTesting section of the UPPTR was used as the testing criteria for passing or failing the PenTest.

In Table 2 below are listed two systems that the VSTLs tested. These two systems were selected by the Director of FVAP to participate in VSTL testing. The AFIT/RedPhone test had three systems. Two of the systems were the systems that the VSTLs tested. One additional vendor was invited to participate in the AFIT/RedPhone test. The table below compares the VSTL testing results and the AFIT/RedPhone PenTesting.

Table 2. Comparison of VSTL test results and AFIT/RedPhone PenTesting

5.9 Penetration Resistance	Requirement Matrix	VSTL System 1	VSTL System 2	AFIT System 1	AFIT System 2	AFIT System 3
5.9.1 Resistance to penetration attempts	High, Medium or Low	Medium	Medium	Medium	Medium	Medium
5.9.1.1	The voting system SHALL be resistant to attempts to	Pass	Pass	Pass	Pass	Pass

5.9 Penetration Resistance	Requirement Matrix	VSTL System 1	VSTL System 2	AFIT System 1	AFIT System 2	AFIT System 3
Resistant to attempts	penetrate the system by any remote unauthorized entity.					
5.9.1.2 System information disclosure	The voting system SHALL be configured to minimize ports, responses and information disclosure about the system v still providing appropriate functionality	Pass	Pass	Pass	Pass	Pass
5.9.1.3 System access	The voting system SHALL provide no access, information or services to unauthorized entities.	System Access: All 215 exploits were unsuccessful.	System Access: All 35 exploits were unsuccessful.	Pass	Pass	Pass
5.9.1.4 Interfaces	All interfaces SHALL be penetration resistant including TCP/IP, wireless, and modems from any point in the system.	Interfaces: All 215 exploits were unsuccessful.	Interfaces: All 35 exploits were unsuccessful.	Pass	Pass	Pass
5.9.1.5 Documentation	The configuration and setup to attain penetration resistance SHALL be clearly and completely documented	Documentation: Machine was preconfigured by manufacturer.	Documentation: Machine was preconfigured by manufacturer.	Pass	Pass	Pass
5.9.2 Penetration Resistance Test and Evaluation	High, Medium or Low	Medium	Medium	Medium	Medium	Medium
5.9.1.2 Scope	The scope of penetration testing SHALL include all the voting system components. The scope of penetration includes but is not limited to the following:	Scope: Using standard network exploitation tools, all machines and ports were identified.	Scope: Using standard network exploitation tools, all machines and ports were identified.	Pass	Pass	Pass
	System server;	Scope: Using standard network exploitation tools, all machines and ports were identified.	Scope: Using standard network exploitation tools, all machines and ports were identified.	Pass	Pass	Pass
	Vote capture devices;	Scope: Using standard network exploitation tools, all machines and ports were identified.	Scope: Using standard network exploitation tools, all machines and ports were identified.	Pass	Pass	Pass
	Tabulation device;	Scope: Using standard network exploitation tools, all machines and ports were identified.	Scope: Using standard network exploitation tools, all machines and ports were identified.	Pass	Pass	Pass
	All items setup and configured per Technical Data Package (TDP) recommendations;	Scope: Using standard network exploitation tools, all machines and ports were identified.	Scope: Using standard network exploitation tools, all machines and ports were identified.	Pass	Pass	Pass
	Local wired and wireless networks; and	Scope: Using standard network exploitation tools,	Scope: Using standard network exploitation tools,	Pass	Pass	Pass

5.9 Penetration Resistance	Requirement Matrix	VSTL System 1	VSTL System 2	AFIT System 1	AFIT System 2	AFIT System 3
		all machines and ports were identified.	all machines and ports were identified.			
	Internet connections.	Scope: Using standard network exploitation tools, all machines and ports were identified.	Scope: Using standard network exploitation tools, all machines and ports were identified.	Pass	Pass	Pass
5.9.2.2 Test Environment	Penetration testing SHALL be conducted on a voting system set up in a controlled lab environment. Setup and configuration SHALL be conducted in accordance with the TDP, and SHALL replicate the real world environment in which the voting system will be used.	Test Environment: Machines were installed on internal VSTL network.	Test Environment: Machines were installed on internal VSTL network.	Pass	Pass	Pass
5.9.2.3 White Box Testing	The penetration testing team SHALL conduct white box testing using manufacturer supplied documentation and voting system architecture information. Documentation includes the TDP and user documentation. The testing team SHALL have access to any relevant information regarding the voting system configuration. This includes, but is not limited to, network layout and Internet Protocol addresses for system devices and components. The testing team SHALL be provided any source code included in the TDP.	White Box Testing: Vendor documentation was reviewed but no vendor source code was tested. (The voting system vendors were not asked to supply a source code for review. This section is here because it is a requirement for PenTesting)	White Box Testing: Vendor documentation was reviewed but no vendor source code was tested. (The voting system vendors were not asked to supply a source code for review. This section is here because it is a requirement for PenTesting)	Not tested by AFIT/RedPhone	Not tested by AFIT/RedPhone	Not tested by AFIT/RedPhone
5.9.2.4 Focus and Priorities	Penetration testing seeks out vulnerabilities in the voting system that might be used to change the outcome of an election, interfere with voter ability to cast ballots, ballot counting, or compromise ballot secrecy. The penetration testing team SHALL prioritize testing efforts based on the following:	Focus and Priorities: Using standard network exploitation tools, all machines and ports were identified. 35 exploits were attempted with no success.	Focus and Priorities: Using standard network exploitation tools, all machines and ports were identified. 35 exploits were attempted with no success.	Pass	Pass	Pass
	a. Threat scenarios for the	Focus and Priorities: Using	Focus and Priorities: Using	Pass	Pass	Pass

5.9 Penetration Resistance	Requirement Matrix	VSTL System 1	VSTL System 2	AFIT System 1	AFIT System 2	AFIT System 3
	voting system under investigation;	standard network exploitation tools, all machines and ports were identified. 35 exploits were attempted with no success.	standard network exploitation tools, all machines and ports were identified. 35 exploits were attempted with no success.			
	b. Remote attacks SHALL be prioritized over in-person attacks;	Focus and Priorities: Using standard network exploitation tools, all machines and ports were identified. 35 exploits were attempted with no success.	Focus and Priorities: Using standard network exploitation tools, all machines and ports were identified. 35 exploits were attempted with no success.	Pass	Pass	Pass
	c. Attacks with a large impact SHALL be prioritized over attacks with a more narrow impact; and	Focus and Priorities: Using standard network exploitation tools, all machines and ports were identified. 35 exploits were attempted with no success.	Focus and Priorities: Using standard network exploitation tools, all machines and ports were identified. 35 exploits were attempted with no success.	Pass	Pass	Pass
	d. Attacks that can change the outcome of an election SHALL be prioritized over attacks that compromise ballot secrecy or cause non-selective denial of service.	Focus and Priorities: Using standard network exploitation tools, all machines and ports were identified. 35 exploits were attempted with no success.	Focus and Priorities: Using standard network exploitation tools, all machines and ports were identified. 35 exploits were attempted with no success.	Pass	Pass	Pass

As Table 2 indicates, the systems tested by the VSTLs maintained an acceptable security posture throughout the PenTesting. The AFIT/RedPhone PenTesting showed similar results. White Box testing was not accomplished by the VSTLs because the voting system vendors were not required as part of their testing to provide a technical data package or submit their source code for review. White Box testing was not accomplished by AFIT/RedPhone for the same reasons.

The results from both the VSTL testing and the AFIT/RedPhone PenTesting suggest the tested voting systems have a good security posture against penetration. No successful penetrations of the systems led to any votes being changed, altered or deleted. This does not mean that manufacturers should be complacent in their security efforts. Each day new cyber threats emerge. A successful electronic voting system must have a very robust security plan and system vendors must continuously strive to improve their security posture throughout the life-cycle of the system.

FVAP continuously works to satisfy its legal mandates and recognizes that some computer science and security experts have strong concerns about security issues associated with online voting. In an effort to move forward and have constructive dialogue on this important topic, FVAP organized the UOCAVA Solutions Working Group (USWG), which brought together a broad cross-section of the election community for constructive discussion on the many associated issues and opportunities for online voting. USWG participants included FVAP, EAC, NIST and other federal agency representatives; voting technology vendors; state and local election officials; computer scientists; political scientists; usability and accessibility specialists; and voting advocates.

FVAP has undertaken three USWG meetings during the past year: August 2010 in Washington, DC prior to the USENIX (Advanced Computing Systems Association) Conference; March 2011 in Chicago prior to the Electronic Verification Network (EVN) workshop; and August 2011 in San Francisco prior to the USENIX Conference. The August 2011 meeting was convened to discuss options for fulfilling 2002 National Defense Authorization Act (NDAA) and the Military and Overseas Voter Empowerment (MOVE) Act of 2009 requirements which authorized FVAP electronic voting pilot programs to test the feasibility of new election technology, and mandated FVAP to carry out an electronic voting demonstration project in which a significant number of uniformed service members could cast ballots in a regularly scheduled election.[i]

The results from both the May 2011 VSTL PenTesting and the August 2011 AFIT/RedPhone PenTesting suggest that the tested online voting systems have the necessary security elements with regard to penetration. There were *no* successful penetrations of any vendor systems that resulted in any vote being changed, altered or deleted. This was a basic computer security expert concern at the USWG meetings and was averted through the AFIT/RedPhone PenTesting exercise.

This does not mean that the tested systems are perfect or that security expert concerns about online voting by are unfounded. However, it does mean the current online voting systems provide a good basis for benchmarking and that more widespread and advanced testing and analysis should be undertaken—in a phased and careful manner—which should include integral and interested members of the election community.

[i] For specific information, please go to: http://www.justice.gov/opa/pr/2010/October/10-crt-1212.html.

5 Recommendations

One of the purposes of the AFIT/RedPhone testing and the VSTL tests mentioned earlier was to determine if the UPPTR requirements are sufficient as written or are in need of revision. Recommended changes to the requirements are shown in Table 4 below. These recommended changes will help voting system manufacturers, the VSTLs, and the EAC to improve online voting system security for systems used in the United States.

Table 4. Recommended Changes to the UPPTR Security Requirements

Section 5.9 UPPTR Requirements	Recommended Changes
5.9.1.1 "The voting system SHALL be resistant to attempts to penetrate the system by any remote unauthorized entity".	Define resistance levels more definitively, utilizing appropriate NIST Special Publication (NIST SP) and by device types and environments within a voting system.
5.9.1.2 "The voting system SHALL be configured to minimize ports, responses and information disclosure about the system while still providing appropriate functionality."	Define "appropriate functionality" by device types and environments within a voting system. Recommend referencing a NIST SP dealing with hardening.
5.9.1.4 "All interfaces SHALL be penetration resistant including TCP/IP, wireless, and modems from any point in the system."	Close all ports and shut down all services not needed to perform voting activities.
5.9.2 "Penetration Resistance Test and Evaluation"	This section is oriented toward the VSTL, not the manufacturer. Manufacturers should not be held to the requirement to put in a "Program Manual" that outlines the certification campaign scope.
5.9.2.2 "Penetration testing SHALL be conducted on a voting system set up in a controlled lab environment. Setup and configuration SHALL be conducted in accordance with the TDP, and SHALL replicate the real world environment in which the voting system will be used."	Requirement is oriented toward the VSTL, not the manufacturer. Manufacturers should not be held to the requirement to put in a "Program Manual" that outlines the certification campaign scope. Some systems are cloud-based, which will be challenging to set up in a controlled lab environment.
5.9.2.3 "The penetration testing team SHALL conduct white box testing using manufacturer supplied documentation and voting system architecture information. Documentation includes the TDP and user documentation. The testing team SHALL have access to any relevant information regarding the voting system configuration. This includes, but is not limited to, network layout and Internet Protocol addresses for system devices and components. The testing team	Requirement is oriented toward the VSTL, not the manufacturer. Manufacturers should not be held to the requirement to put in a "Program Manual" that outlines the certification campaign scope. Some systems are cloud-based, which will be challenging to set up in a controlled lab environment.

SHALL be provided any source code included in the TDP."	
5.9.2.4 "Penetration testing seeks out vulnerabilities in the voting system that might be used to change the outcome of an election, interfere with voter ability to cast ballots, ballot counting, or compromise ballot secrecy. The penetration testing team SHALL prioritize testing efforts based on the following:	Requirement is oriented toward the VSTL, not the manufacturer. Manufacturers should not be held to the requirement to put in a "Program Manual" that outlines the certification campaign scope. Some systems are cloud-based, which will be challenging to set up in a controlled lab environment.
5.9.2.4.a "Threat scenarios for the voting system under investigation;	Requirement is oriented toward the VSTL, not the manufacturer. Manufacturers should not be held to the requirement to put in a "Program Manual" that outlines the certification campaign scope. Some systems are cloud-based, which will be challenging to set up in a controlled lab environment.
5.9.2.4.b "Remote attacks SHALL be prioritized over in-person attacks;	Requirement is oriented toward the VSTL, not the manufacturer. Manufacturers should not be held to the requirement to put in a "Program Manual" that outlines the certification campaign scope. Some systems are cloud-based, which will be challenging to set up in a controlled lab environment.
5.9.2.4.c "Attacks with a large impact SHALL be prioritized over attacks with a more narrow impact; and	Requirement is oriented toward the VSTL, not the manufacturer. Manufacturers should not be held to the requirement to put in a "Program Manual" that outlines the certification campaign scope. Some systems are cloud-based, which will be challenging to set up in a controlled lab environment.
5.9.2.4. d "Attacks that can change the outcome of an election SHALL be prioritized over attacks that compromise ballot secrecy or cause non-selective denial of service."	Requirement is oriented toward the VSTL, not the manufacturer. Manufacturers should not be held to the requirement to put in a "Program Manual" that outlines the certification campaign scope. Some systems are cloud-based, which will be challenging to set up in a controlled lab environment.

Most changes above recommend developing a "Program Manual" for VSTL use. This manual would provide guidance to the VSTLs on how the requirements should be set up and tested in a lab environment. The current UPPTR requirements do not tell the manufacturer how to build a system, but rather how the VSTL should organize and prioritize the testing effort. For example, UPPTR requirement 5.9.2.4 has nothing to do with the manufacturer; however, it does tell the VSTL that they SHALL prioritize testing based on certain criteria. The manufacturer should have the required security in place to avoid being penetrated, but the manufacturer should not be held to a standard designed to help the VSTLs conduct a PenTest.

In general, cyber security best practices use mitigation strategies based on a balanced combination of people, operations/processes, and technology. (See page 79 of the U.S. General Accounting Office's (GAO's) *Cybersecurity for Critical Infrastructure Protection* report at http://www.gao.gov/new.items/d04321.pdf as just one example of this concept.)

- "People" include the appropriate training, background investigations, clearances, recruitment and retention programs, and incentives.
- "Operations/processes" include written, current, maintained, and management-supported policies and procedures proliferated throughout the organization, as appropriate, so they are vetted and well understood by all involved. Contingency plans and continuity of operations plans also are in this category.
- "Technology" includes software, hardware, telecommunications, anti-malware and alternate paths.

These three dimensions (people, operations/processes, and technology) work together to **prevent** unauthorized confidentiality, integrity, and/or availability degradation; **detect** such degradation when it occurs; and **correct** problems quickly and effectively. At the highest levels, these are basic components of a strong cyber security program. To build such a strong cyber security program, a path forward must be outlined and followed.

The USWG will be presented with the findings of the VSTL testing as well as the AFIT/RedPhone PenTesting. The USWG may recommend some additional testing or perhaps the design of a scientific experiment dealing with the security of online voting systems. The USWG may provide the FVAP Director with some ideas for moving forward with testing online voting security, as well as recommendations on how the industry should work toward the goal of continuous improvement in online voting system security.

The findings, and their importance, should be reviewed and analyzed by cyber security experts experienced in implementing strategies and tactics within government agencies to manage security risk. Such a group of cyber security experts has been formed for this explicit purpose. The Cyber Security Review Group (CSRG) was recruited from DoD, civilian, and intelligence community agencies (e.g., DHS, NSA, DIA, and FBI). This group meets regularly to discuss and analyze cyber security findings related to online voting, and to offer advice on how to reduce risks. This group will add value as an independent government body focused on this project.

FVAP initiated a series of tests that exercised the UPPTR and provided comparative data about the Voting System Test Laboratories (VSTLs). This testing should continue and include the development or validation of software assurance practices used by the voting system manufacturers. It should also include more extensive research into how the EAC developed the UPPTR and how each of the VSTLs interprets sections differently.

FVAP is mandated to produce an electronic voting demonstration project for uniformed UOCAVA voters. This system may potentially be used by UOCAVA voters stationed CONUS (Continental United States) and OCONUS (Outside the Continental United States) voters. It may also be used by forward deployed troops and those afloat. The development life cycle for such a system can take several years to develop, and the initial design and architecture of the system could be complicated. FVAP should

encourage commercial voting system vendors to design and develop a system for the demonstration project. The systems developed should then undergo testing by a VSTL to the UPPTR to ensure the system is compliant with all requirements. Extensive penetration testing that are both lab and operational (within the DOD environment of CONUS, OCONUS, ship board and hostile areas) based should be part of any testing done on the demonstration project system. The participating vendors in this PenTest exercise also fully support future PenTesting efforts by FVAP in an effort to continuously improve their systems.

The demonstration project will define the system; but FVAP must also define the target audience to use the system. FVAP should continue to collect data on the number of UOCAVA voters living abroad with emphasis on uniformed service personnel, as the demonstration project will use uniformed UOCAVA voters as participants. Knowing the number of voters expected to use the system will enable the designers to scale the project according to the participants expected. The designers of the demonstration project will need to know how best to build the system to accommodate the number of voters participating.

6 Conclusion

Online voting presents the opportunity for U.S. military service members and their dependents to vote in a timely, effective, and secure manner, regardless of where in the world they may be stationed. However, online voting presents unique security issues because it uses cyber space—computer systems and interconnected networks (such as the internet) to transmit votes.

Before online voting is used, the cyber security risks must be identified and addressed. PenTesting of online voting systems provides an opportunity to proactively identify the threats and address risks.

It is important to state that no penetration attempt was successfully executed. All of the online voting systems that were tested successfully thwarted all attacks posed by the professional RedPhone PenTest team and the trained AFIT students. It is also important to note that this was a modified penetration test, as the time limit was set to 72 hours and no source code review of the vendor's code was conducted. These conditions eliminated any White Box testing from occurring.

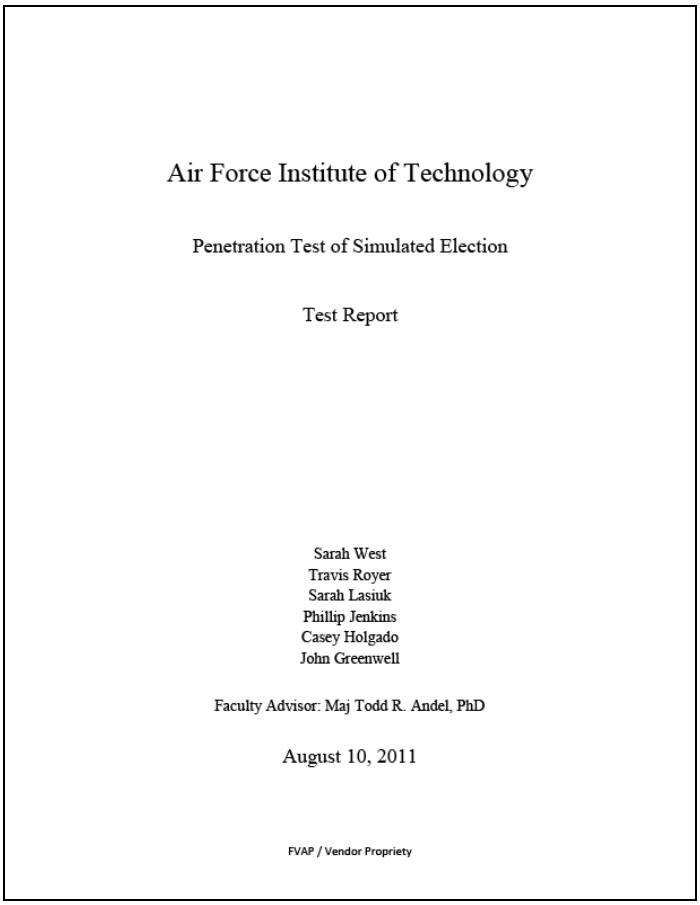
This PenTesting exercise did surface both high and low risk issues, as well as some informational concerns. Each issue and concern may need further analysis as circumstances change. Vendors providing online voting systems should apply best security practices to their systems; including full certification and accreditation (C&A) based on government C&A guidance (see NIST and US DoD guidance). Such a C&A requires a formal risk analysis and remediation schedule that is formally tracked by knowledgeable security professionals. Current C&A guidelines require "continuous monitoring" to ensure systems remain at the acceptable security level.

Additionally, PenTests such as the one conducted by AFIT/RedPhone should be undertaken periodically, as online voting systems and attack methods continue to evolve. All of the vendors who participated in this PenTesting exercise fully support this position. Initially, one PenTest should be conducted annually, with increased frequency as time and resources allow, and with an increasing scope. For example, the AFIT/RedPhone PenTest attack lasted only 72 hours (three days). An attack lasting a full week (24/7) should be conducted in the future. Also, a Denial of Service (DoS) attack was not authorized for this particular PenTest. In a real attack scenario, hackers would most certainly launch a DoS attack – if simply to demonstrate that they can succeed in bringing down a system's capability. A DoS attack should be a part of the next PenTest.

Finally, and most importantly, all findings in this, and subsequent PenTests, as well as findings from other types of security analyses, should be addressed, and any risks reduced to acceptable levels by applying the recommendations stated in this report. The AFIT/RedPhone PenTesting exercise was a good first step in demonstrating the security of online voting systems—its strengths and its opportunities for improvement—with qualitative and quantifiable data that will be reviewed at the next USWG meeting, which is yet to be scheduled.

Appendix A: AFIT Report

To access the AFIT report in PDF format, double-click on the icon below.



Air Force Institute of Technology

Penetration Test of Simulated Election

Test Report

Sarah West
Travis Royer
Sarah Lasiuk
Phillip Jenkins
Casey Holgado
John Greenwell

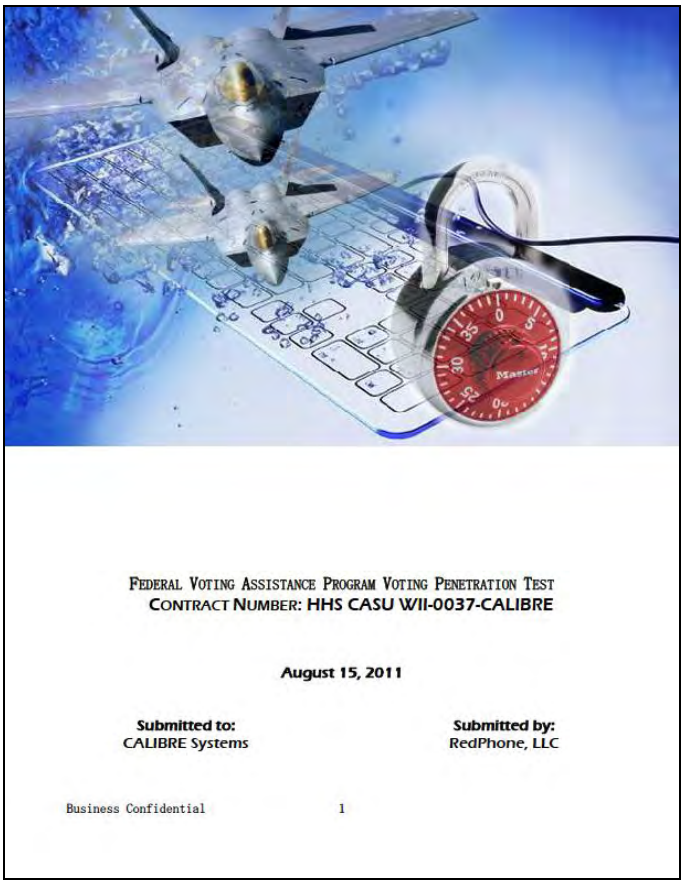
Faculty Advisor: Maj Todd R. Andel, PhD

August 10, 2011

FVAP / Vendor Propriety

Appendix B: RedPhone Report

To access the RedPhone report in PDF format, double click on the icon below.



FEDERAL VOTING ASSISTANCE PROGRAM VOTING PENETRATION TEST
CONTRACT NUMBER: HHS CASU WII-0037-CALIBRE

August 15, 2011

Submitted to:
CALIBRE Systems

Submitted by:
RedPhone, LLC

Business Confidential 1

Appendix C: Security Gap Analysis of UOCAVA Pilot Program Testing Requirements

To access the Security Gap Analysis of UOCAVA Pilot Program Testing Requirements report in PDF format, double-click on the icon below.

Adobe Acrobat Document

Appendix A

Air Force Institute of Technology

Penetration Test of Simulated Election

Test Report

Sarah West
Travis Royer
Sarah Lasiuk
Phillip Jenkins
Casey Holgado
John Greenwell

Faculty Advisor: Maj Todd R. Andel, PhD

August 10, 2011

[redacted]

Table of Contents

[redacted]

Executive Summary

This document summarizes the results of a penetration test done by six Air Force ROTC students interning at the Air Force Institute of Technology (AFIT). We conducted this test to help assist the Federal Voting Assistance Program (FVAP). One of FVAP's primary goals is to ensure that overseas active duty uniformed service members and their families may participate in their right to vote overseas through absentee ballots. One of FVAP's goals is to develop a method of voting entirely online, using personal computers. FVAP initiated an effort to test these systems through conducting multiple penetration tests on three different vendors' online voting systems; these vendors are (*to protect the privacy of the vendors, they will be named only as*) Vendor-1, Vendor-2, and Vendor-3. A simulated election was run for a 72 hour-period between August 2-4, 2011. Our goal was to identify and explore any vulnerabilities present within the system and to exploit as many of these vulnerabilities as possible, under certain rules of engagement. With this goal, we attacked the vendors' systems using a variety of methods, logged all of our actions and the results, and prepared them in Appendix A of this report.

The most notable vulnerability was an open Secure Shell (SSH) login prompt on one vendor's servers. Though identified, we were not able to crack it. A host of vulnerabilities were found and tampered with on the laptops simulating the voter machines, including our infiltration with personal administrator accounts. We did not personally succeed in remotely compromising voter confidentiality. We discovered a wide range of information on the servers from NMap and Nessus scans, but none of which were dangerous to security. In the end, we tried many attack vectors, but were not particularly successful. We provided recommendations regarding improvements which can be made to security; but, having not made any prominent breaches in security, we conclude these voting systems to be quite well defended.

1. Assets of Value

The value of penetration testing lies in providing detailed security assessment on real life applications. We tested these voting systems to provide information regarding any potential vulnerabilities that could be present. This test was to establish a risk mitigation framework for any such vulnerabilities identified. In providing our assessments of these risks, we enable the vendors to correct any problems and eliminate vulnerabilities in their software. The process of penetration testing helps to maintain and improve the confidentiality, availability, and integrity of these systems and to determine the effectiveness of their individual security architecture.

2. Vulnerabilities

The most salient vulnerability that we identified was an open Secure Shell (SSH) login that was available on the Vendor-1 voting server. This is a prominent vulnerability because it was an open line to remotely log in to and gain control over the voting server. Anyone on the Internet could potentially connect to this open service.

Physical vulnerabilities abound; any personal voting machine may be tampered with. Each vendor provided a laptop for the simulated voting process. Due to the fact that the voting is not conducted on a well monitored kiosk station, the vendors cannot control the security of the machine on which a voter accesses their voting application via browser. All bets are off when it comes to the voter's machine; both remote threats and physical threats are present. There are no guarantees whatsoever that the voter's machine is free of malware such as rootkits or malicious

viruses. The primary vulnerability that exists in the case of an infected voter machine is that hackers may view the user's input and thereby compromise their confidentiality.

The voting servers hosted by the vendors were unlike the personal voting machines. Some vulnerabilities were identified with scanning software NMap and Nessus. We proved it possible to identify information about the vendor servers. Namely, we were able to scan the servers and identify certificate information, service detection, device type, Hypertext Transfer Protocol information, operating system, and trace route information. These results were not 100% certain, but possessed reasonable reliability. You may refer to Appendix A for each of the vendor's software vulnerabilities found through performing Nessus scans on each of the vendors voting servers.

3. Threats

The open SSH login vulnerability on the Vendor-1 voting server can be easily accessed by anyone connecting to the IP address ([redacted]) via PuTTY or other remote login software. A username and password is required, but with enough time an attacker can get around this by brute force. Programs such as Hydra may be used to continually brute force attack the username and password until a successful login is established. Social engineering is also a powerful means of obtaining usernames and passwords relatively easy if employees are untrained in operational security. We did not determine the username or password in our penetration test, and therefore were not able to remotely log in to the Vendor-1 server.

[redacted]

The largest threat that we exploited was the physical security of the machines on which the voters cast their votes. From the first hour of the penetration test we were able to have hands on access to the voting machines with no resistance. We were able to place our own administrator accounts on the machines as well as gather data as the voting systems Internet Protocol (IP) configurations and settings. We were personally able to look over the shoulders of voters and view who they had voted for, thereby compromising the confidentiality of their vote.

Like fore-mentioned as a vulnerability, the fact that the systems allow for remote voting via any Internet-accessible device. Such devices could have various types of malware loaded on it prior to voting, either knowingly or unknowingly, and the possibility of remote keylogging or manipulation of a compromised computer is present. Remote threats open the door to ignorance on the part of the voter. Alone in a windowless room, they may be completely unaware that their vote was observed, or that the attacker cut their connection at the last moment and denied them availability. We were not successful in exploiting any remote threats in any way.

The vulnerability shown by the information we were able to gather is a only an indirect threat. Threats such as this can be valuable to a hacker by informing him what exploits he should utilize. For example, knowing that the server is likely running a Linux kernel narrows the exploits that he will try. Likewise, the knowledge of particular certificates could make a hacker privy to software that may be exploitable. He may also use some of this information in a social engineering attack, i.e. by pretending to be a hardware technician.

4. Impacts/Consequences

An open SSH line would allow a malicious individual command line control over the server. Here, he could explore, change, delete, intercept, download files, upload viruses, and more. He is limited by little more than the rights of the account to which he is logged on (which can be further compromised), his imagination, and his personal skill set once he gains this kind of access. Such exploitation would be a massive compromise of the system's integrity.

If one vote can never be fully secure from being modified, the system does not possess perfect integrity. There are multiple ways integrity of these systems could be potentially compromised. The fact that the voting machine is unsecured could create a devastating impact on the confidentiality of a person's vote for the election. An attacker could load a piece of malware onto a voter's machine that would record how they voted and return the information to the attacker. This could be done remotely on a compromised machine by viewing through a Virtual Network Connection (VNC) window. A second impact using VNC would be that the attacker could take control of the voter's system after the voter logs in. Doing this would allow the attacker to use the voter's session to vote for whoever the attacker wants to win the election.

The impact of the leveraged information collected through scans is proportional to the impact of the exploit. This is wide and varied. By itself, the knowledge that a server is running certain software has little to no impact at all. It all depends on how the information is coupled with exploitation techniques such as hacking attempts and social engineering.

5. Risk Level

We categorize the open SSH server as a *medium* risk. A remote login to the server is a powerful exploitation opportunity for a malicious individual. However, brute forcing a password alone is a task which takes a considerable amount of time, let alone being unaware of both the username and the password. Yet social engineering vectors exist and the SSH command shell is a sumptuous feast for a hacker.

We categorize the threat of remote or physical voting machine exploitation as a *medium* risk. A possible impact of this threat is that an attacker could place malware onto the voter's machine that would compromise the confidentiality of their vote. The risk level for this is noteworthy, considering the fact that many users do not update their computers or keep them completely secure. The voting application uses a Hypertext Transfer Protocol Secure (HTTPS) connection that offers protection from the vote data being sniffed, however an attacker can simply view the vote from a VNC shell on the local host as it is taking place. A second consequence was also noted, stating that an attacker could take control the voter's session once they log in, allowing the attacker to vote for who they want to win or denying the right for the voter to cast their legal vote. Even though this would be an easy task for an attacker to do, they may opt not to use it due to the fact that it would be visibly obvious when it happens and the election results would probably be voided. Compromising an insecure system is a fairly easy task, and there is no way of enforcing the user to make sure that their computer is secure prior to voting. Although we were not able to successfully compromise the vendor's systems, these possibilities are always a threat. No vote over such open networks can have complete confidentiality, but public eyes expect 100% and view any loss as calamitous.

We categorize information gained through scanning as a *low* risk. This information is by no means privileged and carries little weight on its own. The knowledge it provides is small in comparison to the working knowledge required for high-risk exploitations.

6. Recommended Controls

We recommend the immediate removal of the SSH login available on the Vendor-1 voting server. If it is necessary that it remain open, the password and username should be frequently changed. Furthermore, the rights provided in the command shell should be as low as possible required to meet its purpose.

Complete security on the voter's machine is not possible. However, as the voter is beginning the process, prior to entering their confidential information, they should be instructed on steps that they may take to ensure immunity to common threats. We recommend the delivery of flags and warnings should the voting client detect that the user lacks antivirus or antispyware programs. Voters' worries can be further calmed by accessibility to the vendor's help and technical support lines where they can be directed to methods of removing malware. It may also be wise to limit the amount of time a voter may be logged in to the voter application to reduce the chance of exploitation.

If possible, it would be wise to limit the information accessible by NMap and Nessus scans. The less a hacker can determine through scans, the less vulnerable the voting servers are. In fact, the vendors may use deception; by this, they may not only dissuade attackers, but divert them into dead ends. Thus, informational scans can be used as a reverse means against potential attackers.

7. Conclusion

In conclusion, we found the vendors Vendor-1, Vendor-2, and Vendor-3 to be admirably secure. Though vulnerabilities were identified in our test, we were unsuccessful in our attempts to exploit and did not achieve compromised systems. Within this report we specified the value of the three voting system vendors on both their confidentiality as well as integrity of each system. We identified low and medium level securities including an open SSH line and information about the machines running the systems. We discovered these threats by conducting reconnaissance and gaining physical access to the three vendor's end kiosk clients, and we elaborated on their impact in this document. Lastly, we suggested recommended controls on these systems such as limiting the amount of time on the servers and possibly the amount of information available on scanning tools open to the public such as Nessus and NMap. The logs of our attacks and scans are shown below in Appendix A and B, respectively.

Appendix A

Penetration Test Time Log

Vendor-3 Time Log			
Date: 8/2/2011			
Time	Action	Outcome	Team Member
815	Placed vote on voting workstation	Gather details on how voting process works	A
820	Placed vote on voting workstation	Gather details on how voting process works	C
820	Explored target workstations and retrieved the IP addresses of the targeted internal voting workstation	Internal IP Address [redacted]	D
820	Attempted to establish a new user account on the target workstation	Unsuccessful at creating a new user	D
830	Used command *ipconfig*in command prompt of voting workstation to obtain IP address of target computer	Internal IP Address [redacted]	A
830	Created account on voting workstation with administrative access	User Name: Support ; Password: H01GaD0	B
830	Placed vote on voting workstation	Gather details on how voting process works	B
830	Logged internal IP address of voting workstations	Internal IP Address: [redacted]	B
845	Scanned the internal voting workstation at [redacted] using Nessus		D
848	Scanned the external vendor web server at [redacted] using Nessus	See Appendix B for report of vulnerabilities	D
852	Ran internal scan on [redacted] using Nessus		A
900	Retrieved voting system web address	https:// [redacted]	A
900	Used command *ping* [redacted] in command prompt to verify communication with target internal voting workstation	Successful response and verification of communication established	B
913	Scanned the internal voting workstation at [redacted] using Nmap		E
919	Downloaded PsTools for Windows and ran the command *psexec* \\ [redacted] *Support cmd*in command prompt of each internal IP address	Connection failed and was unable to connect to desired destination	A
920	Started Cain	Found a workgroup called VENDOR-3_INT with one XP computer named COMP023	C

[redacted]

930	Used command prompt to ping URL https:// [redacted]	Discovered the IP address of voting system server which is [redacted]	B
935	Ran the command *mstsc*in command prompt	Unable to connect to and establish a remote desktop on [redacted]	A
958	Ran a PHP meterpreter, Reverse TCP Incline exploit in Metasploit on internal voting workstation	Unable to exploit target	D
1000	Ran external scan on [redacted] using Nessus		A
1000	Attempted to establish connection to internal voting workstation using the command *windows/smb/psexec/reverse_tcp* in Metasploit	Failed to establish a connection	B
1000	Ran a PHP meterpreter, Reverse TCP Sager exploit in Metasploit on internal voting workstation	Unable to exploit target	D
1010	Ran a multi/handler SSL exploit with payload of meterpreter_reverse_TCP in Metasploit on internal voting workstation	Unable to exploit target	D
1030	Ran internal scan on [redacted] using Nessus	Low vulnerabilities reported	B
1030	Ran a vlc_smb_url msf exploit with payload of meterpreter_reverse_TCP in Metasploit on internal voting workstation	Unable to exploit target	D
1045	started intense, all tcp on Vendor-3 laptop	was interrupted	F
1100	Ran scan on internal IP address [redacted] using Nmap		A
1100	Scanned the voting system URL using Sitedigger	No Vulnerabilities found	B
1125	Ran a slow internal scan on the internal workstation IP [redacted] using Nmap	See Appendix B for results	E
1130	Scanned [redacted] using an intense scan with Nmap		B
1300	Ran an external scan on the voting system website server using Nessus	No Vulnerabilities found	B
1302	tried to visit Vendor-3.com	failed-timed out	F
1305	Used Maltego and began running all transforms on Vendor-3.com	results gathered; no salient breakthroughs	F
1316	started nmap -T4 -A -v -PN [redacted] Vendor-3.com	started	F
1320	nMap completed	results saved, some interesting data, few conclusive, no breakthroughs	F
1330	Ran a SQL injection scan on voting system website using Webcruiser		B

[redacted]

1330	Used Blackwidow and Foca tools in order to crawl the vendor website and look for additional vulnerabilities		C
1400	Completed SQL injection scan on voting system website using Webcruiser	No Vulnerabilities found	B
1406	Attempted to scan range of IP addresses for network which the voting system web server is located [redacted] using Nmap	Scan never completed	E
1430	Ran scan on web server [redacted] using Nmap		B
1449	Scanned the external IP [redacted] using Nessus	No Vulnerabilities found	E
1500	Completed scan on web server [redacted] using Nmap	Discovered that the Vendor-3 system is running Windows	B
1505	Scanned the external IP [redacted] using Nessus	See Appendix A for results	E

Date: 8/3/2011

Time	Action	Outcome	Team Member
900	Manually changed settings on voting workstation to allow remote desktop connection and added the user "Support" to list of users that may access it		A
951	Attempted to ping internal workstation IP [redacted] using the command prompt	No response to ping	E
935	sent fake email to Vendor-3@Vendor-3.com as jason mulbrich, attempted to gain insight into workforce for social engineering	sent; no reply ever received	F
950	sent fake email to [redacted]@Vendor-3.com as "MS Outlook"	failed	F
958	Attempted to ping internal workstation IP [redacted] using the command prompt	No response to ping	E
1000	Attempted to remote desktop into voting workstation	Unsuccessful connection	A
1000	Attempted to ping the internal voting workstation IP [redacted] using the command prompt	No response from the target IP address	A
1000	Ran intense scan on the internal voting workstation IP [redacted] using Nmap		B
1013	Attempted to ping the internal voting workstation IP [redacted] using the command prompt	Response back from targeted IP	E
1030	Ran scan on the internal voting workstation IP [redacted] using Nessus		B
1300	Ran scan on the internal voting workstation IP [redacted] using Armitage		B

[redacted]

1322	sqlite3 db_nmap scan of Vendor-3 laptop in BT4	completed in 40s, results gathered as before	F
1323	db_autopwn -p -t -e of Vendor-3 laptop	completed in 6seconds no sessions	F
1400	Ran Hail Mary exploit on the internal voting workstation IP [redacted] using Armitage		B
1500	Scanned the external IP [redacted] using Nmap		B

Date: 8/4/2011

Time	Action	Outcome	Team Member
816	Scanned the internal voting workstation IP [redacted] using Nmap -p 1-65535 command on Nmap		B
826	Scanned the internal voting workstation IP [redacted] using Nmap -5T -A -v command on Nmap		B
1000	started nmap scan of Vendor-3 server, intence scan no ping except -T4 changed to -T2 for stealth	started	F
1002	prematurely stopped nessus scan of Vendor-3 server (started about 30 mins prior)	results gathered, 14 vulnerabilities 1 med 13 low	F
1030	nmap scan of Vendor-3 server done	results lost… zenmap crashed	F
1052	nmap scan of Vendor-3 server again, intense scan no ping -T2	started	F
1054	nmap scan of Vendor-3 server done	results saved	F

[redacted]

Vendor-1 Time Log			
Date: 8/2/2011			
Time	Action	Outcome	Team Member
815	Placed vote on voting workstation	Gather details on how voting process works	A
820	Placed vote on voting workstation	Gather details on how voting process works	C
820	Retrieved voting system web address	https:// [redacted]	C
820	Pinged URL to retrieve external IP address	Discovered the IP address of voting system server which is [redacted]	C
820	Explored target workstations and retrieved the IP addresses of the targeted internal voting workstation	Internal IP Address: [redacted]	D
820	Vendor-1 laptop voting server: attempt SQLI 'or''1'='1'*/ 'or''1'='1'{('or''1'='1'(/	invalid	F
820	Attempted to establish a new user account on the target workstation	Unsuccessful at creating a new user	D
830	Used command *ipconfig*in command prompt of voting workstation to obtain IP address of target computer	Internal IP Address: [redacted]	A
830	Created account on voting workstation with administrative access	User Name: Support ; Password: H01GaD0	B
830	Placed vote on voting workstation	Gather details on how voting process works	B
830	Logged internal IP address of voting workstations	Internal IP Address: [redacted]	B
850	Ran internal scan on [redacted] using Nessus		A
851	Pinged URL to retrieve external IP address	Discovered the IP address of voting system server which is [redacted]	D
855	Scanned the external vendor web server at [redacted] using Nessus	No Vulnerabilities found	D
900	Retrieved voting system web address	https:// [redacted]	A
900	Gathered URL for voting site	https:// [redacted]	B
900	Used command *ping* [redacted] in command prompt to verify communication with target internal voting workstation	Successful response and verification of communication established	B
900	Used command prompt to ping the URL https:// [redacted]	Discovered the IP address of voting system server which is [redacted]	B
900	Used PuTTY to connect to port 22 (SSH) on vendor web server	Received a prompt for login	D
919	Downloaded PsTools for Windows and ran the command *psexec* \\ [redacted] *-u Support cmd*in command prompt of each internal IP address	Connection failed and was unable to connect to desired destination	A

[redacted]

920	Went to http://testbed.Vendor-1.com/robots.txt in web browser	Browser displayed- user-agent: * Disallow: /	E
935	Ran the command *mstsc*in command prompt	Unable to connect to and establish a remote desktop on [redacted]	A
957	Ran a slow internal scan on the internal workstation IP [redacted] using Nmap	See Appendix B for results	E
958	Ran a web app scan on voting site using Nessus	No Vulnerabilities found	E
1000	Ran external scan on [redacted] using Nessus		A
1000	Attempted to establish connection to internal voting workstation using the command *windows/smb/psexec/reverse_tcp* in Metasploit	Failed to establish a connection	B
1000	Used autopwn consisting of over 100 exploits on the web server [redacted] in order to establish a connection	No successful connection made	C
1005	nessus scan against server complete	2 low vulnerabilities	F
1005	Lost connection with voting site		E
1030	Ran internal scan on [redacted] using Nessus	Low vulnerabilities reported	B
1040	Scanned the external web server IP [redacted] using Nmap	See Appendix B for results	D
1050	Scanned the external web server IP [redacted] using Nessus	See Appendix B for results	D
1100	Ran scan on internal IP address [redacted] using Nmap		A
1100	Scanned the voting system URL using Sitedigger	No Vulnerabilities found	B
1130	Scanned [redacted] using an intense scan with Nmap		B
1134	Scanned the internal voting workstation at IP [redacted] using Nessus		D
1300	Ran an external scan on the voting system website server using Nessus	No Vulnerabilities found	B
1330	Ran a SQL injection scan on voting system website using Webcruiser		B
1330	Used Blackwidow and Foca tools in order to crawl the vendor website and look for additional vulnerabilities		C
1400	Completed SQL injection scan on voting system website using Webcruiser	No Vulnerabilities found	B

[redacted]

1420	Discovered administrative login page for Vendor-1.com	The administrative directory was listed in robots.txt for the website; Login page was a website built with Joomla software; Noted webpage source code uses Joomla 1.5	C
1430	Ran scan on web server [redacted] using Nmap		B
1500	Completed scan on web server [redacted] using Nmap	Discovered that the Vendor-1 voting system is running Linux	B
1500	Attempted the Joomla 1.5 password reset token vulnerability on administrative login page	Failed attempt- website was patched to prevent this	C
1530	attempted metasploit psexec on EC laptop	no reply	F
1540	Ran a Joomla automated attack tool on the administrative login page	No Vulnerabilities found	C

Date: 8/3/2011			
Time	Action	Outcome	Team Member
850	Attempted to ping internal workstation IP [redacted] using the command prompt	No response to ping; Problem with laptop	E
900	Used Vendor-1.com/index.php?option=com_NAME to see if webpage returned a 404 error or blank page	only component found: com_jce	C
900	Found a vulnerability for the com_jce componentvia Exploit-DB	SQL injection failed- the vulnerability was patched; continued running Hydra remote bruteforce	C
908	Scanned the internal voting workstation IP [redacted] using stealthy scan in Nmap		D
1000	Ran intense scan on the internal voting workstation IP [redacted] using Nmap		B
1030	Ran scan on the internal voting workstation IP [redacted] using Nessus		B
1300	Ran scan on the internal voting wokstation IP [redacted] using Armitage		B
1400	Ran Hail Mary exploit on the internal voting workstation IP [redacted] using Armitage		B
1440	Remote SSH puTTY attempt into Vendor-1 server [redacted]	opened login screen, attempted root and five passwords; failure	F
1500	Scanned the external IP range [redacted] using Nmap		B

[redacted]

Date: 8/4/2011			
Time	Action	Outcome	Team Member
820	Scanned the internal voting workstation IP : [redacted] using Nmap -p 1-65535 command on Nmap		B

[redacted]

Vendor-2 Time Log			
Date: 8/2/2011			
Time	Action	Outcome	
815	Placed vote on voting workstation	Gather details on how voting process works	A
820	Placed vote on voting workstation	Gather details on how voting process works	C
820	Retrieved voting system web address	https:/ [redacted]	C
820	Pinged URL to retrieve external IP address	Discoved the IP address of voting system server which is [redacted]	C
820	Explored target workstations and retrieved the IP addresses of the targeted internal voting workstation	Internal IP Address: [redacted]	D
820	Attempted to establish a new user account on the target workstation	Unsuccessful at creating a new user	D
830	Used command *ipconfig*in command prompt of voting workstation to obtain IP address of target computer	Internal IP Address: [redacted]	A
830	Created account on voting workstation with administrative access	User Name: Support ; Password: H01GaD0	B
830	Placed vote on voting workstation	Gather details on how voting process works	B
830	Logged internal IP address of voting workstations	Internal IP Address: [redacted]	B
850	Ran external scan on [redacted] using Nessus	Had open ports: 22, 80, 443	C
850	Used PuTTY to try and connect to Port 22 (SSH) on [redacted]	Received Login Prompt	C
853	Ran internal scan on [redacted] using Nessus		A
900	Retrieved voting system web address	https:/ [redacted]	A
900	Used command *ping* [redacted] in command prompt to verify communication with target internal voting workstation	Successful response and verification of communication established	B
915	nessus scan run against Vendor-2 laptop, saved results	3 low vulnerabilites	0
900	Made basic login attempts within the login prompt received when connecting to Port 22 (SSH) on [redacted] with PuTTY: User Names- Admin, Administrator, root, user ; Passwords- blank, same input as username	No successful match	C
919	Downloaded PsTools for Windows and ran the command *psexec* \\ [redacted] *-u Support cmd*in command prompt of each internal IP address	Connection failed and was unable to connect to desired destination	A

[redacted]

930	Used Command promt to ping URL https:/ [redacted]	Discoved the IP address of voting system server which is [redacted]	B
935	Ran the command *mstsc*in command prompt	Unable to connect to and establish a remote desktop on [redacted]	A
940	Went to http:/ [redacted] in web browser	Discovered later that we wanted [redacted] instead of [redacted]	E
950	Began running Hydra to attempt to brute-force the Login dialog prompted wheb connecting to Port 22 (SSH) with PuTTY: Defined Usernames- Administrator, user, root ; Passwords- 1.7 million common passwords file	No successful match	C
1000	Ran external scan on [redacted] using Nessus		A
1000	Attempted to establish connection to internal voting workstation using the command *windows/smb/psexec/reverse_tcp* in Metasploit	Failed to establish a connection	B
1030	Ran internal scan on [redacted] using Nessus	Low vulnerabilities reported	B
1038	attempted BT5 psexec exploit on Vendor-2 laptop	failed-timed out	F
1044	Ran a slow internal scan on the internal workstation IP [redacted] using Nmap	See Appendix B for results	E
1053	Scanned the external web server IP [redacted] using Nessus	See Appendix B for results	D
1055	Scanned the external web server IP [redacted] using Nmap	See Appendix B for results	D
1100	Ran scan on internal IP address [redacted] using Nmap		A
1100	Scanned the voting system URL using Sitedigger	No Vulnerabilities found	B
1126	Ran exploit Windows/smb/ms09_050smb2 on internal voting workstation using Metasploit	Unable to exploit vulnerability	D
1130	Scanned [redacted] using an intense scan with Nmap		B
1135	Scanned the internal voting workstation at IP [redacted] using Nessus		D
1240	Pinged URL using command prompt to verify response from voting website	Successful response and verification of communication established	D
1300	Ran an external scan on the voting system website server using Nessus	No Vulnerabilities found	B
1312	Attempted to scan range of IP addresses for network which the voting system web server is located [redacted] using Nmap	Scan never completed	E

[redacted]

1330	Ran a SQL injection scan on voting system website using Webcruiser		B
1330	Used Blackwidow and Foca tools in order to crawl the vendor website and look for additional vulnerabilities		C
1400	Completed SQL injection scan on voting system website using Webcruiser	No Vulnerabilities found	B
1430	Ran scan on web server [redacted] using Nmap		B
1500	Completed scan on web server [redacted] using Nmap	Discovered that the Vendor-2 system is running Linux	B
1540	Scanned the external IP [redacted] using Nessus	See Appendix B for results	E
1544	Scanned the external IP [redacted] using Nessus	No Vulnerabilities found	E

Date: 8/3/2011			
Time	Action	Outcome	Team Member
1000	Ran intense scan on the internal voting workstation IP [redacted] using Nmap		B
845	Attempted to ping internal workstation IP [redacted] using the command prompt	No response to ping; Problem with laptop	E
958	Scanned the internal voting workstation IP [redacted] using Nmap		D
1030	Ran scan on the internal voting workstation IP [redacted] using Nessus		B
1300	Ran scan on the internal voting workstation IP [redacted] using Armitage		B
1400	Ran Hail Mary exploit on the internal voting workstation IP [redacted] using Armitage		B
1500	Scanned the external IP range [redacted] using intense scan in Nmap	No response to ping	B

Date: 8/4/2011			
Time	Action	Outcome	Team Member
820	Scanned the internal voting workstation IP [redacted] using Nmap -p 1-65535 command on Nmap		B

[redacted]

Appendix B

NMap Scans of Vendor Systems

Vendor-2 Internal Computer Nmap Scan

Nmap Scan Report- Scanned at Wed Aug 03 10:06:38 2011

Scan Summary [redacted]

Scan Summary

Nmap 5.51 was initiated at Wed Aug 03 10:06:38 2011 with these arguments:
nmap -T4 -A -v -PE -PS?2,25,80 -PA21,2;3,BQ, [redacted]

Verbosity: 1; Debug level 0

[redacted]

Address

[redacted] - (ipv4)

Ports

The 1000 ports scanned but not shown below are in state: filtered

Remote Operating System Detection

Used port: 43127/udp (closed)
OS match: Microsoft Windows Server 2006 (66%)
OS match: Microsoft Windows Server 2006 R2 (66%)
OS match: Microsoft Windows Server 2006 SP1 (66%)
OS match: Microsoft Windows Server 2006 SP2 (66%)
OS match: Microsoft Windows 7 (66%)
OS match: Microsoft Windows 7 Professional (88%)
OS match: Microsoft Windows 7 Ultimate (88%)
OS match: Microsoft Windows Longhorn (66%)
OS match: Microsoft Windows Vista (66%)
OS match: Microsoft Windows Vista Business (88%)

Traceroute Information (dick to expand)
Mise Metrics (dick to expand)

[redacted]

Vendor-2 ServerNmap Scan

Nmap Scan Report- Scanned at Wed Aug 03 14:25:49 2011

Scan Summary 1 [redacted]

Scan Summary

Nmap 5.51 was initiated at Wed Aug 03 14:25:49 2011 with these arguments:
nmap -T5 -A -v -Pn [redacted]

Verbosity: 1; Debug level 0

[redacted]

Address

[redacted] (ipv4)

Ports

The 1000 ports scanned but not shown below are in state: filtered

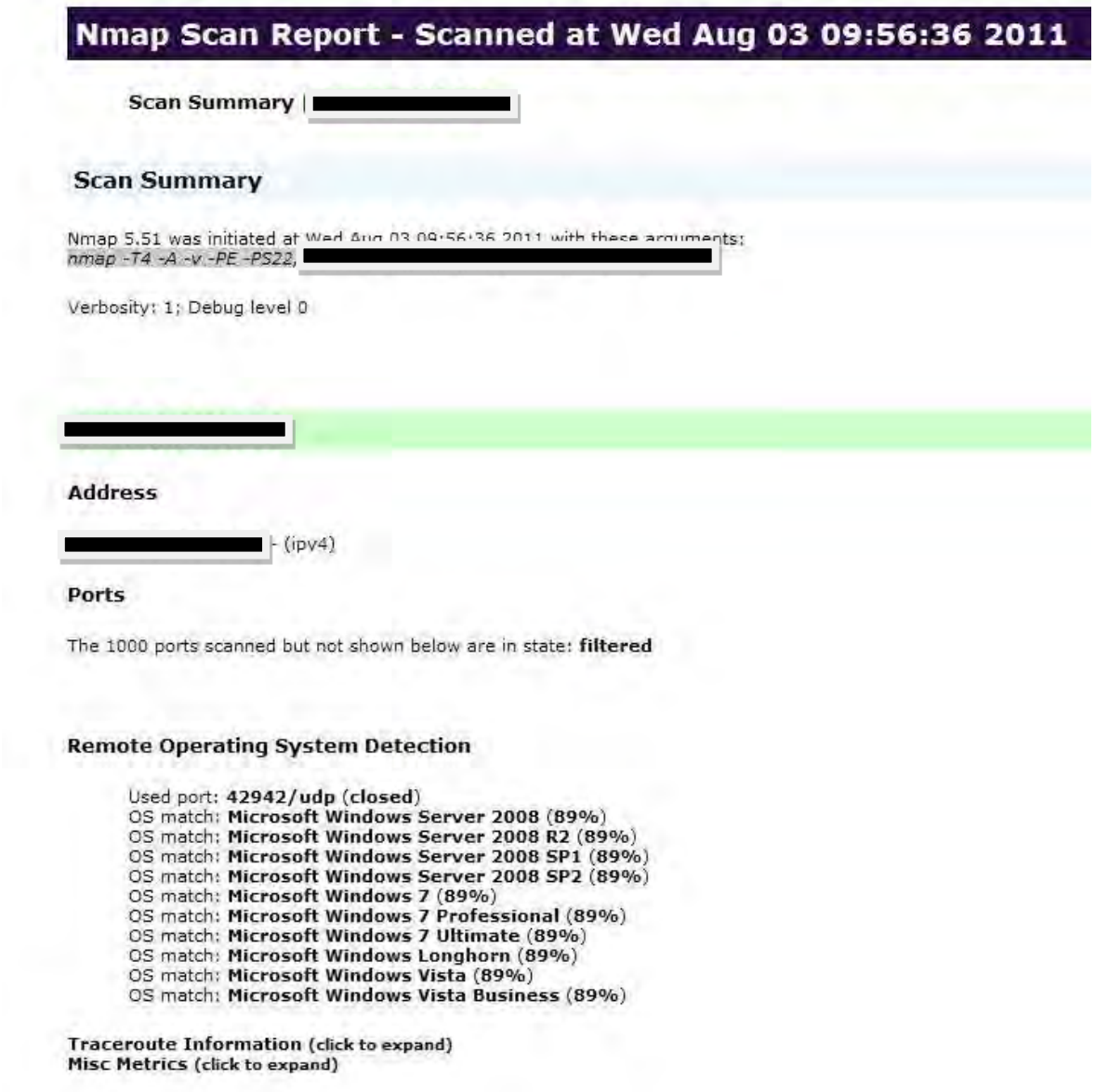
Remote Operating System Detection

Unable to identify operating system.

Traceroute Information (click to expand)
Mise Metrics (click to expand)

[redacted]

Vendor-1 Internal Computer Nmap Scan



Nmap Scan Report - Scanned at Wed Aug 03 09:56:36 2011

Scan Summary | [redacted]

Scan Summary

Nmap 5.51 was initiated at Wed Aug 03 09:56:36 2011 with these arguments:
nmap -T4 -A -v -PE -PS22, [redacted]

Verbosity: 1; Debug level 0

[redacted]

Address

[redacted] - (ipv4)

Ports

The 1000 ports scanned but not shown below are in state: **filtered**

Remote Operating System Detection

Used port: **42942/udp (closed)**
OS match: **Microsoft Windows Server 2008 (89%)**
OS match: **Microsoft Windows Server 2008 R2 (89%)**
OS match: **Microsoft Windows Server 2008 SP1 (89%)**
OS match: **Microsoft Windows Server 2008 SP2 (89%)**
OS match: **Microsoft Windows 7 (89%)**
OS match: **Microsoft Windows 7 Professional (89%)**
OS match: **Microsoft Windows 7 Ultimate (89%)**
OS match: **Microsoft Windows Longhorn (89%)**
OS match: **Microsoft Windows Vista (89%)**
OS match: **Microsoft Windows Vista Business (89%)**

Traceroute Information (click to expand)
Misc Metrics (click to expand)

[redacted]

Vendor-1 ServerNmap Scan

Nmap Scan Report- Scanned at Thu Aug 04 09:25:06 2011

Scan Summary) lwdcdbo2.fa1 34.host4 . 24396 [redacted]

Scan Summary

Nmap S.Sl was initiated at Thu Aug 04 09:25:06 2011 with the-se arguments:
P"l<<l> *:::Ii .:A·v·Pn* ZJQ.JJ/$.4lj

Verbcsity:1: Debug level 0

[redacted] / lwdc.dbo.2.fa1-34.host4.24396 [redacted]

Address

[redacted] - (ipv4)

Hostnzames

lwdc. .dbo2.fa1- 34.host4.24396 [redacted] (PTR)

Ports

The 999 ports scanned but not shown below *are* in state: fittered

State (togle dosed (0) I filtered (OJ)	Product
o n	Aj>ache httpd

Remote Operating System Detection

use<! port: 443/tcp (open)
OS match: Unux x.x.x- x.x.xx (94%)
OS match: Unux x.x.x- x.x.xx (92%)
OS match: Unux x.x.x - x.x.xx (89%)
OS match: Linux x.x.xx (ContOS 5, x86_64, SHP) (89%)
OS match: ZoneAiarm Z100G WAP (89%)
OS match: linux x.x.xx (CentOS 5.2) (88%)
OS metch: Unwc x.x.x- xxx.stabxxx.xx-enterpri.se (CentOS 4.2 x:86} (86%)
OS match: Unux x.x. xx - x.x.xx
(88%) OS match: Unux x.x.xx (88%)
OS match: Unux x.x.xx (Centos 5.3) (88%)

Traceroute Information (dick to expaod)
HIsc Metrics (dick to expand)

[redacted]

Vendor-3 Internal Computer Nmap Scan

Nmap Scan Report- Scanned at Wed Aug 03 10:12:33 2011

Scan Summary : [redacted]

Scan Summary

Nmap 5.51 was initiated at Wed Aug 03 10:12:33 2011 with these arguments:
oma R -T4 -A -v -PE -PSZ2 _ 80 -PA21.2J,S0,338 [redacted] -i!IO

Verbosity: 1; Debug level 0

[redacted]

Address

[redacted] - (ipv4)

Ports

The 1000 ports scanned but not shown below are in state: filtered

Remote Operating System Detection

Used port: 40114/udp (closed)
OS match: Microsoft Windows Server 2008 (89%)
OS match: Microsoft Windows Server 2008 R2 (89%)
OS match: Microsoft Windows Server 2008 SP1 (89%)
OS match: Microsoft Windows Server 2008 SP2 (89%)
OS match: Microsoft Windows 7 (89%)
OS match: Microsoft Windows 7 Professional (89%)
OS match: Microsoft Windows 7 Ultimate (89%)
OS match: Microsoft Windows longhorn (89%)
OS match: Microsoft Windows Vista (89%)
OS match: Microsoft Windows Vista Business (89%)

Traceroute Information (dick to expand)
Mise Metrics (dick to expand)

[redacted]

Vendor-3 ServerNmap Scan

Nmap Scan Report- Scanned at Wed Aug 03 14:28:30 2011

Scan Summary 1 [redacted]

Scan Summary

Nmap 5.51 was initiated at Wed Aug 03 14:28:30 2011 with these arguments:
nmap -T5 -A -v -Pn [redacted]

Verbosity: 1; Debug level 0

[redacted]

Address

[redacted] (ipv4)

Ports

The 999 ports scanned but not shown below are in state: filtered

State (toggle dosed (0]1 filtered (OJ)
open

Remote Operating System Detection

Used port: 443/tcp (open)
OS match: HP 170X print server or Inkjet 3000 printer (94%)
OS match: Crestron XPanel control system (900/o)
OS match: Netgear OG834G WAP (90%)
OS match: Nintendo Wii game console (860/o)
OS match: VodaviXTS-IP PBX (86%)
OS match: Brother MFC-7620N multifunction printer (65%)
OS match: Microsoft Xbox game console {modified, running XboxMediaCenter) (SSOJo)
OS match: Hirschmann L2E Railswitch (85%)

Traceroute nformation (dick to expand)
Mise Metrics (click to expand)

[redacted]

Nessus Scans of Vendor Servers

1. Vendor-2 System Server:

[redacted]

1.1 Port 0- TCP

1.2. Port 0- UDP

[redacted]

2. Vendor-1 Server:

[redacted]

2.1. Port 0- TCP

2.2. Port 0- UPD

[redacted]

2.3 Port 80- TCP

2.4. Port 443- TCP

[redacted]

3. Vendor-3 Server:

3.1. Port 0 – TCP

3.2. Port 0- UDP

3.3. Port 21-TCP

3.4. Port 25- TCP

3.5. Port 53- TCP

[redacted]

3.6. Port 443- TCP

3.7. Port 993- TCP

[redacted]

3.8. Port 5432- TCP

Appendix B

FEDERAL VOTING ASSISTANCE PROGRAM VOTING PENETRATION TEST

CONTRACT NUMBER: HHS CASU WII-0037-CALIBRE

August 15, 2011

Submitted to:
CALIBRE Systems

Submitted by:
RedPhone, LLC

[redacted]

POINT OF CONTACT: L. Jay Aceto, CISSP, ISSAP/MP, CISM, NSA-IAM/IEM

Telephone: 571-334-9225 • E-mail Address: jay.aceto@redphonecorporation.com

Table of Contents

Document Properties
Title: Multi-Vendor Mock Voting Exercise - Operation Orange Black Box Penetration Testing Report
Version V1.0
Author L. Jay Aceto CISSP, CISM, ISSAP/MP, NSA-IAM/IEM
Technical Review: TC McFall
Peer Review: Josha Richards, Aaron Bossert, Michael Carter
RedPhone Penetration testers: TC McFall, L. Jay Aceto

Version control
Version : 1.0
Date : August 15, 2011

Executive Summary

The democratic process rests on a fair, universally accessible, anonymous voting system through which all citizens can easily and accurately cast their vote. At present, over 6,000,000 voters reside outside the United States and rely on traditional paper-based registration and voting processes that are inadequate at meeting their needs, and fraught with inherent delays. The main issues revolve around the inherent latency with the registration, receipt, and delivery of ballots by traditional mail. The Federal Voting Assistance Program (FVAP), a United States Department of Defense (DoD) controlled program, has been systematically gathering, analyzing, and reporting on the voter's experience, and exploring new technologies to improve the delivery of registration and ballot materials.

RedPhone, LLC., a Virginia-based information assurance and security consultancy to the U.S. DoD, civilian, and state governments, as well as commercial enterprises, was contracted to provide penetration testing services to CALIBRE Systems in support of the FVAP to test and evaluate the security of three Internet voting systems. The penetration test team was led by CALIBRE Management, however, the primary responsibility for the testing and analysis resided with RedPhone, LLC. Additionally, RedPhone, LLC. prepared the testing scenario and the rules of engagement that the Air Force Institute of Technology (AFIT) and other outside penetration testing teams would use to determine the scope and boundaries of the engagement. The fictitious *Operation Orange* exercise and the rules of engagement are listed within the appendices.

Beginning in May of 2011, and culminating in the actual penetration testing and mock election exercise that spanned 72 hours from August 2-4, 2011, all three participating vendors' systems were carefully evaluated for their security posture, defensive capabilities, critical logging and security architecture limitations. Historically, the application development processes associated with these critical applications have not followed industry best practices. This flawed state is the result of undisciplined software development, and a process that failed to encourage developers to anticipate or fix security holes. The closed-source approach to software development, which shielded the source code from public review and comment, only served to delay the necessary scrutiny. However, all three vendors have been highly supportive of these tests, and it is obvious that they have made great strides to improve the security posture of their respective products. Six independent technical security experts with an extensive background in web application security and information assurance were charged with attempting to breach the security of each of the three participating vendors. Two AFIT cyber security teams were also participating in the penetration testing process. This

report is the culmination of the penetration test team's findings, potential mitigations, and recommendations.

Penetration testing typically falls into the following three categories: "White box" testing is performed with the full knowledge and support of the vendor, and the vendor provides unlimited access to the software, supporting documentation and staff. "Grey box" testing is a partial knowledge test scenario where the test team has only limited knowledge of the vendor's products and services, and the rest must be obtained via research. In "black box" testing, the test teams are given very little if any advanced knowledge of the vendor's products, and therefore, must gain as much knowledge as possible independently in a discovery and reconnaissance effort. The penetration test team for this exercise used a "black box" approach, wherein little information is provided from the vendors, and only a brief window is available to research each vendor to prepare an attack strategy.

Although the penetration test teams designed various attacks, they generally fell into one of five categories:

1. vote manipulation at the client work station PC or server databases,
2. attacks aimed at breaking the authentication mechanism for PIN's or administrative access,
3. attacks directed at defeating voter anonymity,
4. analysis of data in transit that could have been altered, or
5. denial-of-service that prevents voters from being able to reach or cast votes.

Most attack vectors fell into the first category.

The RedPhone penetration test team applied the Open Web Application Security Project (OWASP) evaluation methodology of attack mapping, threat modeling, and poor trust relationship failure analysis to assess where to focus their attention, and then used standard pen-testing tools including attacking physical security, network scanning to locate and exploit vulnerabilities in each of the vendor system. This approach does not look at possible vulnerabilities that may be inherent in the system architecture or data handling procedures at the precinct level. Because of the very limited time and resources available, RedPhone, LLC. adopted an almost entirely ad hoc approach, focusing our attention on those parts of the system that we believed might provide the best attack vector to less secure devices within the DMZ. While we used some source code analysis tools-and several widely used "hacking" tools like Nessus, NMAP and Metasploit-we applied them only selectively, and instead adopted a more "curious" strategy most often used by an

attacker that seeks out weaknesses in the places where he would most likely find vulnerabilities, and then moving on to the next place of potential weakness. This is a very common approach used when limited time and information is available, and when known security is in place, such as out-sourced managed firewalls, routers, or intrusion detection and prevention devices. Our overall impression of the security posture for all three participating vendors was good. We did not find any significant technical security concerns, only minor correctable issues that can easily be mitigated. While time constraints were the biggest limitation, we did find at least one issues involving SSH installed on a server, presumably for remote management purposes. This was the most serious findings, as given more time, we could have likely cracked the password and gained access to the server. We found obvious places where SQL-injection exists, and were tested, but not to the extent that any were successful. Cross-site scripting (reflected) is another case wherein proper coding procedure isn't being followed; however, other mitigating security controls were in place that did not allow for successful penetration. We've documented a good number of informational findings that should be used to improve overall UOCAVA best practice security guidelines.

RedPhone wishes to emphasize that our results do not extend beyond the scope of our investigation of the technical security of the application as seen from the outside. Our scope was limited to that which is defined in our contract with CALIBBRE Systems, and do not contend that these systems are correct or secure beyond the specific findings we've addressed here. Unless otherwise noted, the results of this investigation should be assumed to be relevant only to these three vendor systems and the software version used for this test.

GLOBAL OBJECTIVES

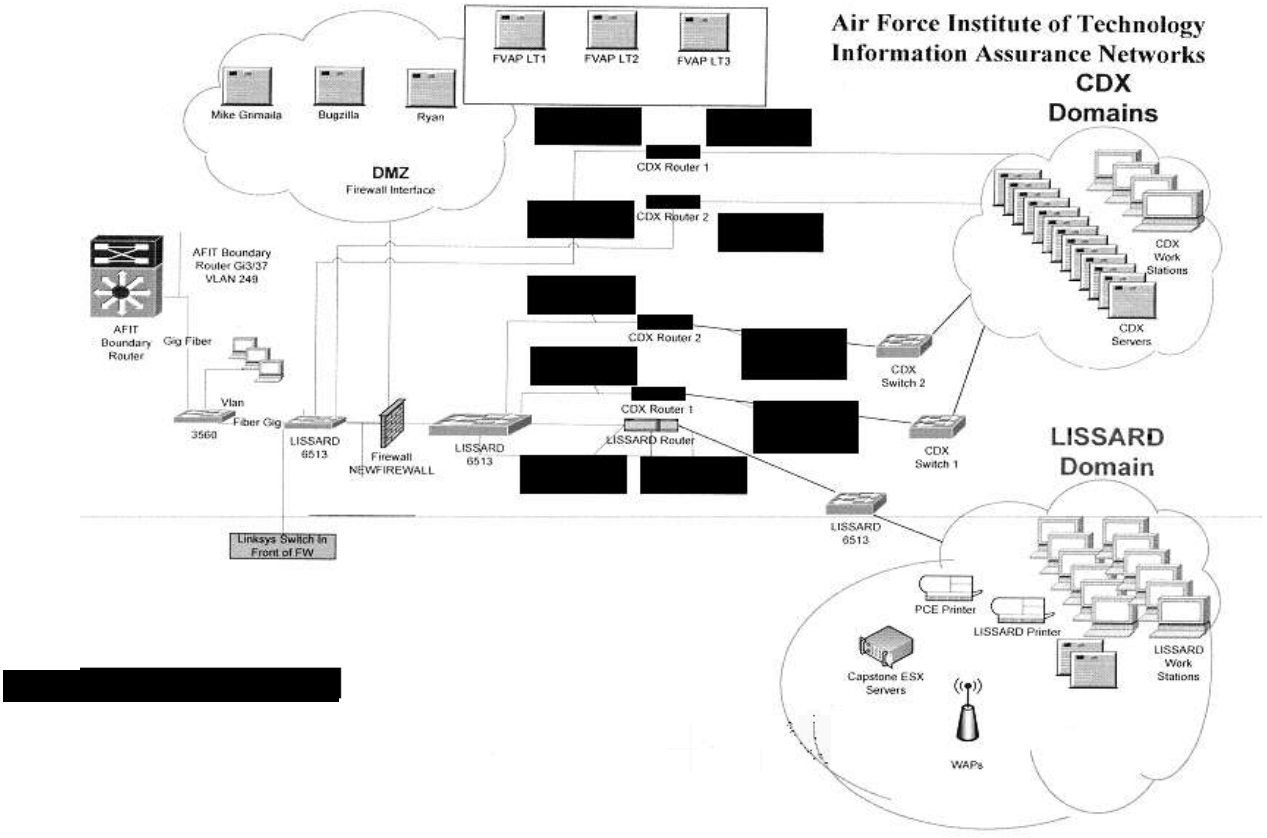
- Breach the security of each vendor's voting systems and gain access to sensitive information on the DMZ Network where a tangential attack vector could be made into the more secure voting systems.
- To emulate a realistic technical threat to the ATF computer networks from persons having no prior access or knowledge other than information that is openly available on the Internet;
- To discover and exploit any vulnerability or combination of vulnerabilities found on the system in order to meet the stated objective of the penetration test; and
- To test the extent an organization's security incident response capability is alerted and to gauge the response to such suspicious activity.

- Recommend best security practices and guidelines that would mitigate these attacks.

PENETRATION TESTING ARCHITECTURE

The AFIT network architecture used by the two internal penetration testing teams is a traditional network architecture that includes a test lab environment, routers, firewalls, a DMZ, and unfiltered access out to the Internet where the penetration test teams used MicroSoft Internet Explorer and Mozilla Firefox browsers to connect to the target servers and local workstations used as voting stations. The AFIT penetration testing team used multiple tools that included, Nessus, NMAP, Metasploit and other tools found on the BackTrack 5 live CD. A complete list of tools used by the AFIT test teams will be provided with their documentation. The RedPhone penetration team performed all their tests remotely, but was on site daily to assist with AFIT testing coordination and support. The laptops used by the AFIT teams were located with the lab environment and provided with unfiltered access to the Internet; the voting station laptops were located within the AFIT's Doolittle lounge where other Air Force personnel could use them for simulated voting. There were no physical security controls placed upon the voting work stations. Below is a high-level representation of the AFIT information assurance network used for the testing. IP addresses have been removed or blacked out.

Figure 1. AFIT Network Architecture



Findings

Each of the vendor's systems provided a level of security that was consistent with most business and technical security best practices. Each vendor's automated security systems detected our attempts to breach the security of the applications at the server side, and response and notification times were well within service level agreement time frames. Also, each vendor was able to quickly identify the attacking IP addresses, shut down the attack, and provide log verification. Therefore, we are confident that each vendor's security systems could detect and respond to most attempts to breach the security and gain access to the system. Specific technical findings are listed below:

FINDING NO. 1: SSH
SEVERITY: HIGH

Brute-force authentication attacks against one vendor's Secure Shell (SSH) service was not successful, but this service should never be made available to a production server, as penetration is almost assured given ample time.

Issue Background

US-CERT issues SSH concerns frequently and should be heeded. The SSH is a network protocol that creates a secure channel between two networked devices in order to allow data to be exchanged. SSH can create this secure channel by using Cipher Block Chaining (CBC) mode encryption. This mode adds a feedback mechanism to a block cipher that operates in a way that ensures that each block is used to modify the encryption of the next block.

SSH contains a vulnerability in the way certain types of errors are handled. Attacks leveraging this vulnerability would lead to the loss of the SSH session. According to CPNI Vulnerability Advisory SSH:

> *If exploited, this attack can potentially allow an attacker to recover up to 32 bits of plaintext from an arbitrary block of ciphertext from a connection secured using the SSH protocol in the standard configuration. If OpenSSH is used in the standard configuration, then the attacker's success probability for recovering 32 bits of plaintext is 2^{-18}. A variant of the attack against OpenSSH in the standard configuration can verifiably recover 14 bits of plaintext with probability 2^{-14}. The success probability of the attack for other implementations of SSH is not known.*

Impact

An attacker may be able to recover up to 32 bits of plaintext from an arbitrary

block of ciphertext.

Issue Mitigation

We are currently unaware of a practical solution to this problem. CERT recommends the use of CTR Mode. This mode generates the keystream by encrypting successive values of a "counter" function. For more information see the Block Cipher Modes article on wikipedia.

In order to mitigate this vulnerability, SSH can be setup to use CTR mode rather CBC mode. According to CPNI Vulnerability Advisory SSH:

> *The most straightforward solution is to use CTR mode instead of CBC mode, since this renders SSH resistant to the attack. An RFC already exists to standardise counter mode for use in SSH (RFC 4344)...*

Systems Affected

Vendor	Status	Date Notified	Date Updated
Bitvise	Vulnerable	2008-11-07	2008-11-24
FiSSH	Vulnerable	2008-11-07	2008-11-24
Icon Labs	Vulnerable	2008-11-07	2008-11-24
OpenSSH	Vulnerable	2008-11-07	2008-11-24
OSSH	Vulnerable	2008-11-07	2008-11-24
PuTTY	Vulnerable	2008-11-07	2009-01-05
Redback Networks, Inc.	Vulnerable	2008-11-07	2008-11-24
SSH Communications Security Corp	Vulnerable	2008-11-07	2008-11-24
TTSSH	Vulnerable	2008-11-07	2008-11-24
VanDyke Software	Vulnerable	2008-11-07	2009-01-12
Wind River Systems, Inc.	Vulnerable	2008-11-07	2008-11-24

References

http://www.cpni.gov.uk/Docs/Vulnerability_Advisory_SSH.txt
http://isc.sans.org/diary.html?storyid=5366
http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

FINDING NO. 2: SQL INJECTION
SEVERITY: MODERATE

The findings listed below are generic and do not reflect any specific vendor's environment. We have kept them generic so that FVAP can assess the overall security posture of these voting systems and make determination about the high-level

guidance and policy recommendations that may be required.

There are five instances of this issue:

Issue background

SQL injection vulnerabilities arise when user-controllable data are incorporated into database SQL queries in an unsafe manner. An attacker can supply crafted input to break out of the data context in which their input appears and interfere with the structure of the surrounding query.

Various attacks can be delivered via SQL injection, including reading or modifying critical application data, interfering with application logic, escalating privileges within the database, and executing operating system commands.

Issue remediation

The most effective way to prevent SQL injection attacks is to use parameterised queries (also known as prepared statements) for all database access. This method uses two steps to incorporate potentially tainted data into SQL queries: first, the application specifies the structure of the query, leaving placeholders for each item of user input; second, the application specifies the contents of each placeholder. Because the structure of the query has already been defined in the first step, it is not possible for malformed data in the second step to interfere with the query structure. Documentation should be reviewed for the database and application platform to determine the appropriate APIs, which can be used to perform parameterised queries. It is strongly recommended that *every* variable data item that is incorporated into database queries is parameterised, even if it is not obviously tainted, to prevent oversights occurring and avoid vulnerabilities being introduced by changes elsewhere within the code base of the application.

FVAP should be aware that some commonly employed and recommended mitigations for SQL injection vulnerabilities are not always effective:

- One common defense is to double up any single quotation marks appearing within user input before incorporating that input into a SQL query. This defense is designed to prevent malformed data from terminating the string in which they are inserted. However, if the data being incorporated into queries are numeric, then the defense may fail, because numeric data may not be encapsulated within quotes, in which case only a space is required to break out of the data context and interfere with the query. Further, in second-order SQL injection attacks, data that has been safely escaped ("escaping" is a technique used to ensure that characters are treated as data, not as characters) when initially inserted into the database is subsequently read

from the database and then passed back to it again. Quotation marks that have been doubled up initially will return to their original form when the data are reused, allowing the defense to be bypassed.

- Another often cited defense is to use stored procedures for database access. While stored procedures can provide security benefits, they are not guaranteed to prevent SQL injection attacks. The same kinds of vulnerabilities that arise within standard dynamic SQL queries can arise if any SQL is dynamically constructed within stored procedures. Further, even if the procedure is sound, SQL injection can arise if the procedure is invoked in an unsafe manner using user-controllable data.

FINDING NO.3: CROSS-SITE SCRIPTING (REFLECTED)
SEVERITY: MODERATE

Issue detail

The value of the parenturl request parameter is copied into a JavaScript string, which is encapsulated in single quotation marks. The payload bb8cf'%3b6b50cb864d6 was submitted in the parenturl parameter. This input was echoed as bb8cf';6b50cb864d6 in the application's response.

This behavior demonstrates that it is possible to terminate the JavaScript string into which data are being copied. An attempt was made to identify a full proof-of-concept attack for injecting arbitrary JavaScript, but this was not successful. The application's behavior should be manually examined and any unusual input validation or other obstacles that may be in place should be identified.

Remediation detail

Echoing user-controllable data within a script context is inherently dangerous, and can make XSS attacks difficult to prevent. If at all possible, the application should avoid echoing user data within this context.

Issue background

Reflected cross-site scripting vulnerabilities arise when data are copied from a request and echoed into the application's immediate response in an unsafe way. An attacker can use the vulnerability to construct a request that, if issued by another application user, will cause JavaScript code supplied by the attacker to execute within the user's browser in the context of that user's session with the application.

The attacker-supplied code can perform a wide variety of actions, such as stealing

the victim's session token or login credentials, performing arbitrary actions on the victim's behalf, and logging their keystrokes.

Users can be induced to issue the attacker's crafted request in various ways. For example, the attacker can send a victim a link containing a malicious URL in an email or instant message. They can submit the link to popular websites that allow content authoring, for example, in blog comments. And they can create an innocuous looking website which causes anyone viewing it to make arbitrary cross-domain requests to the vulnerable application (using either the GET or the POST method).

The security impact of cross-site scripting vulnerabilities is dependent upon the nature of the vulnerable application, the kinds of data and functionality that it contains, and the other applications that belong to the same domain and organization. If the application is used only to display non-sensitive public content, with no authentication or access control functionality, then a cross-site scripting flaw may be considered low risk. However, if the same application resides on a domain that can access cookies for other more security-critical applications, then the vulnerability could be used to attack those other applications, and so may be considered high risk. Similarly, if the organization that owns the application is a likely target for phishing attacks, then the vulnerability could be leveraged to lend credibility to such attacks by injecting Trojan functionality into the vulnerable application and exploiting users' trust in the organization in order to capture credentials for other applications that it owns. In many kinds of application, such as those providing online banking functionality, cross-site scripting should always be considered high risk.

Remediation background

In most situations where user-controllable data are copied into application responses, cross-site scripting attacks can be prevented using two layers of defenses:

- Input should be validated as strictly as possible on arrival, given the kind of content that it is expected to contain. For example, personal names should consist of alphabetical and a small range of typographical characters, and be relatively short; a year of birth should consist of exactly four numerals; email addresses should match a well-defined regular expression. Input which fails the validation should be rejected, not sanitized.

- User input should be HTML-encoded at any point where it is copied into application responses. All HTML metacharacters, including < > " ' and =, should be replaced with the corresponding HTML entities (< > etc).

In cases where the application's functionality allows users to author content

using a restricted subset of HTML tags and attributes (for example, blog comments that allow limited formatting and linking), it is necessary to parse the supplied HTML to validate that it does not use any dangerous syntax; this is a non-trivial task.

FINDING NO.4: SSL COOKIE
SEVERITY: LOW

Issue detail

The following cookie was issued by the application and does not have the secure flag set:

- ASP.NET_SessionId=51dw1odzrv11hdjzl5ztmosw; path=/; HttpOnly

The cookie appears to contain a session token, which may increase the risk associated with this issue. The contents of the cookie should be reviewed to determine its function.

Issue background

If the secure flag is set on a cookie, then browsers will not submit the cookie in any requests that use an unencrypted HTTP connection, thereby preventing the cookie from being trivially intercepted by an attacker monitoring network traffic. If the secure flag is not set, then the cookie will be transmitted in clear-text if the user visits any HTTP URLs within the cookie's scope. An attacker may be able to induce this event by feeding a user suitable links, either directly or via another website. Even if the domain that issued the cookie does not host any content that is accessed over HTTP, an attacker may be able to use links of the form http://example.com:443/ to perform the same attack.

Issue remediation

The secure flag should be set on all cookies that are used for transmitting sensitive data when accessing content over HTTPS. If cookies are used to transmit session tokens, then areas of the application that are accessed over HTTPS should employ their own session handling mechanism and the session tokens used should never be transmitted over unencrypted communications.

FINDING NO. 5: SSL CERTIFICATES
SEVERITY: LOW

This finding is more informational than an actual vulnerability. The vendor had "self-signed" the certificate, and therefore, would not be a trusted certificate, but the vendor had brought this to our attention and explained that this would not be the norm. The other two vendors had implemented the use of certificates

properly.

Issue background

SSL helps to protect the confidentiality and integrity of information in transit between the browser and server, and to provide authentication of the server's identity. To serve this purpose, the server must: present an SSL certificate that is valid for the server's hostname, is issued by a trusted authority and is valid for the current date. If any one of these requirements is not met, SSL connections to the server will not provide the full protection for which SSL is designed.

It should be noted that various attacks exist against SSL in general, and in the context of HTTPS web connections. It may be possible for a determined and suitably-positioned attacker to compromise SSL connections without user detection even when a valid SSL certificate is used.

FINDING NO. 6: COOKIE WITHOUT HTTPONLY FLAG SET
SEVERITY: LOW

This is mostly informational but does constitute a concern.

Issue detail

The following cookie was issued by the application and does not have the HttpOnly flag set:

- JSESSIONID=AB6295DFFAFA6F01E835E88C50F597ED; Path=/portal-webapp; Secure

The cookie appears to contain a session token, which may increase the risk associated with this issue. The contents of the cookie should be reviewed to determine its function.

Issue background

If the HttpOnly attribute is set on a cookie, then the cookie's value cannot be read or set by client-side JavaScript. This measure can prevent certain client-side attacks, such as cross-site scripting, from trivially capturing the cookie's value via an injected script.

Issue remediation

There is usually no good reason not to set the HttpOnly flag on all cookies. Unless legitimate client-side scripts are specifically required within an application to read or set a cookie's value, the HttpOnly flag should be set by including this attribute within the relevant Set-cookie directive.

Guidance should make implementers aware that the restrictions imposed by the

HttpOnly flag can potentially be circumvented in some circumstances, and that numerous other serious attacks can be delivered by client-side script injection, aside from simple cookie stealing.

FINDING NO. 7: REFERER-DEPENDENT RESPONSE
SEVERITY: INFORMATIONAL

Issue description

The application's responses appear to depend systematically on the presence or absence of the Referer header in requests. This behavior does not necessarily constitute a security vulnerability, and the nature of and reason for the differential responses should be investigated to determine whether a vulnerability is present.

Common explanations for Referer-dependent responses include:

- Referer-based access controls, where the application assumes that if the user has arrived from one privileged location then he/she is authorized to access another privileged location. These controls can be trivially defeated by supplying an accepted Referer header in requests for the vulnerable function.
- Attempts to prevent cross-site request forgery attacks by verifying that requests to perform privileged actions originated from within the application itself and not from some external location. Such defenses are not robust- methods have existed through which an attacker can forge or mask the Referer header contained within a target user's requests by leveraging client-side technologies such as Flash and other techniques.
- Delivery of Referer-tailored content, such as welcome messages to visitors from specific domains, search-engine optimisation (SEO) techniques, and other ways of tailoring the user's experience. Such behaviors often have no security impact, however, unsafe processing of the Referer header may introduce vulnerabilities such as SQL injection and cross-site scripting. If parts of the document (such as META keywords) are updated based on search engine queries contained in the Referer header, then the application may be vulnerable to persistent code injection attacks, in which search terms are manipulated to cause malicious content to appear in responses served to other application users.

Issue remediation

The Referer header is not a robust foundation on which to build any security measures, such as access controls or defenses against cross-site request forgery. Any such measures should be replaced with more secure alternatives that are not

vulnerable to Referer spoofing.

If the contents of responses is updated based on Referer data, then the same defenses against malicious input should be employed here as for any other kinds of user-supplied data.

FINDING NO. 8: OPEN REDIRECTION
SEVERITY: INFORMATIONAL

Issue detail

The value of the Referer HTTP header is used to perform an HTTP redirect. The payload //acec8732e3c7ad76d/a%3fhttp%3a//www.google.com/search%3fhl%3den%26q%3d was submitted in the Referer HTTP header. This caused a redirection to the following URL:

- //acec8732e3c7ad76d/a%3fhttp%3a//www.google.com/search%3fhl%3den%26q%3d

The application attempts to prevent redirection attacks by blocking absolute redirection targets starting with http:// or https://. However, an attacker can defeat this defense by omitting the protocol prefix from their absolute URL. If a redirection target starting with // is specified, then the browser will use the same protocol as the page that issued the redirection.

Because the data used in the redirection are submitted within a header, the application's behavior is unlikely to be directly useful in lending credibility to a phishing attack. This limitation considerably mitigates the impact of the vulnerability.

Remediation detail

When attempting to block absolute redirection targets, the application should verify that the target begins with a single slash followed by a letter and should reject any input containing a sequence of two slash characters.

Issue background

Open redirection vulnerabilities arise when an application incorporates user-controllable data into the target of a redirection in an unsafe way. An attacker can construct a URL within the application, which causes a redirection to an arbitrary external domain. This behavior can be leveraged to facilitate phishing attacks against users of the application. The ability to use an authentic application URL, targeting the correct domain with a valid SSL certificate (if SSL is used), lends credibility to the phishing attack because many users, even if they verify these features, will not notice the subsequent redirection to a different

domain.

Remediation background

If possible, applications should avoid incorporating user-controllable data into redirection targets. In many cases, this behavior can be avoided in two ways:

- Remove the redirection function from the application, and replace links to it with direct links to the relevant target URLs.
- Maintain a server-side list of all URLs that are permitted for redirection. Instead of passing the target URL as a parameter to the redirector, pass an index into this list.

If it is considered unavoidable for the redirection function to receive user-controllable input and incorporate this into the redirection target. One of the following measures should be used to minimize the risk of redirection attacks:

- The application should use relative URLs in all of its redirects, and the redirection function should strictly validate that the URL received is a relative URL.
- The application should use URLs relative to the web root for all of its redirects, and the redirection function should validate that the URL received starts with a slash character. It should then prepend http://yourdomainname.com to the URL before issuing the redirect.
- The application should use absolute URLs for all of its redirects, and the redirection function should verify that the user-supplied URL begins with http://yourdomainname.com/ before issuing the redirect.

FINDING NO. 9: CROSS-DOMAIN SCRIPT INCLUDE
SEVERITY: INFORMATIONAL

Issue detail

The response dynamically includes the following script from another domain:

- https://seal.verisign.com/getseal?host_name=www.intvoting.com&size=S&use_flash=NO&use_transparent=NO&lang=en

Issue background

When an application includes a script from an external domain, this script is executed by the browser within the security context of the invoking application. The script can therefore do anything that the application's own scripts can do,

such as accessing application data and performing actions within the context of the current user.

If a script from an external domain is included, then that domain is trusted with the data and functionality of your application, and the domain's own security to prevent an attacker from modifying the script to perform malicious actions within your application.

Issue remediation

Scripts should not be included from untrusted domains. If there is a requirement that a third-party script appears to fulfill, then ideally the contents of that script should be copied onto your own domain and include it from there. If that is not possible (e.g., for licensing reasons), then re-implementing the script's functionality within your own code should be considered.

FINDING NO.10: EMAIL ADDRESSES DISCLOSED
SEVERITY: INFORMATIONAL

Issue detail

During the discovery and reconnaissance phase, we found many vendor email addresses were available. Caution should be taken to train all employees of spear phishing attacks. Spear phishing describes any highly targeted phishing attack. Spear phishers send e-mail that appears genuine to some or all the employees or members within a certain company, government agency, organization, or group. The message might look like it comes from your employer, or from a colleague sending an e-mail message to everyone in the company (such as the person who manages the computer systems) and could include requests for user names or passwords.

The truth is that the e-mail sender information has been faked or "spoofed." Whereas traditional phishing scams are designed to steal information from individuals, spear phishing scams work to gain access to a company's entire computer system. If an employee responds with a user name or password, or if click links or open attachments in a spear phishing e-mail, pop-up window, or website, he/she might become a victim of identity theft and might put his/her employer or group at risk.

Spear phishing also describes scams that target people who use a certain product or website. Scam artists use any information they can to personalize a phishing scam to as specific a group as possible.

Issue background

The presence of email addresses within application responses does not necessarily constitute a security vulnerability. Email addresses may appear intentionally within contact information, and many applications (such as web mail) include arbitrary third-party email addresses within their core content.

However, email addresses of developers and other individuals (whether appearing on-

screen or hidden within page source) may disclose information that is useful to an attacker; for example, they may represent usernames that can be used at the application's login, and they may be used in social engineering attacks against the organization's personnel. Unnecessary or excessive disclosure of email addresses may also lead to an increase in the volume of spam email received.

Issue remediation

FVAP should review and offer guidance concerning the email addresses being disclosed by the application, and consider removing any that are unnecessary, or replacing personal addresses with anonymous mailbox addresses (such as helpdesk@example.com).

FINDING NO. 11: ROBOTS.TXT FILE
SEVERITY: LOW/INFORMATIONAL

While this issue can often give away information to an attacker, this particular instance did not. Therefore, this is informational only.

Issue detail

The web server contains a robots.txt file.

Issue background

The file robots.txt is used to give instructions to web robots, such as search engine crawlers, about locations within the website that robots are allowed, or not allowed, to crawl and index.

The presence of the robots.txt does not in itself present any kind of security vulnerability. However, it is often used to identify restricted or private areas of a site's contents. The information in the file may, therefore, help an attacker to map out the site's contents, especially if some of the locations identified are not linked from elsewhere in the site. If the application relies on robots.txt to protect access to these areas and does not enforce proper access control over them, then this presents a serious vulnerability.

Issue remediation

The robots.txt file is not itself a security threat, and its correct use can represent good practice for non-security reasons. You should not assume that all web robots will honor the file's instructions. Rather, assume that attackers will pay close attention to any locations identified in the file. Do not rely on robots.txt to provide any kind of protection over unauthorized access.

FINDING NO. 12: CACHEABLE HTTPS RESPONSE
SEVERITY: INFORMATIONAL

There are three instances of this issue. This is a minor issue, bordering on informational. These are the result of implementation errors that can be easily corrected.

Issue description

Unless directed otherwise, browsers may store a local cached copy of content received from web servers. Some browsers, including Internet Explorer, cache content accessed via HTTPS. If sensitive information in application responses is stored in the local cache, then this may be retrieved by other users who have access to the same computer at a future time.

Issue remediation

The application should return caching directives instructing browsers not to store local copies of any sensitive data. Often, this can be achieved by configuring the web server to prevent caching for relevant paths within the web root. Alternatively, most web development platforms allow control of the server's caching directives from within individual scripts. Ideally, the web server should return the following HTTP headers in all responses containing sensitive content:

- Cache-control: no-store
- Pragma: no-cache

FINDING NO. 13: SCRIPT FILES
SEVERITY: MODERATE

We successfully downloaded all site scripts from every vendor, no exceptions. With more time allotted to a penetration, this would be a severe issue. Going through the script's contents (and comment sections, etc.) would allow for detailed mapping of site functionality. Hardening of application server configurations is highly recommended for each vendor, in order to mitigate this threat.

Additional tests performed

These types of Distributed Denial-of-Service (DDoS) attacks are not new. Organizations have been battling them since they became popular in the late 1990s. While techniques to defend against DDoS attacks have become more sophisticated, they still represent a difficult challenge and major risk. Limited Denial-of-Service (DoS) attacks were performed. These were unsuccessful. However, mention should be given that no DDoS attacks were performed due to lack of

resources available for the test. It is entirely feasible for a mass denial attack to be successful, and this is an eventuality that is difficult to mitigate.

The DoS attack is focused on making unavailable a resource (site, application, server) for the purpose it was designed. There are many ways to make a service unavailable for legitimate users by manipulating network packets, programming, logical, or resources handling vulnerabilities, among others. If a service receives a very large number of requests, it may stop providing service to legitimate users. In the same way, a service may stop if a programming vulnerability is exploited.

Sometimes the attacker can inject and execute arbitrary code while performing a DoS attack in order to access critical information or execute commands on the server. DoS attacks significantly degrade service quality experienced by legitimate users. It introduces large response delays, excessive losses, and service interruptions, resulting in direct impact on availability.

DoS & DDoS Locking Customer Accounts

The first DoS case to consider involves the authentication system of the target application. A common defense to prevent brute-force discovery of user passwords is to lock an account from use after between three to five failed attempts to login. This means that even if a legitimate user were to provide their valid password, they would be unable to login to the system until their account has been unlocked. This defense mechanism can be turned into a DoS attack against an application if there is a way to predict valid login accounts.

Note: there is a business vs. security balance that must be reached based on the specific circumstances surrounding a given application. There are pros and cons to locking accounts, to customers being able to choose their own account names, to using systems such as CAPTCHA, and the like. Each enterprise will need to balance these risks and benefits, but not all of the details of those decisions are covered here. It should be noted that one vendor does incorporate CAPTCHA as a deterrent to this form of attack. Specific controls to combat DDoS attacks can include:

1. working with the Internet Service Provider (ISP) to establish quality of service rates to limit the amount of bandwidth one customer can utilize;
2. using firewalls and filtering devices to filter all unnecessary ports and protocols;
3. incorporating redundancy and resiliency into designs of key systems; and
4. utilizing IDS/IPS to identify and block attacks in progress

Related Attacks

- Resource Injection
- Setting Manipulation
- Regular expression Denial of Service - ReDoS

Related Vulnerabilities

- Category: Input Validation Vulnerability
- Category: API Abuse

Summary & Conclusions:

Internet based voting systems should be certified and recertified on a regular basis since changes to the operating systems, applications, services, protocols etc. change frequently. All defensive strategies should be risk-based and right-sized to match the risk. In a perfect world, every company could employ every defense possible to protect against every type of attack on every part of its infrastructure. In reality, however, time and resources are not unlimited. Defenses have to be selected and deployed based on a cost-benefit methodology. Voting systems face unique threats, some are at the nation-state level, and therefore, unlimited resources, and game changing technologies could be leveraged to crash services, corrupt votes via insider threats, or devise methods to social engineer perceptions causing voter disenfranchisement. The controls must be appropriate to the risks.

RedPhone suggests that the FVAP determine what department within the federal government is responsible for determining threats associated with the voting process so that an appropriate risk assessment can be done based on known threats. FVAP should use formal risk analysis and cost-benefit analysis to help ensure their control environment is appropriate for their risk profile and tolerance. The risk analysis should include several key steps.

First, the FVAP should perform a formal risk analysis to determine the actual risk to the environment. The risk assessment should consider the value of the assets being protected, likelihood of probable threats and attack vectors, impact of a successful attack, inherent risk of the condition, existing safeguards, and the residual risk as compared to current tolerance.

Next, based on the results of the risk assessment, determine what areas of the voting process are operating at unacceptable levels of risk. Identify controls that can reduce the likelihood of the threat source or lessen the impact to acceptable levels. Perform a cost-benefit analysis to determine if the suggested controls provide an appropriate risk reduction benefit.

The next step should be to implement appropriate controls based on this analysis. Test the controls and likely attack scenarios to validate the controls operate properly and provide the desired effect. Employ monitoring, metrics and measures to ensure key controls continue to perform adequately and provide the expected protections. Continually update the risk assessment as new threats emerge, the business makes changes or other factors change that would affect the risk assessment results. The risk assessment should be updated at least annually to ensure it is still appropriate for the organization and the current environment.

It should be noted that this test had several limitations that would not exist in the “real world”, and therefore additional testing is highly recommended. Also, it should be noted that all testing is a “point-in-time-analysis”, and therefore should never be considered lasting. Testing should be performed with some regularity to maintain the highest level of security posture at all times.

Operational policies for high confidentiality, integrity and availability focus on setting and establishing processes, policies, and strict configuration and patch management. They are divided into the following categories:

- Service Level Management for High Availability
- Planning Capacity to Promote High Availability
- Change Management for High Availability
- Backup and Recovery Planning for High Availability
- Disaster Recovery Planning
- Planning Scheduled Outages
- Staff Training for High Availability
- Documentation as a Means of Maintaining High Availability
- Physical Security Policies and Procedures for High Availability

In addition to the above policies, a well defined and documented software development life-cycle should be adopted. The Capability Maturity Model Integration (CMMI) is a widely followed and adopted best practice that defines practices that include eliciting and managing requirements, decision making, measuring performance, planning work, handling risks, and more. None of the vendors' voting systems are being developed using such a defined life-cycle. We recommend that voting systems vendors adopt rigorous software engineering practices based on CMMI level-3 or better to ensure that system life-cycle, documentation, and methodologies are not random, but instead meet or exceed best practices.

The single greatest risk to Internet voting from an end-users computer is the fact that election officials do not have access to the voting workstation to determine its integrity, nor the upstream Internet supporting infrastructure. However, if a kiosk approach is employed, the election officials still have some control over the environment; it is recommended that the kiosk periodically send "status votes" or "test ballots" that test the integrity and accuracy of the voting system and the end-to-end transmission of the encrypted data. Control of the client-side voting computer, the local network, or upstream Internet Service Providers (ISP's) infrastructure will always present significant challenges to Internet based voting. Therefore, it is imperative that both end-points, and the lines of communication be as secure as possible to maintain the vote integrity, confidentiality, system availability and voter anonymity.

Appendix - C Operation Orange

Jonathan Wright is a tall, handsome, slightly exotic looking Harvard grad, who has served in the U.S. Senate for 8 years. He has recently won the appointment as a candidate for the office of the President of the United States. He has the backing of the military and firefighters of America, as well as various police districts. However, unbeknownst to most of the American public is the fact that though he was born in the U.S., Senator Wright's grandfather, still resides in this fictional nation state.

Now, this nation state is very interested in the latest election because the incumbent president of the U.S. is considering a boycott of all CFS light bulbs, a major product for this nation state. For years they have been the only manufacturers of this product; however, the light bulbs often have defects that have caused severe injuries to American consumers-leading to a public outcry against the product. American and Mexican companies are now producing a superior, if more expensive, light bulb.

Because this issue is in the fore front of the American psyche, the incumbent president wants it to be one of the issues of his platform. A boycott of this product would be a devastating financial blow to their economy. This nation state requires a president sympathetic to their cause in the oval office.
Mr. Wright will champion the product over an American or Mexican one. Primarily, because Mr. Wright still has close family that resides in this nation state; and therefore, he should honor the family name as a proud descendant. This nation state government believes that Mr. Wright would want to support his family's home nation, and maintain their status has the premier supplier of CFS light bulbs. Therefore, this nation state is confident that they will be able to hack the American electronic voting systems to ensure Mr. Wright's election to the office of president.

Specific Objectives:

Acting as hackers, your objective is to hack into the voting system, obtain administrator level rights and access, and *change* the votes so that Senator Wright becomes the next president of the United States. You must "recon" the targeted electronic voting system(s) and thoroughly plan your plan of attack employing sophisticated penetration techniques. If the changes are detected and an audit deems hacking has altered the targeted system(s), the election will merely be deemed void or corrupt and a new one will take place using old fashioned methods beyond the control of the nation state. Furthermore, you must do your best to cover

your “tracks” such that cyber security personnel will not be able to forensically trace the hack to your IP address.

You will have a limited amount of time to perform your reconnaissance of the vendor system(s), determine what tools to use, and ultimately penetrate the system(s) and make the needed changes to ensure the desired outcome. A denial of service attack would quickly be detected and traced, therefore this method of disruption should not be considered.

Keeping in mind that these penetration tests are intended to provide the following:

- Evaluate the protection of the Vendor’s electronic voting systems with a special emphasis on the effectiveness of logical access and system software security controls

- Provide value to the Vendor’s electronic voting system by identifying opportunities to significantly strengthen applicable controls within budgetary and operational constraints

  i.e., documented mitigation strategies, or security patches and/or procedures that improve the security posture of their respective systems.

- To facilitate timely, cost-effective completion of this project, Tiger Teams will make maximum practical use of the relevant work of others where possible (i.e., internal assessments by the auditee, internal and external audits, and vulnerability testing on covered IT assets).

- In order to optimize the effectiveness of the Penetration Test team members, the Vendor’s need to provide access to systems, services, and employees. To perform the work specified in this statement of work, the Tiger Teams will require the following from the customer:

  1. Access to relevant personnel including: technical support, data center personnel, application developers and end-users and functional experts.

  2. Relevant documentation including: System Administration Guides, System Architecture diagrams that include IP addresses of target systems. Previous security threat assessments if available.

  3. A primary point of contact for emergency remediation if needed.

  4. Coordination of events with customer team members.

5. Signed NDA, Authorization to Proceed, and the below Rules of Engagement.

Appendix - D Tools

Information Gatheringbr
Assbr
DMitrybr
DNS-Ptrbr
dnswalkbr
dns-bruteforcebr
dnsenumbr
dnsmapbr
DNSPredictbr
Finger Googlebr
Firewalkbr
Goog Mail Enumbr
Google-searchbr
Goograpebr
Gooscanbr
Hostbr
Itracebr
Netenumbr
Netmaskbr
Piranabr
Protosbr
QGooglebr
Relay Scannerbr
SMTP-Vrfybr
TCtracebr
Network Mappingbr
Amap br
Assbr
Autoscan _Rbr
Fpingbr
Hpingbr
IKE-Scanbr
IKEProbebr
Netdiscoverbr
Nmapbr
NmapFEbr
Pfbr
PSK-Crackbr
Pingbr
Protosbr
Scanrandbr
SinFPbr
Umitbr
UnicornScanbr
UnicornScan pgsql e
module version br
Analysisbr br
Servicesbr
SNORTp
SIPcrackbr
XProbebr
PBNJ br
OutputPBNJbr
ScanPBNJbr
Genlistbr
Vulnerability Identificationbr
Absinthebr
Bedbr
CIRT Fuzzerbr
Checkpwdbr
Cisco Auditing Toolbr
Cisco Enable Bruteforcerbr
Cisco Global Exploiterbr
Cisco OCS Mass Scannerbr
Cisco Scannerbr
Cisco Torchbr
Curlbr
Fuzzer br
GFI LanGuard br
GetSidsbr
HTTP PUTbr
Halberdbr
Httprintbr
Httprint GUIbr
ISR-Formbr
Jbrofuzzbr
List-Urlsbr
Lynxbr
Merge Router Configbr
Metacoretexbr
Metoscanbr
Mezcal HTTPSbr
Mibble MIB Browserbr
Mistressbr
Niktobr
OATbr
Onesixtyonebr
OpenSSL-Scannerbr
Paros Proxybr
Peachbr
RPCDumpbr
RevHostsbr
SMB Bruteforcerbr
SMB Clientbr
SMB Serverscanbr
SMB-NATbr
SMBdumpusersbr
SMBgetserverinfobr
SNMP Scannerbr
SNMP Walkbr
SQL Injectbr
SQL Scannerbr
SQLLibfbr
SQLbrutebr
Sidguessbr
SmbKbr
Snmpcheckbr
Snmp Enumbr
Spikebr
Stompybr
SuperScanbr
TNScmdbr
Taofbr
VNC_bypauthbr
Wapitibr
Yersiniabr
sqlanlzbr
sqldictbr
sqldumploginsbr
sqlquerybr
sqluploadbr
Penetrationbr
Framework-MsfCbr
Framework-MsfUpdatebr
Framework-Msfclibr
Framework-Msfwebbr
Init Pgsql (autopwn)br
Milwrm Archivebr
MsfClibr
MsfConsolebr
MsfUpdatebr
OpenSSL-To-Openbr
Update Milwrmbr
Privilege Escalationbr
Ascend attackerbr
CDP Spooferbr
Cisco Enable Bruteforcerbr
Crunch Dictgenbr
DHCPX Flooderbr
DNSspoofbr
Driftnetbr
Dsniffbr
Etherapebr
EtterCapbr
FileCablebr
HSRP Spooferbr
Hash Collisionbr
Httpcapturebr
Hydrabr
Hydra GTKbr
ICMP Redirectbr
ICMPushbr
IGRP Spooferbr
IRDP Responderbr
IRDP Spooferbr
Johnbr
Lodowepbr
Mailsnarfbr
Medusabr
Msgsnarfbr
Nemesis Spooferbr
NetSedbr
Netenumbr
Netmaskbr
Ntopbr
PHossbr
PackETHbr
Rcrackbr
SIPdumpbr
SMB Snifferbr
Singbr
TFTP-Brutebr
THC PPTPbr
TcPickbr
URLsnarfbr
VNCrackbr
WebCrackbr
Wiresharkbr
Wireshark Wifibr
WyDbr
XSpybr
chntpwbr
Maintaining Accessbr
proxybr
Backdoorsbr
CryptCatbr
HttpTunnel Clientbr
HttpTunnel Serverbr
ICMPTXbr
Iodinebr
NSTXbr
Privoxybr
ProxyTunnelbr
Rinetdbr
TinyProxybr
sbdbr
socatbr
Covering Tracksbr
Housekeepingbr
Radio Network
AFragbr
ASLeapbr
Air Crackbr
Air Decapbr
Air
Replaybr
Airmon Scriptbr
Airpwnbr
AirSnarfbr
Airodumpbr
Hexdumpbr
Airoscriptbr
Airsnortbr
CowPattybr
FakeAPbr
GenKeysbr
Genpmkbr
Hotspotterbr
Karmabr
Kismetbr
Load IPWbr
Load acxbr
MDKbr
MDK for Broadcombr
MacChangerbr
Unload Driversbr
Wep_crackbr
Wep_decryptbr
WifiTapbr
Wicrawlbr
Wlassistantbr
Bluetoothbr
Bluebuggerbr
Blueprintbr
Bluesnarferbr
Btscannerbr
Carwhispererbr
CuteCombr
Ghettotoothbr
HCIDumpbr
Ussp-Pushbr
OllyDBGbr
PcapSipDumpbr
PcapToSip_RTPbr
SIPSakbr
Hexeditbr
SIPdumpbr
SIPpbr
Smapbr
Digital Forensicsbr
Allinbr
Autopsybr
DCFLDDbr
DD_Rescuebr
Foremostbr
Magicrescuebr
Mboxgrepbr
Memfetchbr
Memfetch Findbr
Pascobr
Rootkithunterbr

Sleuthkitbr Vinettobr Reverse Engineeringbr GDB GNU Debuggerbr GDB Console GUIbr
GDB Serverbr GNU DDDbr VOIP & Telephony Analysisbr

Because of some last minute corrections to the ROE/MNDA/ATS documentation, we requested email confirmation of the acceptance. Those e-mail acceptances are below:

From Vendor-2.com
to Jay Aceto <jay.aceto@redphonecorporation.com>
date Sat, Jul 30, 2011 at 9:35 PM
subject RE: Error found. Please resign ROE's & Authorizations to Scan ASAP

Important mainly because it was sent directly to you.

Jay,

On behalf of Vendor-2 I accept the changed documents. I will bring signed copies Monday.

Vice President
Vendor-2

from @Vendor-3.com
to Jay Aceto <jay.aceto@redphonecorporation.com>
date Mon, Aug 1, 2011 at 9:51 AM
subject RE: Error found. Please resign ROE's & Authorizations to Scan ASAP
mailed-by Vendor-3.com

Jay,

I accept the corrections on behalf of Vendor-3.

Vendor-3

From: Vendor-1.com>
To: "Jay Aceto (jay.aceto@redphonecorporation.com)"
<jay.aceto@redphonecorporation.com>
Date: Fri, 22 Jul 2011 15:58:37 -0700
Subject: Student Forms

Hi Jay,

Attached are our authorization signatures and Rules of Engagements for the students…

Vendor-1, Inc.

Appendix C

Federal Voting Assistance Program (FVAP) Security Gap Analysis of UOCAVA Pilot Program Testing Requirements

8 February 2011

FVAP.GOV
FEDERAL VOTING ASSISTANCE PROGRAM

Security Gap Analysis of UOCAVA Pilot Program Testing Requirements

Delivery Order CT 80047-0037

Task 5.1.3

FINAL Report

February 8, 2011

This report was prepared for the Federal Voting Assistance Program by CALIBRE Systems, Inc.

Executive Summary

A complete Internet voting system could provide voter identification and authentication, voter registration, election administration, ballot delivery, voting, tabulation, and results reporting. However, any such electronic voting (eVoting) system must be able to insure privacy and security to the voting individual, as well as confirmation of their vote. However, there are many federal information systems that provide secure data transfer of privacy information and data of higher national security that are arguably far more sensitive than voting information that are currently in use and have met the requirements of the most stringent security guidance.

In December 2010, CALIBRE cyber security subject matter experts (SMEs) reached out to industry and federal agency contacts for additional insights on threats capable of launching a successful distributed denial of service (DDoS) attack or exploiting vulnerabilities associated with an eVoting system. A call for recommendations and insights was sent to senior cyber security experts and national security advisors. Additionally, CALIBRE contacted Carnegie Mellon University's Software Engineering Institute and Computer Emergency Response Team (CERT) for additional recommendations.

Simultaneously, CALIBRE began base-lining current UOCAVA testing requirements to determine if they meet current cyber threats. In total, 259 requirements were identified in the UOCAVA Pilot Program Test document from August 2008−2010. While many are functional requirements, all were evaluated for their security risk and potential exploit impacts. A security matrix was used to map the requirements to multiple industry and federal government security best practices and mandated requirements including: The National Institute of Standards and Technology (NIST), The International Standards Organization (ISO), Federal Information Security Management Act (FISMA), the Government Accountability Office (GAO), the Department of Defense (DoD), and Director of Central Intelligence Directive 6/3 Protecting Sensitive Compartmented Information within Information Systems (DCID 6/3).

Of the 259 requirements identified and evaluated, some only impact one of the three areas (confidentially, integrity and availability), but others could impact more than one. One hundred fifty requirements impacted confidentially, 246 impacted integrity, and 191 impacted availability. Of the 259 requirements, only 41 were categorized as having a low impact to security. However, 130 were considered to have a medium impact, and 88 were considered to have a high potential impact.

Of the 259 identified UOCAVA Pilot Program Testing Requirements, 186 meet specific federal guidance in the seven documents and are listed as "compliant" in the security requirements traceability matrix. Of the 259 requirements, 30 could not be traced directly to a federal requirement in the seven identified guidance documents. Therefore, it was unknown whether these requirements meet technical security requirements. Fifteen of the requirements are functional and do not have a security impact, and thereby, do not need to be reconciled. However, reconciliation with federal or international standards of 15 requirements was recommended. CALIBRE attempted to locate all documents listed as references within the UOCAVA Pilot Program Testing Requirements to match the 15 to possible requirements listed in those references. Not all of the references were located. However, of the un-reconciled 15 UOCAVA

Pilot Program Testing Requirements only 2 were found within the located references and were reconciled. Of the 13 requirements that were not found, they *do* follow best business practices.

Fifty-eight requirements were identified as functional (including the 15 mentioned above) and had no direct impact on security; they are only a functionality of the voting system. The most relevant finding is that NONE of the requirements that were traced were identified as NOT being compliant with the guidance, i.e., there are no notable gaps between UOCAVA Pilot Program Testing Requirements and the security guidance of the seven documents used in this analysis.

Table of Contents

Table of Tables

1 Background

The Federal Voting Assistance Program (FVAP) administers the federal responsibilities of the Presidential designee (Secretary of Defense) under the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) of 1986. The Director, FVAP administers the Act on behalf of the Secretary of Defense.

The Act covers more than six million potential voters including the following:

- Active duty members of the uniformed services including the Coast Guard, commissioned corps of the Public Health Services, the Merchant Marine, and National Oceanic and Atmosphere Administration (NOAA);
- Their voting age dependents; and
- U.S. citizens residing outside the United States.

A complete electronic voting (eVoting) system would provide voter identification and authentication, voter registration, election administration, ballot delivery, voting, tabulation, and results reporting. However, any such eVoting system must be able to insure privacy and security to the voting individual, as well as confirmation of their vote.

2 Scope

The CALIBRE team, in support of FVAP efforts to develop the most secure remote voting capabilities, has been contracted to provide a technical gap analysis of testing procedures and related policies. In accordance with established guidance, [including NIST's research on security issues associated with remote electronic UOCAVA voting, and in coordination with the FVAP Office, the Wounded Warrior Care and Transition Policy (WWCTP) Office, and the Election Assistance Commission (EAC)] the CALIBRE team will conduct a variety of research, analysis, evaluation, and gap mitigation strategies to meet FVAP's strategic goals. The primary intent is to improve the policies, processes, and procedures for Wounded Warriors, disabled military members, military members, their dependents, and overseas civilian voters to register and vote successfully and securely with a minimum amount of effort.

3 Methodology

During the months of December 2010 and January 2011, a policy analysis team assembled relevant UOCAVA and FVAP materials and reviewed all known security-related concerns and policies relative to the UOCAVA Pilot Program Testing Requirements to understand these security issues. These efforts included, but were not limited, to the following:

- Identify all currently available UOCAVA, EAC, and FVAP mission and confidentiality policies.
- Identify mission assurance and confidentiality levels.
- Indentify most appropriate federal and industry best practices and guidance. Perform line-at-a-time comparison of UOCAVA Program Testing Requirements to all the chosen federally recognized and supported guidance standards.
- Produce a gap analysis and correlate identified security weaknesses with national vulnerability databases.
- Provide analysis of results.
- Identify mitigating methodologies and approaches when possible.

3.1 Identification of Mission and Data Classification

3.1.1 The Mission of FVAP

FVAP's mission is to facilitate the absentee voting process for UOCAVA citizens living around the world. This includes: consulting with state and local election officials; prescribing the Federal Post Card Application (FPCA) for absentee registration/ballot requests, along with Federal Write-in Absentee Ballots (FWAB); and distributing descriptive material on state absentee registration and voting procedures. FVAP has three primary focus areas within its mission:

- Assist military and overseas voters in exercising their right to vote.
- Assist state and local election officials in complying with the requirements of federal law, and in providing equal voting opportunity for military and overseas voters.
- Advocate for military and overseas voting rights with federal, state and local governments.

3.1.2 Selection of MAC I and Confidentiality Level Sensitive

It is difficult to assign a DoD Mission Assurance Category (MAC) to the e-Voting system. However, in DoD Directive 8500.1 (Information Assurance) the DoD defines Mission Assurance Category I (MAC I) as the following: "Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include

the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures."[1]

While MAC I relates only to deployed forces outside the continental U.S. (OCONUS) and information that can affect their mission effectiveness, because the electoral process is considered to be an issue of national security, the e-Voting system would fall within this MAC level.

As for the confidentiality level (CL)[2] of the e-Voting system, the data stored in the system most closely matches the definition of sensitive data. For reasons of national security and for the highest level of confidentiality appropriate to the electoral process, we are evaluating the systems based on this level of classified.

Therefore, our analysis of the UOCAVA Pilot Program Testing Requirements in relation to the e-Voting system has been assigned the highest level Mission Assurance Category of I and confidentiality level of Classified, and will be evaluated against those Information Assurance (IA) controls.

Table 1. Applicable IA Controls by MAC and CL Level

Mission Assurance Category and Confidentiality Level	Applicable IA Controls
MAC I, Classified	Encl. 4, Attachments A1 (Mission Assurance Category I Controls for Integrity and Availability) and A4 (Confidentiality Controls for DoD Information Systems Processing Classified Information)
MAC I, Sensitive	Encl. 4, Attachments A1 and A5
MAC I, Public	Encl. 4, Attachments A1 and A6
MAC II, Classified	Encl. 4, Attachments A2 and A4
MAC II, Sensitive	Encl. 4, Attachments A2 and A5
MAC II, Public	Encl. 4, Attachments A3 and A6
MAC III, Classified	Encl. 4, Attachments A3 and A4
MAC III, Sensitive	Encl. 4, Attachments A3 and A5
MAC III, Public	Encl. 4, Attachments A3 and A6

3.1.3 Relevant Government Guidance

The UOCAVA Pilot Program Testing Requirements were derived from 120 references. These references range from a "Request for Proposal" and the Nevada Gaming Commission and State Gaming Control Board to IEEE standards[3]. While a few NIST special publications are listed, there are no references to current DIACAP guidance—which is needed for certification and accreditation if FVAP requires

[1] http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf

[2] http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf, Table E4.T3. Operating Environment Summary by Confidentiality Levels

[3] UOCAVA Pilot Program Testing Requirements, Appendix B.

certification and accreditation (C&A). Of the 259 identified requirements, 99 are security specific (only 32 percent). While UOCAVA made a significant effort to capture and define requirements based on 100-plus seemingly relevant guidance, we believe that fewer, more succinct references will benefit FVAP in the technical gap analysis.

Therefore, CALIBRE used seven prevailing IA documents for the Pilot Program Testing Requirements technical gap analysis. Within the Information Assurance industry there are multiple documents that provide guidance to civilian agencies, DoD and the intelligence community. For the civilian agencies, the dominant guiding documents are the NIST Special Publications; for DoD, there is the DIACAP guidance[4]; and for the intelligence community, there is the DCID 6/3. These three prevailing guidance documents are used to support this technical gap analysis for the following reasons. FVAP is a DoD entity, and therefore, falls under DIACAP processes. FVAP has a mission to support both DoD and civilian overseas personnel; falling under the NIST guidelines. However, because the electoral process is considered to be an issue of national security, the DCID 6/3 guidance must also be considered in the technical gap analysis.

In addition to this guidance, CALIBRE also referenced ISO 17799 (the International Standards Organization) due to the international requirements of FVAP, and ICD 503 (Intelligence Community Directive)—which was to replace DIACAP[1] in the analysis. FISMA guidance[5] and Government Accounting Office (GAO) FISCAM guidance[6] were also used because they are the mandating documents guiding all IA requirements within the U.S. Government.

3.1.4 Industry/Federal Data Call

In addition to the UOCAVA Pilot Testing Program gap analysis, CALIBRE has reached out to industry and federal agency contacts for additional insights on threats capable of launching a successful distributed denial of service (DDoS) attack on an election system. A data call for recommendations and insights were sent to 12 senior cyber security experts and national security advisors. Carnegie Mellon University's Software Engineering Institute and Computer Emergency Response Team (CERT) were contacted for additional guidance and recommendations. Aaron Bossert, a senior software exploit analyst for CERT has recommended that FVAP require vendors to apply the NIST SP-800-137 methodology and tools to the development and implementation of eVoting software. The recently developed NIST Software Assurance Metrics and Tool Evaluation (SAMATE) project defines software assurance as a "planned and systematic" set of activities that ensures that software processes and products conform to requirements, standards and procedures from the NASA Software Assurance Guidebook and Standard to better achieve the following:

- Trustworthiness—no exploitable vulnerabilities exist, either of malicious or unintentional origin (i.e., nothing is transmitted externally that will put the system at risk.)

[4] DIACAP guidance was intended to be replaced by Intelligence Community Directive (ICD503). However, this transition has not been widely adopted.

[5] The Federal Information Security Management Act of 2002.

[6] GAO Federal Information System Controls Audit Manual (FISCAM), 2009.

- Predictable Execution—justifiable confidence that software, when executed, functions as intended.

3.1.5 Internet Search

CALIBRE searched the following international vulnerability databases for technical vulnerabilities associated with the UOCAVA Pilot Program Testing Requirements:

- Microsoft Technical Databases
- NIST National Vulnerability Database
- National Checklist Program (automatable security configuration guidance in XCCDF & OVAL)
- SCAP (program and protocol that NVD supports)
- SCAP Compatible Tools
- SCAP Data Feeds (CVE, CCE, CPE, CVSS, XCCDF, OVAL)
- Product Dictionary (CPE)
- Impact Metrics (CVSS)
- Common Weakness Enumeration (CWE)
- CVE Vulnerabilities−http://cve.mitre.org/
- Checklists−http://web.nvd.nist.gov/view/ncp/repository
- US-CERT Alerts−http://www.us-cert.gov/cas/techalerts/
- US-CERT Vuln Notes− http://www.kb.cert.org/ vuls/byupdate?open&start=1&count=10
- OVAL Queries−http://oval.mitre.org/
- Secunia−http://secunia.com/advisories/search/
- packetstorm− http://packetstormsecurity.org/files/tags/exploit/
- SANS Internet storm center− http://isc.incidents.org/
- OSVDB−http://osvdb.org/project_aims

4 Technical Gap Analysis

CALIBRE performed a technical gap analysis to compare existing UOCAVA internally published testing requirements with multiple federally supported and industry recognized information assurance guidance. The results were then compared to determine the current protection posture specific to e-Voting in order to better understand how effective those policies and requirements were in meeting security needs for eVoting as defined in the current government and industry standards.

This technical gap analysis identifies gaps in the current UOCAVA Pilot Program Testing Requirements (August 2008) based on guidance from multiple sources. The most widely referenced information assurance guidance comes from the following federally supported documents:

Table 2. Referenced Guidance

Selected Guidance	Summary
The National Institute of Standards and Technology (NIST) Special Publications Series SP800-53A Rev2.	NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing the Federal Information Security Management Act (FISMA) of 2002 and in managing cost-effective programs to protect their information and information systems.
The International Standards Organizations (ISO) and the International ElectroTechnical Commission (IEC)	ISO/IEC 17799:2005 is a code improved protection of practice for information security management. The revised ISO/IEC 17799:2005 is the most important standard for managing information security that has been developed.
The Government Accounting Office (GAO) Federal Information System Control Audit Manual (FISCAM)	Provides security requirements for applicable controls specific to the applications they support. However, they generally involve ensuring that: - data prepared for entry are complete, valid, and reliable; - data are converted to an automated form and entered into the application accurately, completely, and on time; - data are processed by the application completely and on time, and in accordance with established requirements; and - output is protected from unauthorized modification or damage and distributed in accordance with prescribed policies.

Selected Guidance	Summary
The FIPS199/200	Standards to be used by all federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels. Guidelines recommending the types of information and information systems to be included in each category. Minimum information security requirements (i.e., management, operational, and technical controls) for information and information systems in each such category. Standards for categorizing information and information systems collected or maintained by or on behalf of each federal agency based on the objective of providing appropriate levels of information security according to a range of risk levels. Guidelines recommending the types of information and information systems to be included in each category. Minimum information security requirements for information and information systems in each such category.
The Department of Defense 8500.2	Implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks.
The Director Central Intelligence Directive 6/3	Provides uniform policy guidance and requirements for ensuring adequate protection of certain categories of intelligence information; Provides guidance to assist an Information System Security Manager (ISSM) or Information System Security Officer/Network Security Officer, (ISSO/NSO) in structuring and implementing the security protections for a system.
Intelligence Community Directive 503 (ICD 503)	ICD focuses on a holistic and strategic process for the risk management of information technology systems, and on processes and procedures designed to develop the use of common standards across the intelligence community.

CALIBRE created a baseline of current UOCAVA Testing Requirements to determine if they meet current cyber threats. In total, 259 requirements were identified in the UOCAVA Pilot Program Test document from August 2008−2010. While many are functional requirements, all were evaluated for their security risk and potential exploit impacts. Using the NIST guidance, DIACAP guidance and DCID 6/3, the impacts were

rated as low, medium and high relative to confidentially, integrity, and availability. The definition of the categories as stated by the three guidance methodologies is shown in the following tables.

Table 3. Operating Environment Summary by Confidentiality Level According to NIST

Security Objective	Potential Impact		
	Low	Medium	High
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction; includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. Basic Testing: A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object.	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Table 4. Operating Environment Summary by Confidentiality Level According to DIACAP

Confidentiality Level	Internal System Exposure	External System Exposure
High (Systems Processing Classified Information)	• Each user has a clearance for **all information** processed, stored or transmitted by the system. • Each user has access approval for **all information** stored or transmitted by the system. • Each user is granted access **only to information for which the user has a valid need-to-know**.	• System complies with DoDD C-5200.5 reference (aj) requirements for physical or cryptographic isolation. • All Internet access is prohibited. • All enclave interconnections with enclaves in the same security domain require boundary protection (e.g., firewalls, IDS, and a DMZ). • All enclave interconnections with enclaves in a different security domain require a controlled interface. • All interconnections undergo a security review and approval.
Medium (Systems Processing Sensitive Information)	• Each user has access approval for **all information** stored or transmitted by the system. • Each user is granted access **only to information for which the user has a valid need-to-know**. • Each IT user meets security criteria commensurate with the duties of the position.	• All non-DoD network access (e.g., Internet) is managed through a central access point with boundary protections (e.g., a DMZ). • All enclave interconnections with enclaves in the same security domain require boundary protection (e.g., firewalls, IDS, and a DMZ). • All remote user access is managed through a central access point. • All interconnections undergo a security review and approval.
Basic (Systems Processing Public Information)	• Each user has access approval for **all information** stored or transmitted by the system. • Each IT user meets security criteria commensurate with the duties of the position.	• N/A as the purpose of system is providing publicly released information to the public.

Table 5. Operating Environment Summary by Confidentiality Level According to DCID 6/3[7]

Level of Concern	Confidentiality Indicators (Chapter 4)	Integrity Indicators (Chapter 5)
Basic	Not applicable to this manual.	Reasonable degree of resistance required against unauthorized modification; or loss of integrity will have an adverse effect.
Medium	Not applicable to this manual.	High degree of resistance required against unauthorized modification; or bodily injury might result from loss of integrity; or loss of integrity will have an adverse effect on organizational-level interests.
High	All Information Protecting Intelligence Sources, Methods and Analytical Procedures. All Sensitive Compartmented Information.	Very high degree of resistance required against unauthorized modification; or loss of life might result from loss of integrity; or loss of integrity will have an adverse effect on national-level interests; or loss of integrity will have an adverse effect on confidentiality.

Protection Levels According to DCID 6/3

Lowest Clearance	Formal Access Approval	Need To Know	Protection Level
At Least Equal to Highest Data	All Users Have ALL	All Users Have ALL	1 (paragraph 4.B.1)
At Least Equal to Highest Data	All Users Have ALL	NOT ALL Users Have ALL	2 (paragraph 4.B.2)
At Least Equal to Highest Data	NOT ALL users have ALL	Not Contributing to Decision	3 (paragraph 4.B.3)
Secret	Not Contributing to Decision	Not Contributing to Decision	4 (paragraph 4.B.4)
Un-cleared	Not Contributing to Decision	Not Contributing to Decision	5 (paragraph 4.B.5)

There are no additional security requirements under the DCID 6/3 guidance, and the translation of the confidentiality, integrity and availability is directed at secure compartmented information (SCI) and the need to know. We've taken the high water mark of a High PL1 DCID 6/3 security profile for the UOCAVA Pilot Program Testing gap analysis.

A Pilot Program Testing Requirements Matrix[8] was created to map the requirements to multiple industry and federal government security best practices and mandated requirements as identified in Table 2.

We searched for security weaknesses and gaps by associating UOCAVA Pilot Program Testing Requirements with the seven guidance documents. Of the 259 requirements identified and evaluated, some only impact one of the three areas (confidentially, integrity and availability), but others could impact more than one; 150 requirements impacted confidentially, 246 impacted integrity, and 191

[7] Director Central Intelligence Directive 6/3, http://www.fas.org/irp/offdocs/DCID_6-3_20Manual.htm#Protection Levels

[8] See Appendix A: Security Requirements Traceability Matrix

impacted availability. Of the 259 requirements, only 41 were categorized as having a low impact to security. However, 130 were considered to have a medium impact, and 88 were considered to have a high potential impact.

Of the 259 identified UOCAVA Pilot Program Testing Requirements, 186 meet specific federal guidance in the seven documents and are listed as "compliant" in the security requirements traceability matrix. Of the 259 requirements, 30 could not be traced directly to a federal requirement in the seven identified guidance documents. Therefore, it was unknown whether these requirements meet technical security requirements. Fifteen of the requirements are functional and do not have a security impact, and thereby, do not need to be reconciled. However, reconciliation with federal or international standards of 15 requirements was recommended. CALIBRE attempted to locate all documents listed as references within the UOCAVA Pilot Program Testing Requirements to match the 15 to possible requirements listed in those references. Not all of the references were located. However, of the un-reconciled 15 UOCAVA Pilot Program Testing Requirements only 2 were found within the located references and were reconciled. Of the 13 requirements that were not found, they *do* follow best business practices.

Fifty-eight requirements were identified as functional (including the 15 mentioned above), and had no direct impact on security; they are only a functionality of the voting system. The most relevant finding is that NONE of the requirements that were traced were identified as NOT being compliant with the guidance, i.e., there are no notable gaps between UOCAVA Pilot Program Testing Requirements and the security guidance of the seven documents used in this analysis.

5 Recommendations

The industry assumption is that technology is a step behind the high level of encryption. This assumption, however, is continually challenged by advances in technology. For FVAP, the challenges are further complicated by the fact that the majority of sophisticated and well-funded threat information is held in a classified status and is not available for general disclosure. Furthermore, in the computer world, information a month old is often outdated. The most recent publication, the *NIST Draft White Paper on Security Considerations for Remote Electronic UOCAVA Voting* (which is still out for comments), documents threats to UOCAVA voting systems using electronic technologies for overseas and military voting. However, by the time it is formally released, the cyber threat community may have ensured that the information is no longer viable.

Therefore, once the new security requirements have been identified and/or mitigated, they should be tracked over time to address changes in regulatory compliance, new attack vectors, threats and known vulnerabilities; the weighing of effort required to protect vulnerabilities will need to be assessed frequently as new technologies and exploit capabilities are developed or become known.

5.1 Recommendations to the UOCAVA Pilot Program Testing Requirements

CALIBRE recommends that FVAP address the following areas based on identified potential technical vulnerabilities and security weaknesses within the UOCAVA Pilot Program Testing Requirements. (See Table 6).

Table 6. Recommendations to the UOCAVA Pilot Program Testing Requirements

Item	UOCAVA Req. No.	Recommendations
1.	2.2.3	Recommend that the following guidance be referenced and followed. NIST SP800-52 provides guidance on protecting transmission integrity using TLS. Other NIST documents include SP800-81, 800-44, 800-45, 800-49, 800-57, 800-58, 800-66, 800-77 and 800-81. FIPS 198 also discusses transmission quality.
2.	2.3.1.1	Recommend that all graphic file formats be tested for corruption from malformed packets. Known vulnerabilities exist with almost all graphic file formats. Appropriate patches to operating systems must be tested.
3.	2.3.1.2	No recommendation. However, the requirement does not specify how this is to be accomplished.
4.	2.6.2.2	See recommendation for 2.3.1.1.
5.	2.6.2.3	See recommendation for 2.3.1.1.
6.	2.7.1.1	Recommend that IDS/IPS system(s) SHALL be used that actively monitors, detects, and notifies system administrators of any potential malicious activity.
7.	4.9.1.3	Recommend the use of application scanning tools such as Fortify 360, Nessus,

Item	UOCAVA Req. No.	Recommendations
		Lumension etc. to identify source code vulnerabilities.
8.	4.9.1.4	See recommendation for 4.9.1.3.
9.	5.1.1.1	See recommendation for 4.9.1.3.
10.	5.1.1.2	See recommendation for 4.9.1.3.
11.	5.2.1.1	Recommend the use of three-factor authentication method to include biometric with a Cross over Error Rates (CER) and Equal Error Rates that meet minimum DoD requirements.
12.	5.2.1.3	Recommend that passwords conform to DOD minimum requirements.
13.	5.2.1.12	Recommend that authentication schema SHALL be commensurate with the highest level technically feasible, as this will constantly change as new schemas become available.
14.	5.3.1.2	See recommendation for 5.2.1.12.
15.	9.5.1.9	Recommend adoption of DoD guidance for erasable media.

The following table is a list of UOCAVA Pilot Program Testing Requirements that were not found in any of the seven governmental guidance documents used for the technical gap analysis. The requirements on this list should be reconciled. (See Table 7).

Table 7. UOCAVA Pilot Program Testing Requirements that are Not Reconciled with Guidances.

Item	UOCAVA Requirement Number	UOCAVA Requirement Title
1.	4.3.1.2	Module Testability
2.	4.3.1.3	Module Size and Identification
3.	4.7.2.7	Nullify Freed Pointers
4.	4.7.2.8	Do not disable error checks
5.	4.7.2.11	Election Integrity Monitoring
6.	5.4.1.2	Cast Vote Integrity Storage
7.	5.4.1.3	Cast Vote Storage
8.	5.4.1.4	Electronic Ballot Box Integrity
9.	6.2	Components from Third Parties
10.	6.3	Responsibilities for Tests
11.	7.5.2	Function Configuration Audit (FCA)
12.	8.2.1	TDP Implementation
13.	8.3.4.1	Hardwired and Mechanical implementations of logic
14.	8.3.4.2	Logic Specifications for PLD's, FPGA's and PIC's
15.	8.4.5.3	Justify Coding Conventions
16.	8.4.6.1	Application Logic Operating Environment
17.	8.4.7.1	Hardware Environment and Constraints
18.	8.4.8.2	Compilers and Assemblers
19.	8.4.8.3	Interpreters
20.	8.4.9.1	Application logic functional specification
21.	9.2.3.3	Traceability of Procured Software
22.	9.4.5.1	Ballot Count and Vote Total Auditing
23.	9.5.1.4	Election Specific Software Identification
24.	9.5.1.7	Compiler Installation Prohibited

Item	UOCAVA Requirement Number	UOCAVA Requirement Title
25.	9.5.1.8	Procurement of System Software
26.	9.6.1.2	Setup Inspection Record generation
27.	9.6.1.12	Consumables quantity of vote capture device
28.	9.6.1.13	Consumables Inspection Procedures
29.	9.6.1.14	Calibration of vote capture devices components nominal range
30.	9.6.1.15	Calibration of vote capture device components inspection procedure

At this point, CALIBRE researched the UOCAVA Pilot Program Testing Requirements references to attempt to map the 30 un-reconciled requirements to other guidance. Of the 30 requirements to be reconciled, 15 were functional and did not have a security impact, and 2 were found in other related federal references. The remaining 13 requirements could not be mapped to specific federal regulatory guidance or requirements, but do support best business practices. (See Table 8.)

Table. 8 UOCAVA Security Control Reconciliation

UOCAVA Requirement	Impact (C,I,A)	Risk	Comment
4.7.2.7 Nullify Freed Pointers	I, A	Medium	A best coding practice. Recommend that coding follow CMMI level-3 methodologies at a minimum.
6.3 Responsibility for tests	I, A	Medium	No specific regulatory requirement for manufactures to perform tests. Normally included within the RFP.
8.3.4.1 Hardwired and mechanical implementation logic	C, I, A	High	Falls under border logic. This should be addressed within the System Security Plan.
8.3.4.2 Logic specification for PLD's, FPGA's, and PIC's	C, I, A	High	Falls under border logic. This should be addressed within the System Security Plan.
8.4.5.3 Justify coding conventions	C, I, A	Medium	No specific regulation identified. Can be addressed within the RFP.
8.4.8.3 Interpreters	C, I, A	Low	No specific NIST or IEEE Requirements identified for COTS runtime code version. However, this should be documented within the System Security Plan.
8.4.9.1 Application logic functional specifications	C, I, A	Low	No specific NIST or IEEE Requirements identified for COTS runtime code version. However, this should be documented within the System Security Plan.
9.5.1.4 Election specific software identification	I	Medium	This is best security practice, but no specific federal regulatory reference could be identified.
9.5.1.7 Compiler installation prohibited	C, I, A	Medium	This is best security practice, but no specific federal regulatory reference could be identified.
9.6.1.2 Setup inspection record generation	C, I, A	Medium	Ref. in NIST SP800-100 speaks to security checklists. Should be addressed within the System Security Plan.
9.6.1.12 Consumables quantity of vote capture device	A	Low	Not a significant risk.
9.6.1.13 Consumables inspection	A	Low	No specific security risk. Mentioned in NIST H143 and media

UOCAVA Requirement	Impact (C,I,A)	Risk	Comment
procedures			storage. Should be addressed within the System Security Plan.
9.6.1.14 Calibration of vote capture device components nominal range	I	Medium	This should fall under System Security Plan guidance. Should be addressed within the System Security Plan.

Note: for column 2, C=Confidentiality, I=Integrity, and A=Availability.

5.2 Things to Consider

5.2.1 Software Monitoring

Our data call research indicates that several automation specifications exist to support the continuous monitoring of software assurance, including the emerging Software Assurance Automation Protocol (SwAAP) that is being developed to measure and evaluate software weaknesses and assurance cases. SwAAP uses a variety of automation specifications such as the Common Weakness Enumeration (CWE), which is a dictionary of weaknesses that can lead to exploitable vulnerabilities, and the Common Weakness Scoring System (CWSS) for assigning risk scores to weaknesses. SwAAP also uses the Common Attack Pattern Enumeration & Classification (CAPEC)—which is a publicly available catalog of attack patterns with a comprehensive schema and classification taxonomy—to provide descriptions of common methods for exploiting software, and the Malware Attribute Enumeration & Characterization (MAEC), which provides a standardized language for encoding and communicating information about malware based upon attributes such as behaviors, artifacts, and attack patterns.

5.2.2 Other Secure Systems

There are many federal information systems that provide secure data transfer of privacy information and data of higher national security that are arguably far more sensitive than voting information and are currently in use and have met the requirements of the most stringent security guidance. For example, the EQIP[9] and JPAS[10] systems have been online for quite some time, and one can draw some very important parallels to an e-Voting system. They have to support the reality that a user may access it from any internet-connected computer system, and they must verify the relative security of that system. Another parallel is that the sensitivity is arguably equal to or greater than an e-Voting system.

Furthermore, the IRS uses the Electronic Federal Tax Payment System (EFTPS). Tax returns contain considerable privacy information including: name, address, rank, SSN, income, income sources, deductions, dependents, donations, and investments. However, since 1986, and with over 400 million

[9] EQIP is the Office of Personnel Managements background investigation tool. It has a diagnostic tool for evaluating the security of a PC to determine if it meets security requirements. This could also be used for remote voting via Internet.

[10] http://www.dss.mil/diss/jpas/jpas.html

returns, the IRS e-file system has never been compromised. According to the IRS website, the following facts and information are true.

- *The IRS* **e-file** *System is not done over e-mail.*
- *The IRS* **e-file** *System has many built-in security features.*
- *The IRS* **e-file** *System employs multiple firewalls.*
- *The IRS* **e-file** *System uses state of the art virus and worm detection.*
- *The IRS* **e-file** *System meets or exceeds all government security standards.*
- *The IRS* **e-file** *System is constantly tested for weaknesses by penetration testing.*
- *The IRS* **e-file** *System has never had a security breach.*
- *All Internet transmissions will use SSL (Secure Sockets Layer) encrypted security measures.*

IRS **e-file** *transmissions are very secure because the IRS has been extremely diligent in the design, development, analysis and testing of the current infrastructure and system. IRS* **e-file** *meets or exceeds all government security standards and includes multiple firewalls.*

Most e-filed online tax returns are transmitted over phone lines from the return preparer to a third-party transmitter. From there, the returns are forwarded over secured lines to the IRS. Intercepting telephone transmissions is quite difficult and requires access to phone company major transmission lines. Also, to transmit data like tax returns over telecommunications lines means that the information gets converted into digital format, which could not be easily read even if it were intercepted.[11]

Because user confidence and demand is high, the IRS has recently designed and deployed a mobile application for use across inherently unsecured wireless connection (e.g., iPhone/Android apps).

In addition to these federally supported, secure online capabilities, financial institutions and stock trading companies (such as eTrade), as well as many healthcare institutions are heavily dependent upon transfer of privacy based data that supports extremely high system availability and data integrity. All of these systems must be compliant with federal guidance. If EQIP, JPAS and these others were certified and accredited and are in use today, then certainly a similar approach and technology could be taken when considering what risks are acceptable in an e-Voting system.

There is yet another consideration—even though there was a valiant effort made to document the risks associated with the current overseas voting system, and a hypothetical electronic system has been discussed, it is very important to make a direct comparison between the current threats to the existing system and the equivalent threats to a proposed electronic system, such as:

- The current paper-based system is susceptible to “man-in-the-middle” attacks with little or no mechanisms in place to detect or prevent them.
- Personal information (PII) can be stolen elsewhere and can be used to forge ballots.

[11] http://www.irs.gov/efile/article/0,,id=121477,00.html

- Physical signatures are less secure than properly implemented digital ones when it is considered that even though one can reliably verify that a physical signature is authentic, it is rarely done due to being prohibitively expensive to implement on this scale.
- This e-Voting system is no more, or less susceptible to DDoS or other types of attack than any other system; as such it could take advantage of the very well accepted countermeasures to these types of attacks. (Recently, DDoS attacks directed at WikiLeaks during the Cablegate scandal proved to be relatively ineffective, and WikiLeaks dealt with the attack quickly.)

While there are some serious security vulnerabilities that need to be addressed in terms of e-Voting, it is not impossible to implement a sufficiently secure e-Voting system, assuming that the cost of the countermeasures is acceptable.

Appendix A Security Requirements Traceability Matrix

FVAP_UOCAVA_SRTM_v16.xls

Appendix A can be found on pg. 706 of this document

Appendix B References

1. Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA), (as modified by the National Defense Authorization Act for FY 2005). http://www.fvap.gov/resources/media/uocavalaw.pdf

2. 107th U.S. Congress (October 29, 2002). "Help America Vote Act of 2002 (Pub. L. 107-252)." U.S. Government Printing Office.

3. National Institute of Standards and Technology Interagency Report: 7551, *A Threat Analysis on UOCAVA Voting Systems*, December 2008.

4. Draft National Institute of Standards and Technology Interagency Report 7682, *Information System Security Best Practices for UOCAVA Supporting Systems*, April 2010.

5. U.S. Election Assistance Commission (March 24, 2010). UOCAVA Pilot Program Testing Requirements, March 24, 2010. Accessed May 10, 2010 at http://www.eac.gov/program-areas/voting-systems/docs/requirements-03-24-10-uocava-pilot-program

6. EAC (2010, April 26). Report to Congress on EAC's Efforts to Establish Guidelines for Remote Electronic Absentee Voting Systems. Accessed May 10, 2010 at http://www.eac.gov/program-areas/voting-systems/docs/04-26-10-move-act-report-to-congress-final-congress/

7. M. Volkamer and R. Vogt. Basic set of security requirements for Online Voting Products. Common Criteria Protection Profile BSI-CC-PP-0037, Bundesamt für Sicherheit in der Informationstechnik, Bonn, April 2008.

8. Council of Europe. Legal, Operational, and Technical Standards for E-Voting. Recommendation Rec (2004)11, September 2004.

9. Federal Voting Assistance Program. *Secure Electronic Registration and Voting Experiment. Threat Risk Assessment- Phase 3*. March 23, 2004.

10. McConnell, Steven (2004), Code Complete (Second Edition), Microsoft Press.

11. Georgia Tech Information Security Center (2008). *Emerging Cyber Threats Report for 2009.* Accessed May 15, 2010 at http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf

12. US-CERT (2008, May 16). *Technical Cyber Security Alert TA08-137A: Debian/Ubuntu OpenSSL Random Number Generator Vulnerability*. Accessed May 15, 2010 at http://www.us-cert.gov/cas/techalerts/TA08-137A.html

13. Symantec (2010, April). *Symantec Global Internet Security Threat Report: Tends for 2009*. Accessed May 15, 2010 at http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf

14. Dierks, T. and Rescorla, E., *The TLS Protocol Version 1.2*, Internet Engineering Task Force, Request for Comment 5246, August 2008, http://tools.ietf.org/html/rfc5246

15. Atsushi Fujioka, Tatsuaki Okamoto, and Kazui Ohta. A Practical Secret Voting Scheme for Large Scale Elections. In Jennifer Seberry and Yuliang Zheng, editors, *Advances in Cryptology - AUSCRYPT '92*, volume 718 of *Lecture Notes in Computer Science*, pages 244--251, Berlin, 1993. Springer-Verlag.

16. Rene Peralta. Issues, non-issues and cryptographic tools for Internet-based voting. In *Secure Electronic Voting* (Boston, 2003), Dimitris A. Gritzalis, editor. Kluwer Academic Publishers, pp. 153-164.

17. Lorrie Faith Cranor and Ron K. Cytron, Sensus: A Security-Conscious Electronic Polling System for the Internet. *Proceedings of the Hawai`i International Conference on System Sciences* , January 7-10, 1997, Wailea, Hawaii, USA.

18. J. Benaloh and D. Tuinstra. Receipt-Free Secret-Ballot Elections. *Proceedings of the 26th ACM Symposium on Theory of Computing*. Montreal, PQ. May 1994. (New York, USA: ACM 1994), pp. 544—553.

19. Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. *A secure and optimally efficient multi-authority election scheme*. European Transactions on Telecommunications, 8:481-489, 1997.

20. Premiere Election Solutions (2008, August 19). *Product Advisory Notice*. Accessed May 15, 2010 at http://www.sos.state.oh.us/sos/upload/news/20081001c.pdf

21. Fink, R.A.; Sherman, A.T.; Carback, R.; , "TPM Meets DRE: Reducing the Trust Base for Electronic Voting Using Trusted Platform Modules," *Information Forensics and Security, IEEE Transactions on* , vol.4, no.4, pp.628-637, Dec. 2009.

22. Ben Adida, Olivier de Marneffe, Olivier Pereira, and Jean-Jacques Quisquater. Electing a University President Using Open-Audit Voting: Analysis of Real-World Use of Helios, In D. Jefferson, J.L. Hall, T. Moran, editor(s), *Electronic Voting Technology Workshop/Workshop on Trustworthy Elections*, Usenix, August 2009.

23. Nathanael Paul, Andrew S. Tanenbaum, "The Design of a Trustworthy Voting System," Computer Security Applications Conference, Annual, pp. 507-517, 2009 Annual Computer Security Applications Conference, 2009.

24. Common Criteria for Information Security Evaluation. Part 3: Security assurance components. Version 3.1, Rev. 3, July 2009.

25. Patrick Peterson, Henry Stern. "Botnets Gone Wild! Captured, Observed, Unraveled, Exterminated." Presented at RSA 2010, San Francisco, CA, March 1-5, 2010.

26. Testimony of Bob Carey, Director of FVAP. (2010) EAC Public Meeting, Dec. 3 2009. Accessed April 5, 2010 at http://www.eac.gov/public_meeting_12032010/

27. United States Postal Service (2007). *2007 Comprehensive Statement*. Accessed March 17, 2010 at http://www.usps.com/strategicplanning/cs07/chpt5_001.htm

28. Alvarez, R. Michael (2005, October 5). "Precinct Voting Denial of Service", *NIST Threats to Voting Systems Workshop*. Accessed March 17, 2010 at http://vote.nist.gov/threats/papers/precinct_dos.pdf

29. Davis, Joshua (2007, August 21). "Hackers Take Down the Most Wired Country in Europe" *Wired Magazine*. Accessed March 5, 2010 at http://www.wired.com/politics/security/magazine/15-09/ff_estonia

30. Markoff, John (2008, August 13). "Before the Gunfire, Cyberattacks" *The New York Times*. Accessed March 5, 2010 at http://www.nytimes.com/2008/08/13/technology/13cyber.html

31. Vixie, Paul, Sneeringer, Gerry, and Mark Schleifer (2002, November 24). Events of 21-Oct-2002." Accessed March 5, 2010 at http://d.root-servers.org/october21.txt

32. Internet Corporation for Assigned Names and Numbers. "Factsheet- Root server attack on 6 February 2007." Accessed March 5, 2010 at http://www.icann.org/announcements/factsheet-dns-attack-08mar07.pdf

33. Worthham, Jenna, and Andrew E. Kramer (2009, August 7) "Professor Main Target of Assault on Twitter" *The New York Times*. Accessed March 5, 2010 at http://www.nytimes.com/2009/08/08/technology/internet/08twitter.html

34. D. J. Bernstein and Eric Schenk (1996). *SYN Cookies*. 1996. Accessed May 15, 2010 at http://cr.yp.to/syncookies.html

35. Mell, Peter and Tim Grance (2009, October 7), *The NIST Definition of Cloud Computing.* Accessed March 2, 2010 at http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc

36. U.S. Election Assistance Commission (2006, December). *Election Crimes: An Initial Review and Recommendations for Future Study*. Accessed June 15, 2010 at http://www.eac.gov/assets/1/workflow_staging/Page/57.PDF

37. Gartner (2009, April 14). *Gartner Says Number of Phishing Attacks on U.S. Consumers Increased 40 Percent in 2008*. Accessed March 5, 2010 at http://www.gartner.com/it/page.jsp?id=936913

38. Cormac Herley and Dinei Florencio, A Profitless Endeavor: Phishing as Tragedy of the Commons, in *Proc. New Security Paradigms Workshop*, Association for Computing Machinery, Inc., September 2008.

39. Anti-Phishing Working Group (2009). *Phishing Activity Trends Report, 4th Quarter 2009*. Accessed March 5, 2010 at http://www.antiphishing.org/reports/apwg_report_Q4_2009.pdf

40. Office of Management and Budget (2006, June 23). *OMB Memo M06-16*. Accessed March 5, 2010 at http://www.whitehouse.gov/OMB/memoranda/fy2006/m06-16.pdf

41. McAfee Labs (2009). *2010 Threat Predictions*. Accessed April 13, 2010 at http://www.mcafee.com/us/local_content/white_papers/7985rpt_labs_threat_predict_1209_v2.pdf

42. Department of Defense. *Common Access Card.* Accessed March 5, 2010 at http://www.cac.mil/

43. National Institute of Standards and Technology (2009). *About Personal Identity Verification (PIV) of Federal Employees and Contractors.* Accessed March 5, 2010 at http://csrc.nist.gov/groups/SNS/piv/

44. Estonian National Electoral Committee. *Internet voting in Estonia*. Accessed March 5, 2010 at http://www.vvk.ee/public/dok/Internet_Voting_in_Estonia.pdf

45. Mozilla Foundation (2006, November 14). *Firefox 2 Phishing Protection Effectiveness Testing.* Accessed April 5, 2010 at http://www.mozilla.org/security/phishing-test.html

46. S. Egelman, L. Cranor, and J. Hong. You've Been Warned: An Empirical Study on the Effectiveness of Web Browser Phishing Warnings. CHI '08: Proceedings of the SIGCHI conference on Human Factors in Computing Systems. April 2008.

47. National Institute of Standards and Technology (2008, August). *The 2008 NIST Speaker Recognition Evaluation Results.* Accessed May 5, 2010 at http://www.itl.nist.gov/iad/mig/tests/sre/2008/official_results/index.html

Appendix C Glossary

This appendix provides definitions for security terminology used within or referenced in this document. The terms in the glossary are consistent with the terms used in the suite of FISMA-related security standards and guidelines developed by NIST. Unless otherwise stated, all terms used in this publication are also consistent with the definitions contained in the CNSS Instruction 4009, *National Information Assurance Glossary*.

Activities	An assessment object that includes specific protection related pursuits or actions supporting an information system that involve people (e.g., conducting system backup operations, monitoring network traffic).
Adequate Security **[OMB Circular A130, Appendix III]**	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost effective management, personnel, operational, and technical controls.
Advanced Persistent Threats	An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception), to generate opportunities to achieve its objectives, which are typically to establish and extend footholds within the information technology infrastructure of organizations for purposes of continually exfiltrating information, and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future. Moreover the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives.
Agency	See *Executive Agency*
Allocation	The process an organization employs to determine whether security controls are defined as system specific, hybrid, or common. The process an organization employs to assign security controls to specific information system components responsible for providing a particular security capability (e.g., router, server, remote sensor).
Application	A software program hosted by an information system.
Assessment	See *Security Control Assessment*.

Assessment Findings	Assessment results produced by the application of an assessment procedure to a security control or control enhancement to achieve an assessment objective; the execution of a determination statement within an assessment procedure by an assessor that results in either a *satisfied* or *other than satisfied* condition.
Assessment Method	One of three types of actions (i.e., examine, interview, test) taken by assessors in obtaining evidence during an assessment.
Assessment Object	The item (i.e., specifications, mechanisms, activities, individuals) upon which an assessment method is applied during an assessment.
Assessment Objective	A set of determination statements that expresses the desired outcome for the assessment of a security control or control enhancement.
Assessment Procedure	A set of assessment objectives and an associated set of assessment methods and assessment objects.
Assessor	See *Security Control Assessor*.
Assurance	The grounds for confidence that the set of intended security controls in an information system are effective in their application.
Assurance Case [Software Engineering Institute, Carnegie Mellon University]	A structured set of arguments and a body of evidence showing that an information system satisfies specific claims with respect to a given quality attribute.
Authentication [FIPS 200]	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See Authentication.
Authorization (to operate)	The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed upon set of security controls.
Authorization Boundary [NIST SP 800-37]	All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is

	connected.
Authorize Processing	See *Authorization*.
Authorizing Official (AO) **[NIST SP 800-37]**	A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
Authorizing Official Designated Representative [NIST SP 800-37]	An organizational official acting on behalf of an authorizing official in carrying out and coordinating the required activities associated with security authorization.
Availability [44 U.S.C., Sec. 3542]	Ensuring timely and reliable access to and use of information.
Basic Testing	A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. Also known as *Black Box Testing*.
Black Box Testing	See *Basic Testing*.
Categorization	The process of determining the security category (the restrictive label applied to classified or unclassified information to limit access) for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS 199 for other than national security systems.
Chief Information Officer (CIO) **[PL 104-106, Sec. 5125(b)]**	Agency official responsible for: 1) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; 2) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and 3) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.
Chief Information Security Officer	See Senior Agency Information Security Officer.
Common Control [NIST SP 800-37]	A security control that is inherited by one or more organizational information systems. See Security Control Inheritance.
Common Control Provider **[NIST SP 800-37, Rev. 1]**	An organizational official responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inherited by information

	systems).
Compensating Security Controls [NIST SP 800-53]	The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provide equivalent or comparable protection for an information system.
Comprehensive Testing	A test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. Also known as *White Box Testing*.
Computer Incident Response Team (CIRT)	Group of individuals usually consisting of Security Analysts organized to develop, recommend, and coordinate immediate mitigation actions for containment, eradication, and recovery resulting from computer security incidents. Also called a Computer Security Incident Response Team (CSIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability, or Cyber Incident Response Team).
Confidentiality [44 U.S.C., Sec. 3542]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Configuration Control (or Configuration Control) [CNSSI 4009]	Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.
Continuous Monitoring	Maintaining ongoing awareness to support organizational risk decisions. See *Information Security Continuous Monitoring*, *Risk Monitoring* and *Status Monitoring.*
Controlled Interface	A boundary with a set of mechanisms that enforces the security policies and controls the flow of information between interconnected information systems.
Controlled Unclassified Information	A categorical designation that refers to unclassified information that does not meet the standards for National Security classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the federal government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. Henceforth, the designation CUI replaces *Sensitive But Unclassified (SBU).*
Countermeasures [CNSSI 4009]	Actions, devices, procedures, techniques, or other measures that

	reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
Cross Domain Solution	A form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains.
Coverage	An attribute associated with an assessment method that addresses the scope or breadth of the assessment objects included in the assessment (e.g., types of objects to be assessed and the number of objects to be assessed by type). The values for the coverage attribute, hierarchically from less coverage to more coverage, are basic, focused, and comprehensive.
Data Loss	The exposure of proprietary, sensitive, or classified information through either data theft or data leakage.
Depth	An attribute associated with an assessment method that addresses the rigor and level of detail associated with the application of the method. The values for the depth attribute, hierarchically from less depth to more depth, are basic, focused, and comprehensive.
Domain [CNSSI 4009]	An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. See *Security Domain*.
Dynamic Subsystem	A subsystem that is not continually present during the execution phase of an information system. Service oriented architectures and cloud computing architectures are examples of architectures that employ dynamic subsystems.
Environment of Operation [NIST SP 800-37]	The physical surroundings in which an information system processes, stores, and transmits information.
Examine	A type of assessment method that is characterized by the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control effectiveness over time.
Executive Agency [41 U.S.C., Sec. 403]	An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.
External Information System	An information system or component of an information system

(or Component)	that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
External Information System Service	An information system service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
External Information System Service Provider	A provider of external information system services to an organization through a variety of consumer producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain arrangements.
Federal Agency	See *Executive Agency*.
Federal Information System **[40 U.S.C., Sec. 11331]**	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
Federal Enterprise Architecture **[FEA Program Management Office]**	A business-based framework for government-wide improvement developed by the Office of Management and Budget that is intended to facilitate efforts to transform the federal government to one that is citizen centered, results-oriented, and market-based.
Focused Testing	A test methodology that assumes some knowledge of the internal structure and implementation detail of the assessment object. Also known as *Gray Box Testing.*
Gray Box Testing	See *Focused Testing*.
High-Impact System [FIPS 200]	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high.
Hybrid Security Control **[NIST SP 800-53]**	A security control that is implemented in an information system in part as a common control and in part as a system-specific control. See *Common Control* and *System-Specific Security Control*.
Individuals	An assessment object that includes people applying specifications, mechanisms, or activities.

Industrial Control System	An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.
Information [FIPS 199]	An instance of an information type.
Information Owner [CNSSI 4009]	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information Resources [44 U.S.C., Sec. 3502]	Information and related resources, such as personnel, equipment, funds, and information technology.
Information Security [44 U.S.C., Sec. 3542]	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Security Risk	The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and /or information systems.
Information Security Architect	Individual, group, or organization responsible for ensuring that the information security requirements necessary to protect the organization's core missions and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting information systems supporting those missions and business processes.
Information Security Continuous Monitoring	Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.
Information Security Policy [CNSSI 4009]	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
Information Security Program Plan [NIST SP 800-53]	Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.

Information Steward	Individual or group that helps to ensure the careful and responsible management of federal information belonging to the nation as a whole, regardless of the entity or source that may have originated, created, or compiled the information. Information stewards provide maximum access to federal information to elements of the federal government and its customers, balanced by the obligation to protect the information in accordance with the provisions of FISMA and any associated security- related federal policies, directives, regulations, standards, and guidance.
Information System [44 U.S.C., Sec. 3502]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information System Boundary	See *Authorization Boundary*.
Information System Owner (or Program Manager)	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
Information System Security Engineer	Individual assigned responsibility for conducting information system security engineering activities.
Information System Security Engineering	Process that captures and refines information security requirements and ensures their integration into information technology component products and information systems through purposeful security design or configuration.
Information System related Security Risks	Information system-related security risks are those risks that arise through the loss of confidentiality, integrity, or availability of information or information systems and consider impacts to the organization (including assets, mission, functions, image, or reputation), individuals, other organizations, and the nation. See *Risk*.
Information System Security Officer (ISSO) [CNSSI 4009]	Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program.
Information Technology [40 U.S.C., Sec. 1401]	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the

	use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term *information technology* includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Information Type [FIPS 199]	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.
Integrity [44 U.S.C., Sec. 3542]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Interview	A type of assessment method that is characterized by the process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence, the results of which are used to support the determination of security control effectiveness over time.
Intrusion Detection and Prevention System (IDPS)	Software that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.
Joint Authorization	Security authorization involving multiple authorizing officials.
Low-Impact System [FIPS 200]	An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low.
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.
Management Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
Measures	All the output produced by automated tools (e.g., IDS/IPS, vulnerability scanners, audit record management tools, configuration management tools, asset management tools) as well as various information security program-related data (e.g., training and awareness data, information system authorization data, contingency planning and testing data, incident response

	data). Measures also include security assessment evidence from both automated and manual collection methods.
Mechanisms	An assessment object that includes specific protection-related items (e.g., hardware, software, or firmware) employed within or at the boundary of an information system.
Metrics	Tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance- related data.
Moderate- Impact System [FIPS 200]	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate, and no security objective is assigned a FIPS 199 potential impact value of high.
National Security Information	Information that has been determined pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.
National Security System [44 U.S.C., Sec. 3542]	Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—(i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
Net-Centric Architecture	A complex system of systems composed of subsystems and services that are part of a continuously evolving, complex community of people, devices, information and services interconnected by a network that enhances information sharing and collaboration. Subsystems and services may or may not be developed or owned by the same entity, and, in general, will not be continually present during the full life cycle of the system of systems. Examples of this architecture include service- oriented

	architectures and cloud computing architectures.
Operational Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an Information system that are primarily implemented and executed by people (as opposed to systems).
Organization [FIPS 200, Adapted]	An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency, or, as appropriate, any of its operational elements).
Organizational Information Security Continuous Monitoring	Ongoing monitoring sufficient to ensure and assure effectiveness of security controls related to systems, networks, and cyberspace, by assessing security control implementation and organizational security status in accordance with organizational risk tolerance – and within a reporting structure designed to make real time, data driven risk management decisions.
Patch Management	The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.
Penetration Testing	A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.
Plan of Action & Milestones (POA&M) [OMB Memorandum 02-01]	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Potential Impact [FIPS 199]	The loss of confidentiality, integrity, or availability could be expected to have: (i) a *limited* adverse effect (FIPS 199 low); (ii) a *serious* adverse effect (FIPS 199 moderate); or (iii) a *severe* or *catastrophic* adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals.
Reciprocity	Mutual agreement among participating organizations to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information.
Records	The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the

	complete set of information on particular items).
Risk [FIPS 200, Adapted]	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.[12]
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.
Risk Executive (Function) [NIST SP 800-37]	An individual or group within an organization that helps to ensure that: (i) security risk- related considerations for individual information systems, to include the authorization decisions, are viewed from an organization- wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and (ii) managing information system- related security risks is consistent across the organization, reflects organizational risk tolerance, and is considered along with organizational risks affecting mission/business success.
Risk Management	The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk- related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.
Risk Monitoring	Maintaining ongoing awareness of an organization's risk environment, risk management program, and associated activities to support risk decisions.
Risk Response	Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or

[12] Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation. Adverse impacts to the nation include, for example, compromises to information systems that support critical infrastructure applications or are paramount to government continuity of operations as defined by the Department of Homeland Security.

	reputation), organizational assets, individuals, other organizations, and the Nation.
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Safeguards [CNSSI 4009]	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with *Security Controls and Countermeasures*.
Security Authorization	See *Authorization*.
Security Categorization	The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS 199 for other than national security systems.
Security Controls [FIPS 199]	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Security Control Assessment	The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Security Control Assessor	The individual, group, or organization responsible for conducting a security control assessment.
Security Control Baseline [FIPS 200, Adapted]	One of the sets of minimum security controls defined for federal information systems in NIST Special Publication 800-53 and CNSS Instruction 1253.
Security Control Effectiveness	The measure of correctness of implementation (i.e., how consistently the control implementation complies with the security plan) and by how well the security plan meets organizational needs in accordance with current risk tolerance.
Security Control Enhancements	Statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control.
Security Control Inheritance	A situation in which an information system or application receives protection from security controls (or portions of security

	controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See *Common Control*.
Security Domain [CNSSI 4009]	A domain that implements a security policy and is administered by a single authority.
Security Impact Analysis	The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.
Security Management Dashboard [NIST SP 800-128]	A tool that consolidates and communicates information relevant to the organizational security posture in near-real time to security management stakeholders.
Security Objective [FIPS 199]	Confidentiality, integrity, or availability.
Security Plan	Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. See *System Security Plan* or *Information Security Program Plan*.
Security Policy [CNSSI 4009]	A set of criteria for the provision of security services.
Security Posture	The security status of an enterprise's networks, information, and systems based on IA resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes.
Security Requirements [FIPS 200]	Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
Senior (Agency) Information Security Officer (SISO) [44 U.S.C., Sec. 3544]	Official responsible for carrying out the Chief Information Officer responsibilities under the Federal Information Security Management Act (FISMA) and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers. Note: Organizations subordinate to federal agencies may use the term *Senior Information Security Officer* or *Chief Information Security Officer* to denote individuals filling positions with similar responsibilities to Senior Agency Information Security Officers.

Senior Information Security Officer	See *Senior Agency Information Security Officer*.
Specification	An assessment object that includes document-based artifacts (e.g., policies, procedures, plans, system security requirements, functional specifications, and architectural designs) associated with an information system.
Status Monitoring	Monitoring the information security metrics defined by the organization in the information security continuous monitoring strategy.
Subsystem	A major subdivision of an information system consisting of information, information technology, and personnel that performs one or more specific functions.
Supplementation (Assessment Procedures)	The process of adding assessment procedures or assessment details to assessment procedures in order to adequately meet the organization's risk management needs.
Supplementation (Security Controls)	The process of adding security controls or control enhancements to a security control baseline from NIST Special Publication 800-53 or CNSS Instruction 1253 in order to adequately meet the organization's risk management needs.
System	See *Information System*.
System Security Plan [NIST SP 800-18]	Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
System-Specific Security Control [NIST SP 800-37]	A security control for an information system that has not been designated as a common security control or the portion of a hybrid control that is to be implemented within an information system.
System Development Life Cycle (SDLC)	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.
Tailored Security Control Baseline	A set of security controls resulting from the application of tailoring guidance to the security control baseline. See *Tailoring.*
Tailoring [NIST SP 800-53, CNSSI 4009]	The process by which a security control baseline is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization defined parameters in the security controls via explicit assignment and selection statements.

Tailoring (Assessment Procedures)	The process by which assessment procedures defined in Special Publication 800-53A are adjusted, or scoped, to match the characteristics of the information system under assessment, providing organizations with the flexibility needed to meet specific organizational requirements and to avoid overly constrained assessment approaches.
Technical Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
Test	A type of assessment method that is characterized by the process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of security control effectiveness over time.
Threat [CNSSI 4009, Adapted]	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Threat Assessment [CNSSI 4009]	Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.
Threat Information	Information about types of attacks rather than specific threat actors.
Threat Source [FIPS 200]	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with Threat Agent.
Vulnerability [CNSSI 4009]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Vulnerability Assessment [CNSSI 4009]	Formal description and evaluation of the vulnerabilities in an information system.
White Box Testing	See *Comprehensive Testing*.

Appendix A Security Requirements Traceability Matrix

FVAP Security Requirement Traceability Matrix		Pilot Program Testing Requirements Security Gap Analysis	
	POC Name:	Michael Teribury (CALIBRE)	Jim Martin (CALIBRE)
	POC Phone:	(703) 588-8104	(703) 588-1179
	POC E-Mail:	michael.teribury.ctr@fvap.gov	James.Martin@calibresys.com
	Last Update: Jan. 31, 2011		

UOCAVA REQ. No. (1)	UOCAVA TEST REQ. (2)	TEST METHOD (3)	TEST ENTITY (4)	POTENTIAL IMPACT (5)
UOCAVA REQ. Number from "UOCAVA Pilot Program Test Requirements"	UOCAVA Req. from "UOCAVA Pilot Program Test Requirements"	UOCAVA Req. Test Method: Functional or Inspection	Test Entity: EAC, Manufacturer, or VSTL	NIST SP800-30: The next major step in measuring level of risk is to determine the adverse impact resulting from a successful threat exercise of a vulnerability. • System mission (e.g., the processes performed by the IT system) • System and data criticality (e.g., the system's value or importance to an organization) • System and data sensitivity. **Rated on a Low, Midium or High Impact** The following list provides a brief description of each security goal and the consequence (or impact) of its not being met: **Loss of Integrity.** System and data integrity refers to the requirement that information be protected from improper modification. **Loss of Availability.** If a mission-critical IT system is unavailable to its end users, the organization's mission may be affected. **Loss of Confidentiality.** System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data.

LEGEND: TEST METHOD A=ANALYSIS D=DEMONSTRATION I=INSPECTION T=TEST	FVAP SRTM DEFINITIONS & EXPLANATIONS										
										Risk	
VERIFICATION METHOD (6)	NIST Control No. (7)	IA Control Name (8)	ISO / IEC 17799 (9)	NIST SP800-26 (10)	GAO FISCAM (11)	DOD 8500.2 (12)	DCID 6/3 (13)	Related Control Guidance and References (14)	Mitagating IA Control (15)	Confidentiality	Integrity
The method for determining if the requirement that is being satisfactorally met. Includes Demonstration, Inspection or Test	NIST Special Publications IA Control Family	NIST Special Publications IA Control Family Name	International Standard Organization and International Electrotechnical Commission Reference Number	NIST SP800-26 Security Self-Assessment Guide Reference	Government Accounting Office Federal Information System Control Audit Manual	Depart of Defense 8500.1/2 IA guidance	Director of Central Intelligence Directive 6/3	Other federal, industy or international IA guidance applicable to this UOCAVA Pilot Program Testing Requirement	FVAP internal/external compensating control	See tab 3 CIA Triad	See tab 3 CIA Triad

See tab 3 CIA Triad	**Availability**		Gap Risk Analysis
This UOCAVA Pilot Program Testing Requirement has been mitigated through another security control	**Mitigated**		
See tab 3 CIA Triad	**Low**	Impact Rating	
See tab 3 CIA Triad	**Medium**		
See tab 3 CIA Triad	**High**		
UOCAVA Pilot Program Testing Requirement meets guidance	**Yes**	Compliant	
UOCAVA Pilot Program Testing Requirement does NOT meet guidance	**No**		
None of the seven guidance documents has a direct reference to this UOCAVA test requirement	**No available reference**		
This is a UOCAVA test requirement that is functional and does not have a security related component	**Functional Requirement**		

FVAP

FVAP Security Requirement Traceability Matrix

Pilot Program Testing Requirements Security Gap Analysis

Last Update: Jan. 31, 2011

LEGEND: TEST METHOD

A=ANALYSIS

D=DEMONSTRATION

I=INSPECTION

T=TEST

FVAP SRTM DEFINITIONS & EXPLANATIONS

Gap Risk Analysis

UOCAVA REQ. No. (1)	UOCAVA TEST REQ. (2)	TEST METHOD (3)	TEST ENTITY (4)	POTENTIAL IMPACT (5)	VERIFICATION METHOD (6)	NIST Control No. (7)	IA Control Name (8)	ISO / IEC 17799 (9)	NIST SP800-26 (10)	GAO FISCAM (11)	DOD 8500.2 (12)	DCID 6/3 (13)	Related Control Guidance and References (14)	Mitagating IA Control (15)	Risk: Confidentiality	Risk: Integrity	Risk: Availability	Mitigated	Impact Rating: Low	Impact Rating: Medium	Impact Rating: High	Compliant: Yes	Compliant: No	Compliant: No available reference	Functional Requirement	Reconciled in other documentation (Yes or No)	Identified Reference Documentation
4.3.1.2 Module testability	Each module SHALL have a specific function that can be tested and verified independently from the remainder of the code.	Inspection	Manufacturer	Relates to software integrity	I=INSPECTION	None	None	None	None	None	None	None	None	No reference documentation identified.		1				1				1	Yes	Found in Voting Systems Standards produced by the EAC. Other references relate to cryptographic modules within NIST Guidance and FIPS
4.3.1.3 Module size and identification	Modules SHALL be small and easily identifiable.	Inspection	Manufacturer	Relates to software integrity	I=INSPECTION	None	None	None	None	None	None	None	Nonme	N/A		1				1				1	1	Yes	Good coding practices woud dictate that modules be easily identified. The IEEE Software Engineering Body of Knowledge (SWEBOK) provides exception guidance and best practice knowledge that has been vetted by hundreds of industy experts. However, none of the additional reference documents speak to size of the modules.
4.7.2.7 Nullify freed pointers	If pointers are used, any pointer variables that remain within scope after the memory they point to is deallocated SHALL be set to null or marked as invalid (pursuant to the idiom of the programming language used) after the memory they point to is deallocated.	Inspection	Manufacturer	Integrity and Availability: Relates to software quality and best programming practices. No specific security control.	I=INSPECTION	None	None	None	None	None	None	None	None	None		1	1			1				1		No	Good coding practices woud dictate that all Null Pointers are reset. Additionally, there are specific requirements that agencies must follow when implementing cookies. See OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, available at: http://www.whitehouse.gov/omb/memoranda/m03-22.html.
4.7.2.11 Election integrity monitoring	The voting system SHALL proactively detect or prevent basic violations of election integrity (e.g., stuffing of the ballot box or the accumulation of negative votes) and alert an election official or administrator if such violations they occur.	Inspection	Manufacturer	N/A to IT Security capability	I=INSPECTION	None	None	None	None	None	None	None	None Identified	N/A		1				1				1	1	Yes	A requirement of 4.1.4 of The Voting Over the Internet Pilot Project 2001.
5.4.1.2 Cast vote integrity; storage	The integrity and authenticity of each individual cast vote SHALL be preserved by means of a digital signature during storage.	Functional	VSTL	Functional Requirement. Loss of Integrity.	T=TEST	None	None	None	None	None	None	None	Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), Draft March 2006.	N/A		1					1	1		1		Yes	Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), Draft March 2006.
5.4.1.3 Cast vote storage	Cast vote data SHALL NOT be permanently stored on the vote capture device.	Functional	VSTL	Functional Requirement. Loss of Integrity.	T=TEST	None	None	None	None	None	None	None	Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), Draft March 2006.	N/A		1					1			1	1	Yes	Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), Draft March 2006.
5.4.1.4 Electronic ballot box integrity	The integrity and authenticity of the electronic ballot box SHALL be protected by means of a digital signature.	Functional	VSTL	Functional Requirement. Loss of Integrity and/or Confidentiality.	T=TEST	None	None	None	None	None	None	None	Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), Draft March 2006.	N/A		1					1			1	1	Yes	Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), Draft March 2006.
6.2 Components from Third Parties	A manufacturer who does not manufacture all the components of its voting system, but instead procures components as standard commercial items for assembly and integration into a voting system, SHALL verify that the supplier manufacturers follow documented quality assurance procedures that are at least as stringent as those used internally by the voting system manufacturer.	Inspection	Manufacturer	loss of Integrity, availability and/or Confidentiality	I=INSPECTION	None	None	None	None	None	None	None	Nothing found in referencfed documentation. However, this may be referenced within another publication involving acquisitions.	N/A	1	1	1			1				1		Yes	The June 2010 Accessibility and Usability Consideration of Remote Voting Systems DRAFT Whitepaper prepared by NIST discusses 3rd party components. It specifically recommends that "design and test voting system components against standards and guidelines for interoperability and test all likely configurations."
6.3 Responsibility for Tests	Manufacturer SHALL be responsible for performing all quality assurance tests, acquiring and documenting test data, and providing test reports for examination by the VSTL as part of the national certification process. These reports SHALL also be provided to the purchaser upon request.	Inspection	Manufacturer	loss of Integrity or availability	I=INSPECTION	None	None	None	None	None	None	None	Nothing found in referencfed documentation. However, this may be referenced within another publication involving acquisitions.	N/A		1	1			1			1		No	No reference materials define responsibility for manufacturer to test systems.
7.5.2 Functional Configuration Audit (FCA)	The Functional Configuration Audit is conducted by the VSTL to verify that the voting system performs all the functions described in the system documentation. Manufacturers SHALL: a. Completely describe its procedures and related conventions used to support this audit for all voting system components; and b. Provide the following information to support this audit: c. Copies of all procedures used for module or unit testing, integration testing, and system testing; d. Copies of all test cases generated for each module and integration test, and sample ballot formats or other test cases used for system tests; and e. Records of all tests performed by the procedures listed above, including error corrections and retests.	Functional / Inspection	VSTL	Configuration/Testing	I=INSPECTION	None	None	None	None	None	None	None		N/A	1	1	1			1				1		Yes	Technical Guidelines Development Committee to the Election Assistance Commission: A reference was located in Chapter 4: Documentation and Design Reviews (Inspection) under section 4.1-A Applies to Voting Systems: An accredited test lab SHALL verify that the documentation submitted by the manufacturer in the TDP meets all the requirements applicable to the TDP, is sufficient to enable the inspections specified in this chapter, and is sufficient to enable tests specified.
8.2.1 TDP Implementation Statement	The TDP SHALL include an implementation statement.	Inspection	Manufacturer	Documentation	I=INSPECTION	None	None	None	None	None	None	None	None	N/A			1		1					1	1	Yes	This requirement is only mentioned in the VVSG Recommendations to the EAC in Chapter 2-10.
8.3.4.1 Hardwired and mechanical implementations of logic	For each non-COTS hardware component (e.g., an application-specific integrated circuit or a manufacturer-specific integration of smaller components), manufacturers SHALL provide complete design and logic specifications, such as Computer Aided Design and Hardware Description Language files.	Inspection	Manufacturer	Industrial controll logic could impact Confidentiality, Integrity and/or Availability.	I=INSPECTION	None	None	None	None	None	None	None	NIST SP800-53 Reference: An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.	Full Documentation of boarder logic and identification of all devices. Border logic should be minimized.	1	1	1				1			1		No	This falls under "border Logic" within the definition found in Appendix A of VVSG-0807. This does represent a significant threat to integrity and confidentiality.

8.3.4.2 Logic specifications for PLDs, FPGAs and PICs	For each Programmable Logic Device (PLD), Field-Programmable Gate Array (FPGA), or Peripheral Interface Controller (PIC) that is programmed with non- COTS logic, manufacturers SHALL provide complete logic specifications, such as Hardware Description Language files or source code.	Inspection	Manufacturer	Industrial controll logic could impact Confidentiality, Integrity and/or Availability.	I=INSPECTION	None	None	None	None	None	None	None	NIST SP800-53 Reference: An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.	Full Documentation of boarder logic and identification of all devices. Border logic should be minimized.	1	1	1			1				1			No	This falls under "border Logic" within the definition found in Appendix A of VVSG-0807. This does represent a significant threat to integrity and confidentiality.
8.4.5.3 Justify coding conventions	Manufacturers SHALL furnish evidence that the selected coding conventions are "published" and "credible" as specified in section 4.3.1.	Inspection	Manufacturer	Documentation normally contained within the System Security Plan under "robustness". Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	None	None	None	None	None	None	None	NIST SP800-137 References coding practices. DCID 6/3: 1.H.1 In the following pages, the term "good engineering practice" refers to the state of the engineering art for commercial systems that have equivalent problems and solutions; a good engineering practice by definition meets commercial requirements. These practices are usually part of the normal installation and operating procedures for systems. When placing security reliance on items that implement good engineering practice (such as commercial off-the shelf [COTS] software), the DAAs or their designees shall verify that the item(s) are set up properly and are operating as	Full Documentation of boarder logic and identification of all devices, manufacturer and design.	1	1	1			1				1			No	There is a discussion DRAFT posted on Dec. 1, 2006 regarding coding convention and logic verification that was prepared by NIST for the TGDC. This paper outlines specific requirements and guidance for coding best practices.
8.4.6.1 Application logic operating environment	Manufacturers SHALL describe or make reference to all operating environment factors that influence the design of application logic.	Inspection	Manufacturer	Documentation normally contained within the System Security Plan under "robustness". Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	None	None	None	None	None	None	None	None	PE-1 through PE-19 define environmental controls and related requirements.	1	1	1			1				1			Yes	NIST SP800-18 provides guidance for operating environements.
8.4.7.1 Hardware environment and constraints	Manufacturers SHALL identify and describe the hardware characteristics that influence the design of the application logic, such as: a. Logic and arithmetic capability of the processor; b. Memory read-write characteristics; c. External memory device characteristics; d. Peripheral device interface hardware; e. Data input/output device protocols; and f. Operator controls, indicators, and displays.	Inspection	Manufacturer	Documentation normally contained within the System Security Plan under "robustness". Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	None	None	None	None	None	None	None	None	PE-1 through PE-19 define environmental controls and related requirements.	1	1	1		1					1			Yes	NIST SP800-18 provides guidance for operating environements.
8.4.8.2 Compilers and assemblers	For systems containing compiled or assembled application logic, manufacturers SHALL identify the COTS compilers or assemblers used in the generation of executable code, and the specific versions thereof.	Inspection	Manufacturer	Documentation normally contained within the System Security Plan. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	None	None	None	None	None	None	None	None. Only references backups should provide for the protection of compilers.	None. Only references backups should provide for the protection of compilers.	1	1	1		1					1			Yes	The TGDC Recommendations from August, 2007 specify requirements. There are numerous IEEE standards and requirements defined that relate to compilers and assemblers.
8.4.8.3 Interpreters	For systems containing interpreted application logic, manufacturers SHALL specify the COTS runtime interpreter that SHALL be used to run this code, and the specific version thereof.	Inspection	Manufacturer	Documentation normally contained within the System Security Plan. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	None	None	None	None	None	None	None	None. Only references backups should provide for the protection of compilers.	None. Only references backups should provide for the protection of compilers.	1	1	1		1					1			No	No specific NIST or IEEE requirement located.
8.4.9.1 Application logic functional specification	Manufacturers SHALL provide a description of the operating modes of the system and of application logic capabilities to perform specific functions.	Inspection	Manufacturer	Documentation normally contained within the System Security Plan. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	None	None	None	None	None	None	None	None	None	1	1	1		1					1			No	No specific NIST or IEEE requirement located.
9.2.3.3 Traceability of procured software	The system description SHALL include a declaration that procured software items were obtained directly from the manufacturer or from a licensed dealer or distributor.	Inspection	Manufacturer	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTION	None	None	None	None	None	None	None			1	1	1			1				1			Yes	The DOE has a specific requirement for traceability of procured software.
9.4.5.1 Ballot count and vote total auditing	The system's user documentation SHALL fully specify a secure, transparent, workable and accurate process for producing all records necessary to verify the accuracy of the electronic tabulation result.	Inspection	Manufacturer	Loss of data Integrity	I=INSPECTION	None	None	None	None	None	None	None	None	None	1	1	1				1			1			Yes	IEEE P1583 speaks to voting system standards for election accuracy, and auditable results.
9.5.1.4 Election specific software identification	Manufacturers SHALL identify election specific software in the user documentation.	Inspection	Manufacturer	No securiyt impact	I=INSPECTION	None	None	None	None	None	None	None	None	Special denotation within the supplied documentation		1				1				1			No	This requirement is not clear as to its meaning. Now references available. However, this is a good security practice and should be followed.
9.5.1.7 Compiler installation prohibited	The software installation procedures used to install software on programmed devices of the system SHALL specify that no compilers SHALL be installed on the programmed device.	Inspection	Manufacturer	No direct security implication of this addition to the documentation. However, installation of compilers could impact confidentiality, availability and integrity.	I=INSPECTION	None	None	None	None	None	None	None	End user software is prohibited. However, no specific guidance on compilers within the referenced documetation.	None	1	1	1			1				1			No	Now references available. However, this is a good security practice and should be followed.
9.6.1.2 Setup inspection record generation	The setup inspection process SHALL describe the records that result from performing the setup inspection process.	Inspection	Manufacturer	This requirement could impact Confidentiality and/or integrity and availability.	I=INSPECTION	None	None	None	None	None	None	None	NIST SP800-100 States: In addition, developing a security requirements checklist based on the security requirements specified for the system during the conceptual, design, and implementation phases of the SDLC can be used to provide a 360-degree inspection of the system.	None	1	1	1			1				1			No	No specific reference documentation for this requirement.
9.6.1.12 Consumables quantity of vote capture device	Manufacturers SHALL provide a list of consumables associated with the vote capture device, including estimated number of usages per quantity of consumable.	Inspection	Manufacturer	No known security risk.	I=INSPECTION	None	None	None	None	None	None	None	No specific IA Control referenced.	None			1		1					1			No	This is specific to the voting system. NIST H143 makes a brief reference to consumables. However, this is a reasponable requirement. Media storage is a requirement of NIST guidance for DIACAP, and while it is not specifically mentioned, it would be reasonable to assume that it would fall under this guidance.
9.6.1.13 Consumable inspection procedure	Manufacturers SHALL provide the procedures to inspect the remaining amount of each consumable of the vote capture device.	Inspection	Manufacturer	No known security risk.	I=INSPECTION	None	None	None	None	None	None	None	No specific IA Control referenced.	None			1		1					1			No	This is specific to the voting system. NIST H143 makes a brief reference to consumables. However, this is a reasponable requirement. Media storage is a requirement of NIST guidance for DIACAP, and while it is not specifically mentioned, it would be reasonable to assume that it would fall under this guidance.
9.6.1.14 Calibration of vote capture device components nominal range	Manufacturers SHALL provide a list of components associated with the vote capture devices that require calibration and the nominal operating ranges for each component.	Inspection	Manufacturer	No known security risk.	I=INSPECTION	None	None	None	None	None	None	None	No specific IA Control referenced.	None		1				1				1			No	This should fall under the SSP guidance. However, this is election specific, and no other reference documentation was located.
9.6.1.15 Calibration of vote capture device components inspection procedure	Manufacturers SHALL provide the procedures to inspect the calibration of each component.	Inspection	Manufacturer	No known security risk.	I=INSPECTION	None	None	None	None	None	None	None	No specific IA Control referenced.	None		1				1				1			Yes	This is a HAVA requirement under Quality Assurance and Configuration Management.

FVAP Security Requirement Traceability Matrix

	UOCAVA Pilot Program Testing Requirements Security Gap Analysis	
POC Name:		
POC Phone:		
POC E-Mail:		
Last Update: Jan.31, 2011		

LEGEND: TEST METH

A=ANALYSIS

D=DEMONSTRATION

I=INSPECTION

T=TEST

UOCAVA REQ. No. (1)	UOCAVA TEST REQ. (2)	TEST METHOD (3)	TEST ENTITY (4)	POTENTIAL IMPACT (5)	VERIFICATION METHOD (6)	NIST Control No. (7)	IA Control Name (8)	ISO / IEC 17799 (9)	NIST SP800-26 (10)	GAO FISCAM (11)	DOD 8500.2 (12)	DCID 6/3 (13)	Related Control Guidance and References (14)	Mitagating IA Control (15)	Gap Risk Analysis: Risk: Confidentiality	Integrity	Availability	Mitigated	Impact Rating: Low	Medium	High	Compliant: Yes	No	No available reference	Functional Requirement	Recommended Technical or UOCAVA Requirement Change N/C = No Change
2.1.1.1 Component accuracy	Memory hardware, such as semiconductor devices and magnetic storage media, SHALL be accurate.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST & Demonstration	MP-1	Media Protection Policy and Procedures	10.1.1 10.7 15.1.1 15.1.3	8.2	---	PESP-1 DCAR-1	DCID: B.2.a Manual: 2.B.6.c(7) 8.B.2		N/A	1	1	1				1	1				N/C
2.1.1.2 Equipment design	The design of equipment in all voting systems SHALL provide for protection against mechanical, thermal, and electromagnetic stresses that impact voting system accuracy.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST & Demonstration	MP-2	Media Access	10.7.3	8.2.1; 8.2.2; 8.2.3; 8.2.6; 8.2.7	---	PEDI-1; PEPF-1	2.B.9.b(4); 4.B.1.a(1); 4.B.1.a(7)		N/A	1	1	1				1	1				N/C
2.1.1.3 Voting system accuracy	To ensure vote accuracy, all voting systems SHALL: a. Record the election contests, candidates, and issues exactly as defined by election officials; b. Record the appropriate options for casting and recording votes; c. Record each vote precisely as indicated by the voter and be able to produce an accurate report of all votes cast; d. Include control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) to demonstrate that the voting system has been designed for accuracy; and e. Provide software that monitors the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST & Demonstration	SI-10	Information Accuracy, Completeness, Validity, and Authenticity	10.7.3; 12.2.1; 12.2.2	---	---	---	7.B.2.h; 2.B.4.d		N/A	1	1	1				1	1				N/C
2.1.2 Environmental Range	All voting systems SHALL meet the accuracy requirements over manufacturer specified operating conditions and after storage under non-operating conditions.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST & Demonstration	None	None	None	None	None	None	None	FIPS 200; NIST Special Publications 800-12, 800-14, 800-66, 800-100. Protecting information residing on portable and mobile devices (e.g., employing cryptographic mechanisms to provide confidentiality and integrity protections during storage and while in transit when outside of controlled areas) is covered in the media protection family. Related security controls: MP-4, MP-5.	The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.	1	1	1				1				1	N/C
2.1.3.1 Election management system accuracy	Voting systems SHALL accurately record all election management data entered by the user, including election officials or their designees.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST & Demonstration	PL-3	System Security Plan Update	6.1	3.2.10; 5.2.1	SP-2.1	5.7.5	2.B.7.c(5)		Significant changes are defined in advance by the organization and identified in the configuration management process. NIST Special Publication 800-18 provides guidance on security plan updates.	1	1	1				1	1				N/C
2.1.3.2 Recording accuracy	For recording accuracy, all voting systems SHALL: a. Record every entry made by the user except where it violates voter privacy; b. Accurately interpret voter selection(s) and record them correctly to memory; c. Verify the correctness of detection of the user selections and the addition of the selections correctly to memory; d. Verify the correctness of detection of data entered directly by the user and the addition of the selections correctly to memory; and e. Preserve the integrity of election management data stored in memory against corruption by stray electromagnetic emissions, and internally generated spurious electrical signals.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST & Demonstration	SI-10	Information Accuracy, Completeness, Validity, and Authenticity	10.7.3; 12.2.1; 12.2.2	---	---	---	7.B.2.h; 2.B.4.d		N/A	1	1	1				1	1				N/C
2.1.4 Telecommunications Accuracy	The telecommunications components of all voting systems SHALL achieve a target error rate of no more than one in 10,000,000 ballot positions, with a maximum acceptable error rate in the test process of one in 500,000 ballot positions.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST & Demonstration	None	None	None	None	None	None	None			1	1	1				1	1				N/C
2.1.5.1 Simulators	If a simulator is used, it SHALL be verified independently of the voting system in order to produce ballots as specified for the accuracy testing.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. Inaccurate testing with potential false validation of results.	A=ANALYSIS	None	None	None	None	None	None	None			1	1	1				1				1	N/C
2.1.5.2 Ballots	Ballots used for accuracy testing SHALL include all the supported types (i.e., rotation, alternative languages) of contests and election types (primary, general).	Functional	VSTL	Functional requirement with no direct security impact.	T=TEST & Demonstration	None	None	None	None	None	None	None				1				1					1	N/C

2.1.6 Reporting Accuracy	Processing accuracy is defined as the ability of the voting system to process stored voting data. Processing includes all operations to consolidate voting data after the voting period has ended. The voting systems SHALL produce reports that are consistent, with no discrepancy among reports of voting data.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST & Demonstration	SI-7	Software and Information Integrity	12.2.1; 12.2.2; 12.2.4	11.2.1; 11.2.4	---	FVAP ECSD-2	UOCA 4.B.1.c(2); 5.B.1.a(3); 5.B.2.a(6)	ECAT-2 Audit Trail, Monitoring, Analysis and Reporting; ECTP-1 Audit Trail Protection SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY	N/A		1				1	1				N/C
2.2.1 Maximum Capacities	The manufacturer SHALL specify at least the following maximum operating capacities for the voting system (i.e. server, vote capture device, tabulation device, and communications links): Throughput, Memory, Transaction processing speed, and Election constraints: Number of jurisdictions Number of ballot styles per jurisdiction Number of contests per ballot style Number of candidates per contest Number of voted ballots	Functional	VSTL	No direct security impact	T=TEST & Demonstration	None	None	None	None	None	None	None		N/A					1			1			N/C
2.2.1.1 Capacity testing	The voting system SHALL achieve the maximum operating capacities stated by the manufacturer in section 2.2.1.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST & Demonstration	None	None	None	None	None	None	None			1	1	1			1			1		N/C
2.2.2 Operating Capacity notification	The voting system SHALL provide notice when any operating capacity is approaching its limit.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST & Demonstration	None	None	None	None	None	None	None			1	1	1			1			1		N/C
2.2.3 Simultaneous Transmissions	The voting system SHALL protect against the loss of votes due to simultaneous transmissions.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST & Demonstration	SC-8	Transmission Integrity	10.6.1; 10.8.1; 10.9.1	11.2.1; 11.2.4; 11.2.9; 16.2.14	AC-3.2	ECTM-1 Transmission Integrity Controls ECTM-2 Transmission Integrity Controls	5.B.3.a(11)	NIST Special Publication 800-52 provides guidance on protecting transmission integrity using Transport Layer Security (TLS). NIST Special Publication 800-77 provides guidance on protecting transmission integrity using IPsec. NIST Special Publication 800-81 provides guidance on Domain Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems. Others include: FIPS 198; NIST Special Publications 800-44, 800-45, 800-49, 800-52, 800-57, 800-54, 800-58, 800-66, 800-77, 800-81, 800-95, 800-97	N/A		1				1	1				N/C
2.3.1.1 Import the election definition	The voting system SHALL: a. Keep all data logically separated by, and accessible only to, the appropriate state and local jurisdictions; b. Provide the capability to import or manually enter ballot content, ballot instructions and election rules, including all required alternative language translations from each jurisdiction; c. Provide the capability for the each jurisdiction to verify that their election definition was imported accurately and completely; d. Support image files (e.g., jpg or gif) and/or a handwritten signature image on the ballot so that state seals, official signatures and other graphical ballot elements may be properly displayed; and e. Support multiple ballot styles per each local jurisdiction.	Inspection / Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST & Demonstration	PE-2 AC-5 SEPARATION OF DUTIES	Physical Access Authorizations	9.1.2; 9.1.6; 10.1.3; 10.6.1; 10.10.1	7.1.1; 7.1.2; 6.1.1; 6.1.2; 6.1.3; 15.2.1; 16.1.2; 17.1.5	AC-3.1; AC-3.2; SD-1.2	PECF-1 DCPA-1 Partitioning the Application ECCD-2 Changes to Data PRAS-2 Access to Information ECLP-1	4.B.1.a(1); 8.E; 2.A.1; 4.B.3.a(18)	The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.	Discretionary Access Control (DAC). A means of restricting access to an object (e.g., files, data entities) based on the identity and need-to-know of a subject (e.g., user, process) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) to any other subject (unless restrained by a mandatory access control).	1	1	1			1		1				Graphic formats are subject to corruption and remote code execution when malformed. Graphic file formats should be evaluated for potential risks and vulnerabilities. Appropriate Microsoft security bulletins and patches should be updated prior to elections.
2.3.1.2 Protect the election definition	The voting system SHALL provide a method to protect the election definition from unauthorized modification.	Functional	VSTL	A loss of integrity is the unauthorized modification or destruction of information.Information, the loss, misuse, or unauthorized access to or modification of, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of title 5, United States Code,	T=TEST & Demonstration	SI-7	Software and Information Integrity	12.2.1; 12.2.2; 12.2.4	11.2.1; 11.2.4	---	ECSD-2	4.B.1.c(2); 5.B.1.a(3); 5.B.2.a(6)		Information Security [44 U.S.C., Sec. 3542] The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.Integrity [44 U.S.C., Sec. 3542] Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	1	1				1	1				Does not specify how this is to be accomplished. No recommendation
2.3.2.1 Voting system test mode	The voting system SHALL provide a test mode to verify that the voting system is correctly installed, properly configured, and all functions are operating to support pre-election readiness testing for each jurisdiction.	Functional	VSTL	A system self test. NIST has SP800-126 Rev. 1 DRAFT Technical Specifications for the Security Content Automation Protocol (SCAP) that may relate testing requirements and specifications for security software flaws.	T=TEST & Demonstration	None	None	None	None	None	None	None		No specific findings for diagnostics or test mode analysis. Howvever, remote diagnostic is mentioned.	1	1	1			1			1		N/C
2.3.2.2 Test data segregation	The voting system SHALL provide the capability to zero-out or otherwise segregate test data from actual voting data.	Functional	VSTL	Functional test.	T=TEST & Demonstration	None	None	None	None	None	None	None			1	1	1			1			1		N/C
2.4.1.1 Accessing the ballot	The voting system SHALL: a. Present the correct ballot style to each voter; b. Allow the voting session to be canceled; and c. Prevent a voter from casting more than one ballot in the same election.	Functional	VSTL	Functional test.	T=TEST & Demonstration	None	None	None	None	None	None	None			1	1	1			1			1		N/C

2.4.2.1 Record voter selections	The voting system SHALL: a. Record the selection and non-selection of individual vote choices; b. Record the voter's selection of candidates whose names do not appear on the ballot, if permitted under state law, and record as many write-ins as the number of candidates the voter is allowed to select; c. Prohibit the voter from accessing or viewing any information on the display screen that has not been authorized and preprogrammed into the voting system (i.e., no potential for display of external information or linking to other information sources); d. Allow the voter to change a vote within a contest before advancing to the next contest; e. Provide unambiguous feedback regarding the voter's selection, such as displaying a checkmark beside the selected option or conspicuously changing its appearance; f. Indicate to the voter when no selection, or an insufficient number of selections, has been made for a contest (e.g., undervotes); g. Provide the voter the opportunity to correct the ballot for an undervote before the ballot is cast; h. Allow the voter, at the voter's choice, to submit an undervoted ballot without correction. i. Prevent the voter from making more than the allowable number of selections for any contest (e.g., overvotes); and j. In the event of a failure of the main power supply external to the voting system, provide the capability for any voter who is voting at the time to complete casting a ballot, allow for the successful shutdown of the voting system without loss or degradation of the voting and audit data, and allow voters to resume voting once the voting system has reverted to back-up power.	Functional	VSTL	Functional test.	D=DEMONSTRATION	None	None	None	None	None	None	None			1	1	1				1				1	N/C
2.4.2.2 Verify voter selections	The voting system SHALL: a. Produce a paper record each time the confirmation screen is displayed; b. Generate a paper record identifier. This SHALL be a random identifier that uniquely links the paper record with the cast vote record; c. Allow the voter to either cast the ballot or return to the vote selection process to make changes after reviewing the confirmation screen and paper record; and d. Prompt the voter to confirm his choices before casting the ballot, signifying to the voter that casting the ballot is irrevocable and directing the voter to confirm his intention to cast the ballot.	Functional	VSTL	Functional test.	D=DEMONSTRATION	None	None	None	None	None	None	None			1	1	1				1				1	N/C
2.4.2.3 Cast ballot	The voting system SHALL: a. Store all cast ballots in a random order; logically separated by, and only accessible to, the appropriate state/local jurisdictions; b. Notify the voter after the vote has been stored persistently that the ballot has been cast; c. Notify the voter that the ballot has not been cast successfully if it is not stored successfully, and provide clear instruction as to steps the voter should take to cast his ballot should this event occur; and d. Prohibit access to voted ballots until such time as state law allows for processing of absentee ballots.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	D=DEMONSTRATION	PE-2 AC-5 SEPARATION OF DUTIES	Physical Access Authorizations	9.1.2; 9.1.6; 10.1.3; 10.6.1; 10.10.1	7.1.1; 7.1.2; 6.1.1; 6.1.2; 6.1.3; 15.2.1; 16.1.2; 17.1.5	AC-3.1; AC-3.2; SD-1.2	PECF-1 DCPA-1 Partitioning the Application ECCD-2 Changes to Data PRAS-2 Access to Information ECLP-1	4.B.1.a(1); 8.E; 2.A.1; 4.B.3.a(18)	The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.	Discretionary Access Control (DAC). A means of restricting access to an object (e.g., files, data entities) based on the identity and need-to-know of a subject (e.g., user, process) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) to any other subject (unless restrained by a mandatory access control).	1	1	1				1	1					N/C
2.4.2.4.1 Absentee model	The cast ballot SHALL be linked to the voter's identity without violating the privacy of the voter.	Functional	VSTL	Privacy requirements and Audit Trail Requirements	D=DEMONSTRATION	None	None	None	None	None	None	None		National Institute of Standards and Technology Federal Information Processing Standards Publication 201-1, Personal Identity Verification of Federal Employees and Contractors, March 2006.	1	1					1				1	N/C
2.4.2.4.2 Early voting model	The cast ballot SHALL NOT be linked to the voter's identity.	Inspection	VSTL	Privacy requirements and Audit Trail Requirements	D=DEMONSTR	None	None	None	None	None	None	None			1						1				1	N/C
2.4.3.1 Link to voter	The voting system SHALL be capable of producing a cast vote record that does not contain any information that would link the record to the voter.	Functional	VSTL	Integrity: Privacy requirements and Audit Trail Requirements	D=DEMONSTR	None	None	None	None	None	None	None			1						1				1	N/C
2.4.3.2 Voting session records	The voting system SHALL NOT store any information related to the actions performed by the voter during the voting session.	Functional	VSTL	Integrity: Privacy requirements and Audit Trail Requirements	T=TEST & Demonstration	None	None	None	None	None	None	None			1	1					1				1	N/C
2.5.1.1 Seal and sign the electronic ballot box	The voting system SHALL seal and sign each jurisdiction's electronic ballot box, by means of a digital signature, to protect the integrity of its contents.	Functional	VSTL	Integrity: Privacy requirements and Audit Trail Requirements	T=TEST & Demonstration	None	None	None	None	None	None	None	NIST FIPS 140-2 validated cryptography (e.g., DoD PKI class 3 or 4 token) is used to implement encryption (e.g., AES, 3DES, DES, Skipjack), key exchange (e.g., FIPS 171), digital signature (e.g., DSA, RSA, ECDSA), and hash (e.g., SHA-1, SHA-256, SHA-384, SHA-512). Newer standards should be applied as they become available.	National Institute of Standards and Technology Federal Information Processing Standards Publication 186-2, Digital Signature Standard (DSS), January 2000. National Institute of Standards and Technology Federal Information Processing Standards Publication 186-3 (Draft), Digital Signature Standard (DSS), March 2006. National Institute of Standards and Technology Special Publication 800-89, Recommendation for Obtaining Assurances for Digital Signature Applications November 2006.		1					1				1	N/C
2.5.1.2 Electronic ballot box retrieval	The voting system SHALL allow each jurisdiction to retrieve its electronic ballot box.	Functional	VSTL	Functional Requirement	T=TEST & Demonstration	None	None	None	None	None	None	None			1	1	1				1				1	N/C
2.5.1.3 Electronic ballot box integrity check	The voting system SHALL perform an integrity check on the electronic ballot box verifying that it has not been tampered with or modified before opening.	Functional	VSTL	Functional Requirement	T=TEST & Demonstration	None	Physical Access Control	None	None	None	None	None			1	1	1				1				1	N/C
2.5.2.1 Tabulation device connectivity	The tabulation device SHALL be physically, electrically, and electromagnetically isolated from any other computer network.	Inspection	VSTL	Functional Requirement related to a loss of integrity	T=TEST & Demonstration	None	None	None	None	None	DCSP-1 EBBD-2	None	DCSP-1 Security Support Structure Partitioning: The security support structure is isolated by means of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform security functions. The security support structure maintains separate execution domains (e.g., address spaces) for each executing process. EBBD-2 Boundary Defense Boundary: defense mechanisms to include firewalls and network intrusion detection systems (IDS) are deployed at the enclave boundary to the wide area network, at layered or internal enclave boundaries and at key points in the network, as required. All Internet access is proxied through Internet access points that are under the management and control of the enclave and are isolated from other DoD information systems by physical or technical means.	Control: The organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facility. The organization controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.	1	1	1			1					1	N/C

2.5.2.2 Open ballot box	The tabulation device SHALL allow only an authorized entity to open the ballot box.	Functional	VSTL	Functional Requirement related to a loss of confidentiality due to physical access	T=TEST & Demonstration	PE-1 PE-2 PE-3 PE-6	Physical and Environmental Protection Policy and Procedures	15.1.1	7	PETN-1; DCAR-1	DCID: B.2.a; Manual: 2.B.4.e(5)	8.D	PECF-2 Access to Computing Facilities Only authorized personnel with appropriate clearances are granted physical access to computing facilities that process classified information.PECF-1 Access to Computing Facilities Only authorized personnel with a need-to-know are granted physical access to computing facilities that process sensitive information or unclassified information that has not been cleared for release. PEPF-1 Physical Protection of Facilities Every physical access point to facilities housing workstations that process or display sensitive information or unclassified information that has not been cleared for release is controlled during working hours and guarded or locked during non-work hours.	Control: The organization develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and issues appropriate authorization credentials. Designated officials within the organization review and approve the access list and authorization credentials [Assignment: organization-defined frequency, at least annually].	1	1	1				1	1				N/C
2.5.2.3.1 Adjudication	The tabulation device SHALL allow the designation of electronic ballots as “accepted” or “not accepted” by an authorized entity.	Functional	VSTL	Functional Requirement related to Operations and Integrity. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None				1						1			1	N/C
2.5.2.4 Ballot decryption	The tabulation device decryption process SHALL remove all layers of encryption and breaking all correlation between the voter and the ballot, producing a record that is in clear text.	Functional	VSTL	Functional Requirement related to Operations and Confidentiality. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None			1	1					1				1	N/C
2.5.2.5 Tabulation report format	The tabulation device SHALL have the capability to generate a tabulation report of voting results in an open and non-proprietary format.	Functional	VSTL	Functional Requirement related to Operations. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None			1	1					1				1	N/C
2.6.2.1 All records capable of being exported	The voting system SHALL provide the capability to export its electronic records in an open format, such as XML, or include a utility to export log data into a publicly documented format.	Functional	VSTL	Functional Requirement related to Operations. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None			1	1				1					1	N/C
2.6.2.2 Ballot images	The voting system SHALL have the capability to generate ballot images in a human readable format.	Functional	VSTL	Functional Requirement related to Operations. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None			1					1					1	Ballot Image format should meet security requirements in 2.3.1.1
2.6.2.3 Ballot image content	The voting system SHALL be capable of producing a ballot image that includes: a. Election title and date of election; b. Jurisdiction identifier; c. Ballot style; d. Paper record identifier; and e. For each contest and ballot question: i. The choice recorded, including write-ins; and ii. Information about each write-in.	Functional	VSTL	Functional Requirement related to Operations. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None			1	1					1				1	Ballot Image format should meet security requirements in 2.3.1.1
2.6.2.4 All records capable of being printed	The tabulation device SHALL provide the ability to produce printed forms of its electronic records. The printed forms SHALL retain all required information as specified for each record type other than digital signatures.	Functional	VSTL	Functional Requirement related to Operations. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None			1	1					1				1	N/C
2.6.2.5 Summary count record	The voting system SHALL produce a summary count record including the following: a. Time and date of summary record; and b. The following, both in total and broken down by ballot style and voting location: i. Number of received ballots ii. Number of counted ballots iii. Number of rejected electronic CVRs iv. Number of write-in votes v. Number of undervotes.	Functional	VSTL	Functional Requirement related to Operations. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None	None Identified	N/A		1					1				1	N/C
2.6.3.1 Paper record creation	Each vote capture device SHALL print a human readable paper record.	Functional	VSTL	Functional Requirement related to Operations. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None	None Identified	N/A		1				1					1	N/C
2.6.3.2 Paper record contents	Each paper record SHALL contain at least: a. Election title and date of election; b. Voting location; c. Jurisdiction identifier; d. Ballot style; e. Paper record identifier; and f. For each contest and ballot question: i. The recorded choice, including write-ins; and ii. Information about each write-in.	Inspection	VSTL	Functional Requirement related to Operations. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None	None Identified	N/A		1				1					1	N/C
2.6.3.3 Privacy	The vote capture device SHALL be capable of producing a paper record that does not contain any information that could link the record to the voter.	Inspection	VSTL	Functional Requirement related to Operations and Confidentiality. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None	None Identified	N/A	1	1					1				1	N/C
2.6.3.4 Multiple pages	When a single paper record spans multiple pages, each page SHALL include the voting location, ballot style, date of election, and page number and total number of the pages (e.g., page 1 of 4).	Functional	VSTL	Functional Requirement related to Operations. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None	None Identified	N/A		1				1					1	N/C
2.6.3.5 Machine-readable part contains same information as humanreadable part	If a non-human-readable encoding is used on the paper record, it SHALL contain the entirety of the human-readable information on the record.	Inspection	VSTL	Functional Requirement related to Operations and loosly to encryption. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None	None Identified	N/A	1	1				1					1	N/C
2.6.3.6 Format for paper record non-human-readable data	Any non-human-readable information on the paper record SHALL be presented in a non-proprietary format.	Inspection	VSTL	Functional Requirement related to Operations and loosly to encryption. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None	None Identified	N/A	1	1	1			1					1	N/C
2.6.3.7 Linking the electronic CVR to the paper record	The paper record SHALL: a. Contain the paper record identifier; and b. Identify whether the paper record represents the ballot that was cast.	Inspection	VSTL	Functional Requirement related to Operations. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None	None Identified	N/A		1				1					1	N/C
2.7.1.1 Network monitoring	The system server SHALL provide for system and network monitoring during the voting period.	Functional	VSTL	Functional Requirement related to Network Monitoring and Audit capability.	D=DEMONSTRATION	SI-4	Information System Monitoring Tools and Techniques	10.6.2; 10.10.1; 10.10.2; 10.10.4	11.2.5; 11.2.6	---	EBBD-1; EBVC-1; ECID-1	4.B.2.a(5)(b); 4.B.3.a(8)(b); 6.B.3.a(8)	Supplemental Guidance: The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system. The organization specifies which information system components carry out auditing activities.Control Enhancements: (1) The organization interconnects and configures individual intrusion detection tools into a systemwide intrusion detection system using common protocols. (2) The organization employs automated tools to support near-real-time analysis of events. (3) The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination. (4) The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.	Control: The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.	1	1	1			1		1				IDS/IPS systems SHALL be used that actively monitors, detects, and notifies administrators of any potential malicious activity.
2.7.1.2 Tool access	The system and network monitoring functionality SHALL only be accessible to authorized personnel from restricted consoles.	Functional	VSTL	Functional and Technical security requirement related to access controls and Roles and Responsibilities.	D=DEMONSTRATION	SI-4	PS-6	Access Agreements	6.1.5; 8.1.3	6.1.5; 6.2.2	SP-4.1	PRRB-1	E2.1.44. Privileged User. An authorized user who has access to system control, monitoring, or administration functions.PRRB-1 - Security Rules of Behavior or Acceptable Use Policy A set of rules that describe the IA operations of the DoD information system and clearly delineate IA responsibilities and expected behavior of all personnel is in place. The rules include the consequences of inconsistent behavior or non-compliance. Signed acknowledgement of the rules is a condition of access.	N/A	1	1	1			1		1				N/C
2.7.1.3 Tool privacy	System and network monitoring functionality SHALL NOT have the capability to compromise voter privacy or election integrity.	Functional	VSTL	Functional Requirement related to voter privacy and Integrity.	D=DEMONSTRATION	None	None	None	None	None	None	None		No reference documentation identified.	1	1					1			1	N/C
4.1.1 Acceptable Programming Language Constructs	Application logic SHALL be produced in a high-level programming language that has all of the following control constructs: a. Sequence; b. Loop with exit condition (e.g., for, while, and/or do-loops); c. If/Then/Else conditional; d. Case conditional; and e. Block-structured exception handling (e.g., try/throw/catch).	Inspection	Manufacturer	Integrity: Error Handling and system logic could jeopardize confidentiality, integrity and/or availability of the voting system.	I=INSPECTION	SI-11 SI-10	Error Handling Information Accuracy, Completeness, Validity, and Authenticity	12.2.1; 12.2.2; 12.2.3; 12.2.4; 10.7.3; 12.2.1; 12.2.2	---	---	---	2.B.4.d 7.B.2.h; 2.B.4.d	ERROR HANDLING: Control: The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries. NIST Special Publications 800-44, 800-57	N/A		1				1		1				N/C
4.2.1 Acceptable Coding Conventions	Application logic SHALL adhere to (or be based on) a published, credible set of coding rules, conventions or standards (herein simply called “coding conventions”) that enhance the workmanship, security, integrity, testability, and maintainability of applications.	Inspection	Manufacturer	Integrity: Relates to software integrity	I=INSPECTION	None	None	None	None	None	DCSQ-1 Software Quality	None	DCSQ-1 Software Quality: Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives.	N/A		1					1			1	N/C

4.2.1.1 Published	Coding conventions SHALL be considered published if they appear in publicly available media.	Inspection	Manufacturer	Integrity: Relates to software integrity	I=INSPECTION	None	None	None	None	None	DCSQ-1 Software Quality	None	DCSQ-1 Software Quality: Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives.	N/A		1				1				1	N/C
4.2.1.2 Credible	Coding conventions SHALL be considered credible if at least two different organizations independently decided to adopt them and made active use of them at some time within the three years before conformity assessment was first sought.	Inspection	Manufacturer	Relates to software integrity	I=INSPECTION	None	None	None	None	None	DCSQ-1 Software Quality	None	DCSQ-1 Software Quality: Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives.	N/A	1	1	1			1				1	N/C
4.3.1.2 Module testability	Each module SHALL have a specific function that can be tested and verified independently from the remainder of the code.	Inspection	Manufacturer	Relates to software integrity	I=INSPECTION	None	None	None	None	None	None	None	None	No reference documentation identified.		1			1				1	1	N/C
4.3.1.3 Module size and identification	Modules SHALL be small and easily identifiable.	Inspection	Manufacturer	Relates to software integrity	I=INSPECTION	None	None	None	None	None	None	None	Nonme	N/A		1			1				1	1	N/C
4.4.1.1 Exception handling	Application logic SHALL handle exceptions using block-structured exception handling constructs.	Inspection	Manufacturer	Relates to software integrity and quality	I=INSPECTION	SI-11 SI-10	Error Handling Information Accuracy, Completeness, Validity, and Authenticity	12.2.1; 12.2.2; 12.2.3; 12.2.4; 10.7.3; 12.2.1; 12.2.2	---	---	---	2.B.4.d 7.B.2.h; 2.B.4.d	ERROR HANDLING: Control: The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries. NIST Special Publications 800-44, 800-57	N/A		1	1			1		1				N/C
4.4.1.2 Legacy library units must be wrapped	If application logic makes use of any COTS or third-party logic callable units that do not throw exceptions when exceptional conditions occur, those callable units SHALL be wrapped in callable units that check for the relevant error conditions and translate them into exceptions, and the remainder of application logic SHALL use only the wrapped version.	Inspection	Manufacturer	Relates to software integrity, quality and error handling of third party software	I=INSPECTION	SI-7 SI-10	Software and Information Integrity	12.2.1; 12.2.2; 12.2.4	11.2.1; 11.2.4	---	ECSD-2	4.B.1.c(2); 5.B.1.a(3); 5.B.2.a(6)	SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY Control: The information system checks information for accuracy, completeness, validity, and authenticity. Supplemental Guidance: Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements.	N/A		1	1			1		1				N/C
4.4.2 Unstructured Control Flow is Prohibited	Application logic SHALL contain no unstructured control constructs.	Inspection	Manufacturer	Relates to software integrity and quality	I=INSPECTION	SI-11 SI-10	Error Handling Information Accuracy, Completeness, Validity, and Authenticity	12.2.1; 12.2.2; 12.2.3; 12.2.4; 10.7.3; 12.2.1; 12.2.2	---	---	---	2.B.4.d 7.B.2.h; 2.B.4.d	ERROR HANDLING: Control: The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries. NIST Special Publications 800-44, 800-57	N/A		1	1				1	1				N/C
4.4.2.1 Branching	Arbitrary branches (a.k.a. GoTos) SHALL NOT be allowed.	Inspection	Manufacturer	Relates to software integrity, quality and error handling of third party software	I=INSPECTION	SI-7 SI-10	Software and Information Integrity	12.2.1; 12.2.2; 12.2.4	11.2.1; 11.2.4	---	ECSD-2	4.B.1.c(2); 5.B.1.a(3); 5.B.2.a(6)	SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY Control: The information system checks information for accuracy, completeness, validity, and authenticity. Supplemental Guidance: Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements.	N/A		1	1			1		1				N/C
4.4.2.2 Intentional exceptions	Exceptions SHALL only be used for abnormal conditions. Exceptions SHALL NOT be used to redirect the flow of control in normal ("non-exceptional") conditions.	Inspection	Manufacturer	Relates to software integrity, quality and error handling of third party software	I=INSPECTION	SI-7 SI-10	Software and Information Integrity	12.2.1; 12.2.2; 12.2.4	11.2.1; 11.2.4	---	ECSD-2	4.B.1.c(2); 5.B.1.a(3); 5.B.2.a(6)	SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY Control: The information system checks information for accuracy, completeness, validity, and authenticity. Supplemental Guidance: Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin	N/A		1	1			1		1				N/C
4.4.2.3 Unstructured exception handling	Unstructured exception handling (e.g., On Error GoTo, setjmp/longjmp) SHALL NOT be allowed.	Inspection	Manufacturer	Relates to software integrity, quality and error handling of third party software	I=INSPECTION	SI-7 SI-10	Software and Information Integrity	12.2.1; 12.2.2; 12.2.4	11.2.1; 11.2.4	---	ECSD-2	4.B.1.c(2); 5.B.1.a(3); 5.B.2.a(6)	SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY Control: The information system checks information for accuracy, completeness, validity, and authenticity. Supplemental Guidance: Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements.	N/A	1	1	1			1		1				N/C
4.4.2.4 Separation of code and data	Application logic SHALL NOT compile or interpret configuration data or other input data as a programming language.	Inspection	Manufacturer	Relates to software integrity and quality	I=INSPECTION	SI-9	Information Input Restrictions	12.2.1; 12.2.2	---	SD-1	---	2.B.9.b(11)	SI-9 INFORMATION INPUT RESTRICTIONS Control: The organization restricts the capability to input information to the information system to authorized personnel. Supplemental Guidance: Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.	N/A		1	1			1		1				N/C
4.5.1 Header Comments	Application logic modules SHALL include header comments that provide at least the following information for each callable unit (e.g., function, method, operation, subroutine, procedure.): a. The purpose of the unit and how it works (if not obvious); b. A description of input parameters, outputs and return values, exceptions thrown, and side-effects; and c. Any protocols that must be observed (e.g., unit calling sequences).	Inspection	Manufacturer	Relates to software integrity and quality	I=INSPECTION	None	None	None	None	None	None	None	SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY Control: The information system checks information for accuracy, completeness, validity, and authenticity. Supplemental Guidance: Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements.	N/A		1	1			1		1			1	N/C
4.6.1 Code Coherency	Application logic SHALL conform to the following sub-requirements: a. Self-modifying code SHALL NOT be allowed; b. Application logic SHALL be free of race conditions, deadlocks, livelocks, and resource starvation; c. If compiled code is used, it SHALL only be compiled using a COTS compiler; and d. If interpreted code is used, it SHALL only be run under a specific, identified version of a COTS runtime interpreter.	Inspection	Manufacturer	Relates to mobile code and best coding practices to prevent error that could impact system availability, integrity and confidentiality. This also implies that code support IA robustness requirements.	I=INSPECTION	SI-7	Software and Information Integrity	12.2.1; 12.2.2; 12.2.4	11.2.1; 11.2.4	---	ECSD-2	4.B.1.c(2); 5.B.1.a(3); 5.B.2.a(6)	SI-7: SOFTWARE AND INFORMATION INTEGRITY Control: The information system detects and protects against unauthorized changes to software and information. Supplemental Guidance: The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts.	N/A		1	1			1		1				N/C
4.6.2 Prevent Tampering With Code	Programmed devices SHALL defend against replacement or modification of executable or interpreted code.	Inspection	Manufacturer	Relates to mobile code and best coding practices to prevent error that could impact system availability, integrity and confidentiality. This also implies that code support IA robustness requirements.	I=INSPECTION	SI-7	Software and Information Integrity	12.2.1; 12.2.2; 12.2.4	11.2.1; 11.2.4	---	ECSD-2	4.B.1.c(2); 5.B.1.a(3); 5.B.2.a(6)	SI-7: SOFTWARE AND INFORMATION INTEGRITY Control: The information system detects and protects against unauthorized changes to software and information. Supplemental Guidance: The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts. NIST Special Publication 800-83 provides guidance on detecting malware-based attacks through malicious code protection software.	N/A	1	1				1		1				N/C
4.6.3 Prevent Tampering With Data	The voting system SHALL prevent access to or manipulation of configuration data, vote data, or audit records.	Inspection	Manufacturer	Relates to audit capabilities and configuration management and data integrity.	I=INSPECTION	AU-1	Audit and Accountability Policy and Procedures	10.10; 15.1.1	17	---	ECAT-1; ECTB 1; DCAR-1	DCID: B.2.d; Manual:; 2.B.4.e(5); 2.B.2.a(4)		N/A		1	1			1		1				N/C

4.7.1.1 Validity check	Programmed devices SHALL check information inputs for completeness and validity.	Inspection	Manufacturer	Relates to the accuracy of information and integrity of data.	I=INSPECTION	SI-10	Information Accuracy, Completeness, Validity, and Authenticity	10.7.3; 12.2.1; 12.2.2	---	---	---	7.B.2.h; 2.B.4.d		N/A		1				1	1				N/C
4.7.1.2 Defend against garbage input	Programmed devices SHALL ensure that incomplete or invalid inputs do not lead to irreversible error.	Inspection	Manufacturer	Functional requirement and Error handling	I=INSPECTION	SI-11	Error Handling	12.2.1; 12.2.2; 12.2.3; 12.2.4	---	---	---	2.B.4.d	SI-11: ERROR HANDLING Control: The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries. Supplemental Guidance: The structure and content of error messages are carefully considered by the organization. Error messages are revealed only to authorized personnel. Error messages generated by the information system provide timely and useful information without revealing potentially harmful information that could be used by adversaries. Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) are not listed in error logs or associated administrative messages. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.	N/A		1	1			1		1				N/C
4.7.2.1 Error checking	Application logic that is vulnerable to the following types of errors SHALL check for these errors at run time and respond defensively (as specified by Requirement 4.7.2.8) when they occur: Out-of-bounds accesses of arrays or strings (includes buffers used to move data); Stack overflow errors; CPU-level exceptions such as address and bus errors, dividing by zero, and the like; Variables that are not appropriately handled when out of expected boundaries; Numeric overflows; and Known programming language specific vulnerabilities.	Inspection	Manufacturer	Relates to the accuracy of information and integrity of data.	I=INSPECTION	SI-11	Error Handling	12.2.1; 12.2.2; 12.2.3; 12.2.4	---	---	---	2.B.4.d	SI-11: ERROR HANDLING Control: The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries. Supplemental Guidance: The structure and content of error messages are carefully considered by the organization. Error messages are revealed only to authorized personnel. Error messages generated by the information system provide timely and useful information without revealing potentially harmful information that could be used by adversaries. Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) are not listed in error logs or associated administrative messages. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.	N/A		1	1			1		1				N/C
4.7.2.2 Range checking of indices	If the application logic uses arrays, vectors, character sequences, strings or any analogous data structures, and the programming language does not provide automatic run-time range checking of the indices, the indices SHALL be rangedchecked on every access.	Inspection	Manufacturer	Relates to the accuracy of information and integrity of data.	I=INSPECTION	SI-11	Error Handling	12.2.1; 12.2.2; 12.2.3; 12.2.4	---	---	---	2.B.4.d	SI-11: ERROR HANDLING Control: The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries. Supplemental Guidance: The structure and content of error messages are carefully considered by the organization. Error messages are revealed only to authorized personnel. Error messages generated by the information system provide timely and useful information without revealing potentially harmful information that could be used by adversaries. Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) are not listed in error logs or associated administrative messages. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.	N/A		1					1	1				N/C
4.7.2.3 Stack overflows	If stack overflow does not automatically result in an exception, the application logic SHALL explicitly check for and prevent stack overflow.	Inspection	Manufacturer	Relates to the accuracy of information and integrity of data.	I=INSPECTION	SI-11	Error Handling	12.2.1; 12.2.2; 12.2.3; 12.2.4	---	---	---	2.B.4.d	SI-11: ERROR HANDLING Control: The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries. Supplemental Guidance: The structure and content of error messages are carefully considered by the organization. Error messages are revealed only to authorized personnel. Error messages generated by the information system provide timely and useful information without revealing potentially harmful information that could be used by adversaries. Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) are not listed in error logs or associated administrative messages. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.	N/A		1					1	1				N/C
4.7.2.4 CPU traps	The application logic SHALL implement such handlers as are needed to detect and respond to CPU-level exceptions including address and bus errors and dividing by zero.	Inspection	Manufacturer	Relates to the accuracy of information and integrity of data.	I=INSPECTION	SI-11	Error Handling	12.2.1; 12.2.2; 12.2.3; 12.2.4	---	---	---	2.B.4.d	SI-11: ERROR HANDLING Control: The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries. Supplemental Guidance: The structure and content of error messages are carefully considered by the organization. Error messages are revealed only to authorized personnel. Error messages generated by the information system provide timely and useful information without revealing potentially harmful information that could be used by adversaries. Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) are not listed in error logs or associated administrative messages. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.	N/A		1	1			1		1				N/C
4.7.2.5 Garbage input parameters	All scalar or enumerated type parameters whose valid ranges as used in a callable unit (e.g., function, method, operation, subroutine, procedure.) do not cover the entire ranges of their declared data types SHALL be range-checked on entry to the unit.	Inspection	Manufacturer	Relates to error handling and data range values.	I=INSPECTION	SI-10	Information Accuracy, Completeness, Validity, and Authenticity	10.7.3; 12.2.1; 12.2.2	---	---	---	7.B.2.h; 2.B.4.d	SI-10: INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY Control: The information system checks information for accuracy, completeness, validity, and authenticity. Supplemental Guidance: Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements.	N/A		1				1		1				N/C
4.7.2.6 Numeric overflows	If the programming language does not provide automatic run-time detection of numeric overflow, all arithmetic operations that could potentially overflow the relevant data type SHALL be checked for overflow.	Inspection	Manufacturer	Integrity: Relates to error handling and data range values.	I=INSPECTION	SI-10	Information Accuracy, Completeness, Validity, and Authenticity	10.7.3; 12.2.1; 12.2.2	---	---	---	7.B.2.h; 2.B.4.d	SI-10: INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY Control: The information system checks information for accuracy, completeness, validity, and authenticity. Supplemental Guidance: Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements.	N/A		1				1		1				N/C
4.7.2.7 Nullify freed pointers	If pointers are used, any pointer variables that remain within scope after the memory they point to is deallocated SHALL be set to null or marked as invalid (pursuant to the idiom of the programming language used) after the memory they point to is deallocated.	Inspection	Manufacturer	Integrity and Availability: Relates to software quality and best programming practices. No specific security control.	I=INSPECTION	None	None	None	None	None	None	None	None	None		1	1			1				1		N/C
4.7.2.8 React to errors detected	The detection of any of the errors enumerated in Requirement 4.7.2.1 SHALL be treated as a complete failure of the callable unit in which the error was detected. An appropriate exception SHALL be thrown and control SHALL pass out of the unit forthwith.	Inspection	Manufacturer	Integrity and Availability: Relates to software quality and best programming practices. No specific security control.	I=INSPECTION	SI-11	Error Handling	12.2.1; 12.2.2; 12.2.3; 12.2.4	---	---	---	2.B.4.d	None	N/A		1	1			1					1	N/C

											FVAP	UOCA													
4.7.2.9 Do not disable error checks	Error checks detailed in Requirement 4.7.2.1 SHALL remain active in production code.	Inspection	Manufacturer	Integrity and Availability: Relates to error handling and data range values.	I=INSPECTION	SI-10	Information Accuracy, Completeness, Validity, and Authenticity	10.7.3; 12.2.1; 12.2.2	---	---	---	7.B.2.h; 2.B.4.d	SI-10: INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY Control: The information system checks information for accuracy, completeness, validity, and authenticity. Supplemental Guidance: Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements.	N/A		1	1			1		1				N/C
4.7.2.10 Roles authorized to respond to errors	Exceptions resulting from failed error checks or CPU-level exceptions SHALL require intervention by an election official or administrator before voting can continue.	Inspection	Manufacturer	Integrity: Relates to error handling and data range values.	I=INSPECTION	SI-11 SI-10	Error Handling	12.2.1; 12.2.2; 12.2.3; 12.2.4	---	---	---	2.B.4.d		N/A		1	1			1		1				N/C
4.7.2.11 Election integrity monitoring	The voting system SHALL proactively detect or prevent basic violations of election integrity (e.g., stuffing of the ballot box or the accumulation of negative votes) and alert an election official or administrator if such violations they occur.	Inspection	Manufacturer	N/A to IT Security capability	I=INSPECTION	None	None	None	None	None	None	None	None Identified	N/A		1				1				1	1	N/C
4.8.1.1 Resuming normal operations	All voting systems SHALL be capable of resuming normal operations following the correction of a failure in any device.	Functional	Manufacturer	Integrity: Relates to system error handling and recovery of operations.	I=INSPECTION	CP-10	Information System Recovery and Reconstitution	14.1.4	9.2.8	SC-2.1	COTR-1; ECND-1	4.B.1.a(4); 6.B.1.a(1); 6.B.2.a(3)(d)	CP-10: INFORMATION SYSTEM RECOVERY AND RECONSTITUTION Control: The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure. Supplemental Guidance: Information system recovery and reconstitution to a known secure state means that all system parameters (either default or organization-established) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded, and the system is fully tested.	N/A		1					1	1				N/C
4.8.1.2 Failures not compromise voting or audit data	Exceptions and system recovery SHALL be handled in a manner that protects the integrity of all recorded votes and audit log information.	Functional	Manufacturer	Integrity: Relates to error handling and data range values.	I=INSPECTION	SI-11 SI-10	Error Handling	12.2.1; 12.2.2; 12.2.3; 12.2.4	---	---	---	2.B.4.d		N/A		1				1		1				N/C
4.8.1.3 Device survive component failure	All vote capture device SHALL be capable of resuming normal operation following the correction of a failure in any component (e.g., memory, CPU, printer) provided that catastrophic electrical or mechanical damage has not occurred.	Functional	Manufacturer	Integrity: Relates to system error handling and recovery of operations.	I=INSPECTION	SI-11 SI-10	Error Handling	12.2.1; 12.2.2; 12.2.3; 12.2.4	---	---	---	2.B.4.d	CP-10: INFORMATION SYSTEM RECOVERY AND RECONSTITUTION Control: The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure. Supplemental Guidance: Information system recovery and reconstitution to a known secure state means that all system parameters (either default or organization-established) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded, and the system is fully tested.	N/A	1	1	1			1		1				N/C
4.8.2 Controlled Recovery	Error conditions SHALL be corrected in a controlled fashion so that voting system status may be restored to the initial state existing before the error occurred.	Functional	Manufacturer	Integrity: Relates to system error handling and recovery of operations.	I=INSPECTION	SI-11 SI-10	Error Handling	12.2.1; 12.2.2; 12.2.3; 12.2.4	---	---	---	2.B.4.d	CP-10: INFORMATION SYSTEM RECOVERY AND RECONSTITUTION Control: The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure. Supplemental Guidance: Information system recovery and reconstitution to a known secure state means that all system parameters (either default or organization-established) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded, and the system is fully tested.	N/A		1	1			1		1				N/C
4.8.2.1 Nested error conditions	Nested error conditions that are corrected without reset, restart, reboot, or shutdown of the vote capture device SHALL be corrected in a controlled sequence so that voting system status may be restored to the initial state existing before the first error occurred.	Functional	Manufacturer	Integrity: Relates to system error handling and recovery of operations.	I=INSPECTION	SI-11 SI-10	Error Handling	12.2.1; 12.2.2; 12.2.3; 12.2.4	---	---	---	2.B.4.d	CP-10: INFORMATION SYSTEM RECOVERY AND RECONSTITUTION Control: The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure. Supplemental Guidance: Information system recovery and reconstitution to a known secure state means that all system parameters (either default or organization-established) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded, and the system is fully tested.	N/A		1	1			1		1				N/C
4.8.2.2 Reset CPU error states	CPU-level exceptions that are corrected without reset, restart, reboot, or shutdown of the vote capture device SHALL be handled in a manner that restores the CPU to a normal state and allows the voting system to log the event and recover as with a software-level exception.	Functional	Manufacturer	Integrity and Availability: Relates to system error handling and recovery of operations.	D=DEMONSTRATION	SI-11	Error Handling	12.2.1; 12.2.2; 12.2.3; 12.2.4	---	---	---	2.B.4.d	SI-11 ERROR HANDLING Control: The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries.	N/A		1	1			1		1				
4.8.3 Restore Device to Checkpoints	When recovering from non-catastrophic failure or from any error or malfunction that is within the operator's ability to correct, the voting system SHALL restore the device to the operating condition existing immediately prior to the error or failure, without loss or corruption of voting data previously stored in the device.	Functional	Manufacturer	Integrity: Relates to system error handling and recovery of operations.	I=INSPECTION	SI-11 SI-10	Error Handling	12.2.1; 12.2.2; 12.2.3; 12.2.4	---	---	---	2.B.4.d	CP-10: INFORMATION SYSTEM RECOVERY AND RECONSTITUTION Control: The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure. Supplemental Guidance: Information system recovery and reconstitution to a known secure state means that all system parameters (either default or organization-established) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded, and the system is fully tested.	N/A		1	1				1	1				N/C
4.9.1.1 Review source versus manufacturer specifications	The test lab SHALL assess the extent to which the application logic adheres to the specifications made in its design documentation.	Inspection	VSTL	Functional and ST&E Requirement defined ins Appendix F of the NIST SP800-53A Rev.2	I=INSPECTION	SI-9	Information Input Restrictions	12.2.1; 12.2.2	---	SD-1	---	2.B.9.b(11)	SI-9 INFORMATION INPUT RESTRICTIONS Control: The organization restricts the capability to input information to the information system to authorized personnel. Supplemental Guidance: Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.	N/A		1	1			1		1				N/C
4.9.1.2 Review source versus coding conventions	The test lab SHALL assess the extent to which the application logic adheres to the published, credible coding conventions chosen by the manufacturer.	Inspection	VSTL	Integrity and Availability: Application programming best practices.	I=INSPECTION	SI-9	Information Input Restrictions	12.2.1; 12.2.2	---	SD-1	---	2.B.9.b(11)	SI-9 INFORMATION INPUT RESTRICTIONS Control: The organization restricts the capability to input information to the information system to authorized personnel. Supplemental Guidance: Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.	N/A		1	1			1		1				N/C
4.9.1.3 Review source versus workmanship requirements	The test lab SHALL assess the extent to which the application logic adheres to the requirements of Section 4 Software.	Inspection	VSTL	Application programming best practices.	I=INSPECTION	SI-9	Information Input Restrictions	12.2.1; 12.2.2	---	SD-1	---	2.B.9.b(11)	SI-9 INFORMATION INPUT RESTRICTIONS Control: The organization restricts the capability to input information to the information system to authorized personnel. Supplemental Guidance: Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.	N/A		1	1			1		1				Recommend the use of application scvanning tools such as Lumension, Nessus or Fortify for source code analysis.
4.9.1.4 Efficacy of built-in self-tests	The test lab SHALL verify the efficacy of built-in measurement, self-test, and diagnostic capabilities.	Inspection	VSTL	Relates to Self test and diagnostic capability. Impacts Confedentiality, Integrity and Availability	I=INSPECTION	SI-6	Security Functionality Verification	---	11.2.1; 11.2.2	SS-2.2	DCSS-1	4.B.1.c(2); 5.B.2.b(2)	SI-6: SECURITY FUNCTIONALITY VERIFICATION Control: The information system verifies the correct operation of security functions [Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every [Assignment: organization-defined time-period]] and [Selection (one or more): notifies system administrator, shuts the system down, restarts the system] when anomalies are discovered. Supplemental Guidance: The need to verify security functionality applies to all security functions. For those security functions that are not able to execute automated self-tests, the organization either implements compensating security controls or explicitly accepts the risk of not performing the verification as required.	N/A		1	1			1		1				Recommend the use of application scvanning tools such as Lumension, Nessus or Fortify for source code analysis.

4.9.2.1 Security control source code review	The test lab SHALL analyze the source code of the security controls to assess whether they function correctly and cannot be bypassed.	Inspection	VSTL	Loss of Integrity, availability and/or Confidentiality	I=INSPECTION	RA-5	Vulnerability Scanning	12.6.1	10.3.2; 14.2.1	---	FVAP ECMT-1; VIVM-1	UOCA 4.B.3.a(8)(b); 4.B.3.b(6)(b); 9.B.4.e	RA-5: VULNERABILITY SCANNING Control: The organization scans for vulnerabilities in the information system [Assignment: organization-defined frequency] or when significant new vulnerabilities potentially affecting the system are identified and reported. Supplemental Guidance: Vulnerability scanning is conducted using appropriate scanning tools and techniques. The organization trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques. Vulnerability scans are scheduled and/or random in accordance with organizational policy and assessment of risk. The information obtained from the vulnerability scanning process is freely shared with appropriate personnel throughout the organization to help eliminate similar vulnerabilities in other information systems. Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools for applications, source code reviews, static analysis of source code). NIST Special Publication 800-42 provides guidance on network security testing. NIST Special Publication 800-40 (Version 2) provides guidance on patch and vulnerability management.	N/A	1	1	1				1	1				Recommend the use of application scvanning tools such as Lumension, Nessus or Fortify for source code analysis.
5.1.1.1 Definition of roles	The voting system SHALL allow the definition of personnel roles with segregated duties and responsibilities on critical processes to prevent a single person from compromising the integrity of the system.	Functional	VSTL	Relates to the separation of duties, least priviledge and account management. Roles and Responsibilities are discussed in many different sections. Impacts include: Loss of Confidentiality, Availability and Integrity. This is an operating system functional requirement to meet the above.	D=DEMONSTRATION	AC-2	Account Management	6.2.2; 6.2.3; 8.3.3; 11.2.1; 11.2.2; 11.2.4; 11.7.2	6.1.8; 15.1.1; 15.1.4; 15.1.5; 15.1.8; 15.2.2; 16.1.3; 16.1.5; 16.2.12	AC-2.1; AC-2.2; AC-3.2; SP-4.1	IAAC-1	4.B.2.a(3)	ECLP-1 Least Privilege Access procedures enforce the principles of separation of duties and "least privilege." Access to privileged accounts is limited to privileged users. Use of privileged accounts is limited to privileged functions; that is, privileged users use non-privileged accounts for all non-privileged functions. This control is in addition to an appropriate security clearance and need-to-know authorization.	N/A	1	1	1			1		1				Recommend the use of application scvanning tools such as Lumension, Nessus or Fortify for source code analysis.
5.1.1.2 Access to election data	The voting system SHALL ensure that only authorized roles, groups, or individuals have access to election data.	Functional	VSTL	Relates to the separation of duties, least priviledge and account management. Roles and Responsibilities are discussed in many different sections. Impacts include: Loss of Confidentiality, Availability and Integrity. This is an operating system functional requirement to meet the above.	D=DEMONSTRATION	AC-2	Account Management	6.2.2; 6.2.3; 8.3.3; 11.2.1; 11.2.2; 11.2.4; 11.7.2	6.1.8; 15.1.1; 15.1.4; 15.1.5; 15.1.8; 15.2.2; 16.1.3; 16.1.5; 16.2.12	AC-2.1; AC-2.2; AC-3.2; SP-4.1	IAAC-1	4.B.2.a(3)		N/A	1	1	1			1		1				Recommend the use of application scvanning tools such as Lumension, Nessus or Fortify for source code analysis.
5.1.1.3 Separation of duties	The voting system SHALL require at least two persons from a predefined group for validating the election configuration information, accessing the cast vote records, and starting the tabulation process.	Functional	VSTL	Integrity & Confidentiality: Procedual requirement to prevent collusion	D=DEMONSTRATION	AC-4	Information Flow Enforcement	10.6.2; 11.4.5; 11.4.6; 11.4.7	---	---	EBBD-1; EBBD-2	4.B.3.a(3); 7.B.3.g	AC-5 SEPARATION OF DUTIES Control: The information system enforces separation of duties through assigned access authorizations. Supplemental Guidance: The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.	N/A	1	1	1			1		1				N/C
5.1.2.1 Identity verification	The voting system SHALL identify and authenticate each person to whom access is granted, and the specific functions and data to which each person holds authorized access.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	D=DEMONSTRATION	AC-7	Unsuccessful Login Attempts	11.5.1	15.1.14	AC-3.2	ECLO-1	4.B.2.a(17)(c)-(d)		N/A	1	1	1				1	1				N/C
5.1.2.2 Access control configuration	The voting system SHALL allow the administrator group or role to configure permissions and functionality for each identity, group or role to include account and group/role creation, modification, and deletion.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	D=DEMONSTRATION	AC-5	Separation of Duties	10.1.3; 10.6.1; 10.10.1	6.1.1; 6.1.2; 6.1.3; 15.2.1; 16.1.2; 17.1.5	AC-3.2; SD-1.2	ECLP-1	2.A.1; 4.B.3.a(18)	AC-5 SEPARATION OF DUTIES Control: The information system enforces separation of duties through assigned access authorizations. Supplemental Guidance: The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.	N/A	1	1	1			1	1	1				N/C
5.1.2.3 Default access control configuration	The voting system's default access control permissions SHALL implement the least privileged role or group needed.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	D=DEMONSTRATION	AC-5	Separation of Duties	10.1.3; 10.6.1; 10.10.1	6.1.1; 6.1.2; 6.1.3; 15.2.1; 16.1.2; 17.1.5	AC-3.2; SD-1.2	ECLP-1	2.A.1; 4.B.3.a(18)	AC-5 SEPARATION OF DUTIES Control: The information system enforces separation of duties through assigned access authorizations. Supplemental Guidance: The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.	N/A	1	1	1			1		1				N/C
5.1.2.4 Escalation prevention	The voting system SHALL prevent a lower-privilege process from modifying a higher-privilege process.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	D=DEMONSTRATION	AC-5	Separation of Duties	10.1.3; 10.6.1; 10.10.1	6.1.1; 6.1.2; 6.1.3; 15.2.1; 16.1.2; 17.1.5	AC-3.2; SD-1.2	ECLP-1	2.A.1; 4.B.3.a(18)	SC-3 SECURITY FUNCTION ISOLATION Control: The information system isolates security functions from nonsecurity functions. Supplemental Guidance: The information system isolates security functions from nonsecurity functions by means of partitions, domains, etc., including control of access to and integrity of, the hardware, software, and firmware that perform those security functions. The information system maintains a separate execution domain (e.g., address space) for each executing process.	N/A	1	1	1			1		1				N/C

5.1.2.5 Operating system privileged account restriction	The voting system SHALL NOT require its execution as an operating system privileged account and SHALL NOT require the use of an operating system privileged account for its operation.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	D=DEMONSTRATION	AC-5	Separation of Duties	10.1.3; 10.6.1; 10.10.1	6.1.1; 6.1.2; 6.1.3; 15.2.1; 16.1.2; 17.1.5	AC-3.2; SD-1.2	ECLP-1	2.A.1; 4.B.3.a(18)	AC-5 SEPARATION OF DUTIES Control: The information system enforces separation of duties through assigned access authorizations. Supplemental Guidance: The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.	N/A	1	1	1				1	1				N/C
5.1.2.6 Logging of account	The voting system SHALL log the identification of all personnel accessing or attempting to access the voting system to the system event log.	Functional	VSTL	Forensic auditing abilities. Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	D=DEMONSTRATION	AU-2	Auditable Events	10.10.1	17.1.1; 17.1.2; 17.1.4	---	ECAR-3	4.B.2.a(4)(d)	ECAR-3 Audit Record Content Audit records include: - User ID. - Successful and unsuccessful attempts to access security files - Date and time of the event. - Type of event. - Success or failure of event. - Successful and unsuccessful logons. - Denial of access resulting from excessive number of logon attempts. - Blocking or blacklisting a user ID, terminal or access port, and the reason for the action. - Activities that might modify, bypass, or negate safeguards controlled by the system. - Data required to audit the possible use of covert channel mechanisms. - Privileged activities and other system-level access. - Starting and ending time for access to the system. - Security relevant actions associated with periods processing or the changing of security labels or categories of information.	N/A	1	1	1			1		1				
5.1.2.7 Monitoring voting system access	The voting system SHALL provide tools for monitoring access to the system. These tools SHALL provide specific users real time display of persons accessing the system as well as reports from logs.	Functional	VSTL	Forensic auditing abilities. Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	D=DEMONSTRATION	AU-2	Auditable Events	10.10.1	17.1.1; 17.1.2; 17.1.4	---	ECAR-3	4.B.2.a(4)(d)	ECAR-3 Audit Record Content Audit records include: - User ID. - Successful and unsuccessful attempts to access security files - Date and time of the event. - Type of event. - Success or failure of event. - Successful and unsuccessful logons. - Denial of access resulting from excessive number of logon attempts. - Blocking or blacklisting a user ID, terminal or access port, and the reason for the action. - Activities that might modify, bypass, or negate safeguards controlled by the system. - Data required to audit the possible use of covert channel mechanisms. - Privileged activities and other system-level access. - Starting and ending time for access to the system. - Security relevant actions associated with periods processing or the changing of security labels or categories of information.	N/A	1	1	1			1	1	1				N/C
5.1.2.8 Login failures	The vote capture devices at the kiosk locations and the central server SHALL have the capability to restrict access to the voting system after a preset number of login failures. a. The lockout threshold SHALL be configurable by appropriate administrators/operators. b. The voting system SHALL log the event. c. The voting system SHALL immediately send a notification to appropriate administrators/operators of the event. d. The voting system SHALL provide a mechanism for the appropriate administrators/operators to reactivate the account after appropriate confirmation.	Functional	VSTL	Forensic auditing abilities. Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	D=DEMONSTRATION	AU-2	Auditable Events	10.10.1	17.1.1; 17.1.2; 17.1.4	---	ECAR-3	4.B.2.a(4)(d)	ECAR-3 Audit Record Content Audit records include: - User ID. - Successful and unsuccessful attempts to access security files - Date and time of the event. - Type of event. - Success or failure of event. - Successful and unsuccessful logons. - Denial of access resulting from excessive number of logon attempts. - Blocking or blacklisting a user ID, terminal or access port, and the reason for the action. - Activities that might modify, bypass, or negate safeguards controlled by the system. - Data required to audit the possible use of covert channel mechanisms. - Privileged activities and other system-level access. - Starting and ending time for access to the system. - Security relevant actions associated with periods processing or the changing of security labels or categories of information.	N/A	1	1	1			1		1				N/C
5.1.2.9 Account lockout logging	The voting system SHALL log a notification when any account has been locked out.	Functional	VSTL	Forensic auditing abilities. Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	D=DEMONSTRATION	AU-2	Auditable Events	10.10.1	17.1.1; 17.1.2; 17.1.4	---	ECAR-3	4.B.2.a(4)(d)	ECAR-3 Audit Record Content Audit records include: - User ID. - Successful and unsuccessful attempts to access security files - Date and time of the event. - Type of event. - Success or failure of event. - Successful and unsuccessful logons. - Denial of access resulting from excessive number of logon attempts. - Blocking or blacklisting a user ID, terminal or access port, and the reason for the action. - Activities that might modify, bypass, or negate safeguards controlled by the system. - Data required to audit the possible use of covert channel mechanisms. - Privileged activities and other system-level access. - Starting and ending time for access to the system. - Security relevant actions associated with periods processing or the changing of security labels or categories of information.	N/A		1	1			1		1				N/C
5.1.2.10 Session time-out	Authenticated sessions on critical processes SHALL have an inactivity time-out control that will require personnel re-authentication when reached. This time-out SHALL be implemented for administration and monitor consoles on all voting system devices.	Functional	VSTL	Forensic auditing abilities. Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	D=DEMONSTRATION	AU-2	Auditable Events	10.10.1	17.1.1; 17.1.2; 17.1.4	---	ECAR-3	4.B.2.a(4)(d)	ECAR-3 Audit Record Content Audit records include: - User ID. - Successful and unsuccessful attempts to access security files - Date and time of the event. - Type of event. - Success or failure of event. - Successful and unsuccessful logons. - Denial of access resulting from excessive number of logon attempts. - Blocking or blacklisting a user ID, terminal or access port, and the reason for the action. - Activities that might modify, bypass, or negate safeguards controlled by the system. - Data required to audit the possible use of covert channel mechanisms. - Privileged activities and other system-level access. - Starting and ending time for access to the system. - Security relevant actions associated with periods processing or the changing of security labels or categories of information.	N/A	1					1		1				N/C
5.1.2.11 Screen lock	Authenticated sessions on critical processes SHALL have a screen-lock functionality that can be manually invoked.	Functional	VSTL	Access control and session lock: Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	D=DEMONSTRATION	AC-11	Session Lock	11.3.2	16.1.4	AC-3.2	PESL-1	4.B.1.a(5)	SESSION LOCK Control: The information system prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures. Supplemental Guidance: Users can directly initiate session lock mechanisms. A session lock is not a substitute for logging out of the information system. Organization-defined time periods of inactivity comply with federal policy; for example, in accordance with OMB Memorandum 06-16, the organization-defined time period is no greater than thirty minutes for remote access and portable devices.	N/A		1	1			1		1				

5.2.1.1 Strength of authentication	Authentication mechanisms supported by the voting system SHALL support authentication strength of at least 1/1,000,000.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	D=DEMONSTRATION	IA-2	User Identification and Authentication	11.2.3; 11.4.2; 11.5.2	15.1	---	FVAP IAIA-1	UOCA 4.B.2.a(7)	USER IDENTIFICATION AND AUTHENTICATION Control: The information system uniquely identifies and authenticates users (or processes acting on behalf of users). Supplemental Guidance: Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance security control AC-14. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. NIST Special Publication 800-63 provides guidance on remote electronic authentication including strength of authentication mechanisms.	N/A	1	1	1			1		1				Recommendation: The use of three factor authentication method to include biometric. Cross-over error rates (CER) and Equal Error Rates should be known.
5.2.1.2 Minimum authentication methods	The voting system SHALL authenticate users per the minimum authentication methods outlined below.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	D=DEMONSTRATION	IA-2	User Identification and Authentication	11.2.3; 11.4.2; 11.5.2	15.1	---	IAIA-1	4.B.2.a(7)	IA-2 USER IDENTIFICATION AND AUTHENTICATION Control: The information system uniquely identifies and authenticates users (or processes acting on behalf of users). Supplemental Guidance: Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance security control AC-14. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof.	N/A	1	1	1			1		1				N/C
5.2.1.3 Multiple authentication mechanisms	The voting system SHALL provide multiple authentication methods to support multi-factor authentication.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	D=DEMONSTRATION	IA-2	User Identification and Authentication	11.2.3; 11.4.2; 11.5.2	15.1	---	IAIA-1	4.B.2.a(7)	IA-2 USER IDENTIFICATION AND AUTHENTICATION Control: The information system uniquely identifies and authenticates users (or processes acting on behalf of users). Supplemental Guidance: Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance security control AC-14. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof.	N/A	1	1	1				1	1				N/C
5.2.1.4 Secure storage of authentication data	When private or secret authentication data is stored by the voting system, it SHALL be protected to ensure that the confidentiality and integrity of the data are not violated.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	D=DEMONSTRATION	IA-5	Authenticator Management	11.5.2; 11.5.3	15.1.6; 15.1.7; 15.1.9; 15.1.10; 15.1.11; 15.1.12; 15.1.13; 16.1.3; 16.2.3	AC-3.2	IAKM-1; IATS-1; IAIA-2	4.B.2.a(7); 4.B.3.a(11)	IA-5 AUTHENTICATOR MANAGEMENT Control: The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically. Supplemental Guidance: Information system authenticators include, for example, tokens, PKI certificates, biometrics, passwords, and key cards. Users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. For password-based authentication, the information system: (i) protects passwords from unauthorized disclosure and modification when stored and transmitted; (ii) prohibits passwords from being displayed when entered; (iii) enforces password minimum and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified number of generations.	N/A	1	1				1		1				N/C
5.2.1.5 Password reset	The voting system SHALL provide a mechanism to reset a password if it is forgotten, in accordance with the system access/security policy.	Functional	VSTL	Passwords, tokens, or other devices are used to identify and authenticate users. Loss of Integrity, Availability and Confidentiality	D=DEMONSTRATION	IA-5	Authenticator Management	11.5.2; 11.5.3	15.1.6; 15.1.7; 15.1.9; 15.1.10; 15.1.11; 15.1.12; 15.1.13; 16.1.3; 16.2.3	AC-3.2	IAKM-1; IATS-1	4.B.2.a(7); 4.B.3.a(11)	Related security controls: AC-14, AC-17	N/A	1	1				1		1				N/C
5.2.1.6 Password strength configuration	The voting system SHALL allow the administrator group or role to specify password strength for all accounts including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters per NIST 800 63 Electronic Authentication Guideline Standards.	Functional	VSTL	Medium Impact. Administrave roles and responsibilities	D=DEMONSTRATION	IA-5	Authenticator Management	11.5.2; 11.5.3	15.1.6; 15.1.7; 15.1.9; 15.1.10; 15.1.11; 15.1.12; 15.1.13; 16.1.3; 16.2.3	AC-3.2	IAKM-1; IATS-1	4.B.2.a(7); 4.B.3.a(11)	IA-5 AUTHENTICATOR MANAGEMENT Control: The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.	N/A	1	1				1		1				N/C
5.2.1.7 Password history configuration	The voting system SHALL enforce password histories and allow the administrator to configure the history length when passwords are stored by the system. 1 NIST Special Publication 800-57	Functional	VSTL	Medium: Impacts Integrity.	D=DEMONSTRATION	IA-5	Authenticator Management	11.5.2; 11.5.3	15.1.6; 15.1.7; 15.1.9; 15.1.10; 15.1.11; 15.1.12; 15.1.13; 16.1.3; 16.2.3	AC-3.2	IAKM-1; IATS-1	4.B.2.a(7); 4.B.3.a(11)	IA-5 AUTHENTICATOR MANAGEMENT Control: The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.	N/A	1	1				1		1				N/C
5.2.1.8 Account information password restriction	The voting system SHALL ensure that the user name is not used in the password.	Functional	VSTL	Medium: Impacts Integrity.	D=DEMONSTRATION	IA-5	Authenticator Management	11.5.2; 11.5.3	15.1.6; 15.1.7; 15.1.9; 15.1.10; 15.1.11; 15.1.12; 15.1.13; 16.1.3; 16.2.3	AC-3.2	IAKM-1; IATS-1	4.B.2.a(7); 4.B.3.a(11)	IA-5 AUTHENTICATOR MANAGEMENT Control: The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.	N/A	1	1				1		1				N/C
5.2.1.9 Automated password expiration	The voting system SHALL provide a means to automatically expire passwords.	Functional	VSTL	Medium: Impacts Integrity.	D=DEMONSTRATION	IA-5	Authenticator Management	11.5.2; 11.5.3	15.1.6; 15.1.7; 15.1.9; 15.1.10; 15.1.11; 15.1.12; 15.1.13; 16.1.3; 16.2.3	AC-3.2	IAKM-1; IATS-1	4.B.2.a(7); 4.B.3.a(11)	IA-5 AUTHENTICATOR MANAGEMENT Control: The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.	N/A	1	1				1		1				Passwords SHALL conform to DoD DIACAP minimum standards.
5.2.1.10 Device authentication	The voting system servers and vote capture devices SHALL identify and authenticate one another using NIST - approved cryptographic authentication methods at the 112 bits of security.	Functional	VSTL	Medium: Impacts Integrity.	D=DEMONSTRATION	CA-3	Information System Connections	10.6.2; 10.9.1; 11.4.5; 11.4.6; 11.4.7	1.1.1; 3.2.9; 4.1.8; 12.2.3	CC-2.1	DCID-1; EBCR-1; EBRU-1; EBPW-1; ECIC-1	9.B.3; 9.D.3.c	CA-3 INFORMATION SYSTEM CONNECTIONS Control: The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis.	N/A	1	1					1	1				N/C

5.2.1.11 Network authentication	Remote voting location site Virtual Private Network (VPN) connections (i.e., vote capture devices) to voting servers SHALL be authenticated using strong mutual cryptographic authentication at the 112 bits of security.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	D=DEMONSTRATION	AC-17	Remote Access	11.4.2; 11.4.3; 11.4.4	16.2.4; 16.2.8	AC-3.2	EBRP-1; EBRU-1	4.B.1.a(1)(b); 4.B.3.a(11); 7.D.2.e	FISCAM Requirement FIPS 200 Requirements AC-17 REMOTE ACCESS Control: The organization authorizes, monitors, and controls all methods of remote access to the information system. Supplemental Guidance: Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless. Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology). NIST Special Publication 800-63 provides guidance on remote electronic authentication. If the federal Personal Identity Verification (PIV) credential is used as an identification token where cryptographic token-based access control is employed, the access control system conforms to the requirements of FIPS	N/A	1	1	1			1	1				N/C
5.2.1.12 Message authentication	Message authentication SHALL be used for applications to protect the integrity of the message content using a schema with 112 bits of security.	Functional	VSTL	Loss of Integrity.	D=DEMONSTRATION	SC-23	Session Authenticity	---	---	---	---	---	SC-23 SESSION AUTHENTICITY Control: The information system provides mechanisms to protect the authenticity of communications sessions. Supplemental Guidance: This control focuses on communications protection at the session, versus packet, level. The intent of this control is to implement session-level protection where needed (e.g., in service-oriented architectures providing web-based services). NIST Special Publication 800-52 provides guidance on the use of transport layer security (TLS) mechanisms. NIST Special Publication 800-77 provides guidance on the deployment of IPsec virtual private networks (VPNs) and other methods of protecting communications sessions. NIST Special Publication 800-95 provides guidance on secure web services.	N/A		1				1		1				Recommend that authentication schema SHALL be commensurate with the highest level technically feasable. This requirement will constantly change as new schema's become available.
5.2.1.13 Message authentication mechanisms	IPsec, SSL, or TLS and MAC mechanisms SHALL all be configured to be compliant with FIPS 140-2 using approved algorithm suites and protocols.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	D=DEMONSTRATION	AC-17	Remote Access	11.4.2; 11.4.3; 11.4.4	16.2.4; 16.2.8	AC-3.2	EBRP-1; EBRU-1	4.B.1.a(1)(b); 4.B.3.a(11); 7.D.2.e	AC-17 REMOTE ACCESS Control: The organization authorizes, monitors, and controls all methods of remote access to the information system. Supplemental Guidance: Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless. Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology). NIST Special Publication 800-63 provides guidance on remote electronic authentication. If the federal Personal Identity Verification (PIV) credential is used as an identification token where cryptographic token-based access control is employed, the access control system conforms to the requirements of FIPS 201 and NIST Special Publications 800-73 and 800-78. NIST Special Publication 800-77 provides guidance on IPsec-based virtual private networks. Related security control: IA-2.	N/A	1	1	1			1	1				N/C
5.3.1.1 Cryptographic functionality	All cryptographic functionality SHALL be implemented using NIST-approved cryptographic algorithms/schemas, or use published and credible cryptographic algorithms/schemas/protocols.	Inspection	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST	IA-7	Cryptographic Module; Authentication	---	16.1.7	---	16.1.7	---	National Institute of Standards and Technology Special Publication 800-29, A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2, June 2001. IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION Control: The information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module. Supplemental Guidance: The applicable federal standard for authentication to a cryptographic module is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect, and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval.	N/A	1	1	1			1	1				N/C
5.3.1.2 Required security strength	Cryptographic algorithms and schemas SHALL be implemented with a security strength equivalent to at least 112 bits of security to protect sensitive voting information and election records.	Inspection	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST	IA-7	Cryptographic Module; Authentication	---	16.1.7	---	16.1.7	---	National Institute of Standards and Technology Special Publication 800-29, A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2, June 2001. IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION Control: The information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module. Supplemental Guidance: The applicable federal standard for authentication to a cryptographic module is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect, and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval.	N/A	1	1	1			1	1				Recommend that authentication schema SHALL be commensurate with the highest level technically feasable. This requirement will constantly change as new schema's become available.
5.3.1.3 Use NIST-approved cryptography for communications	Cryptography used to protect information in-transit over public telecommunication networks SHALL use NIST-approved algorithms and cipher suites. In addition the implementations of these algorithms SHALL be NIST-approved (Cryptographic Algorithm Validation Program).	Test Method: Function	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST	IA-7	Cryptographic Module; Authentication	---	16.1.7	---	16.1.7	---	National Institute of Standards and Technology Special Publication 800-29, A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2, June 2001. IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION Control: The information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module. Supplemental Guidance: The applicable federal standard for authentication to a cryptographic module is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect, and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval.	N/A	1	1	1			1	1				N/C
5.3.2.1 Key generation methods	Cryptographic keys generated by the voting system SHALL use a NIST-approved key generation method, or a published and credible key generation method.	Inspection	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST	SC-12	Cryptographic Key Establishment and Management	12.3.1; 12.3.2	16.1.7; 16.1.8	---	IAKM-1	1.G	SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT Control: When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures. Supplemental Guidance: NIST Special Publication 800-56 provides guidance on cryptographic key establishment. NIST Special Publication 800-57 provides guidance on cryptographic key management.	N/A	1	1	1			1	1				N/C
5.3.2.2 Security of key generation methods	Compromising the security of the key generation method (e.g., guessing the seed value to initialize the deterministic random number generator (RNG)) SHALL require as least as many operations as determining the value of the generated key.	Inspection	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST	None	None	None	None	None	None	None	National Institute of Standards and Technology Special Publication 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised), March 2007.	N/A	1	1	1			1	1				N/C
5.3.2.3 Seed values	If a seed key is entered during the key generation process, entry of the key SHALL meet the key entry requirements in 5.3.3.1. If intermediate key generation values are output from the cryptographic module, the values SHALL be output either in encrypted form or under split knowledge procedures.	Inspection	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST	SC-12	Cryptographic Key Establishment and Management	12.3.1; 12.3.2	16.1.7; 16.1.8	---	IAKM-1	1.G	National Institute of Standards and Technology Special Publication 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised), March 2007.SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT Control: When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures. Supplemental Guidance: NIST Special Publication 800-56 provides guidance on cryptographic key establishment. NIST Special Publication 800-57 provides guidance on cryptographic key management.	N/A	1	1	1			1	1				N/C

5.3.2.4 Use NIST-approved key generation methods for communications	Cryptographic keys used to protect information in-transit over public telecommunication networks SHALL use NIST-approved key generation methods. If the approved key generation method requires input from a random number generator, then an approved (FIPS 140-2) random number generator SHALL be used.	Inspection	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST	SC-12	Cryptographic Key Establishment and Management	12.3.1; 12.3.2	16.1.7; 16.1.8	---	FVAP IAKM-1	UOCA 1.G	National Institute of Standards and Technology Special Publication 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised), March 2007.SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT Control: When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures. Supplemental Guidance: NIST Special Publication 800-56 provides guidance on cryptographic key establishment. NIST Special Publication 800-57 provides guidance on cryptographic key management.	N/A	1	1	1				1	1				N/C
5.3.2.5 Random number generator health tests	Random number generators used to generate cryptographic keys SHALL implement one or more health tests that provide assurance that the random number generator continues to operate as intended (e.g., the entropy source is not stuck).	Inspection	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST	None	None	None	None	None	None	None	National Institute of Standards and Technology Special Publication 800-90, The health test function determines that the DRBG mechanism continues to function correctly.	Covered in NIST Special Publication 800-90	1	1	1				1	1				N/C
5.3.3.1 Key entry and output	Secret and private keys established using automated methods SHALL be entered into and output from a voting system in encrypted form. Secret and private keys established using manual methods may be entered into or output from a system in plaintext form.	Inspection	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST	None	None	None	None	None	None	None	National Institute of Standards and Technology Special Publication 800-90, The health test function determines that the DRBG mechanism continues to function correctly.	Covered in NIST Special Publication 800-90	1	1	1				1	1				N/C
5.3.4.1 Key storage	Cryptographic keys stored within the voting system SHALL NOT be stored in plaintext. Keys stored outside the voting system SHALL be protected from disclosure or modification.	Inspection	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST	None	None	None	None	None	None	None	National Institute of Standards and Technology Special Publication 800-90, The health test function determines that the DRBG mechanism continues to function correctly.	N/A	1	1	1				1	1				N/C
5.3.4.2 Key zeroization	The voting system SHALL provide methods to zeroize all plaintext secret and private cryptographic keys within the system.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST	None	None	None	None	None	None	None	National Institute of Standards and Technology Special Publication 800-90, The health test function determines that the DRBG mechanism continues to function correctly.	N/A	1	1	1				1	1				N/C
5.3.4.3 Support for rekeying	The voting system SHALL support the capability to reset cryptographic keys to new values.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST	None	None	None	None	None	None	None	National Institute of Standards and Technology Special Publication 800-90, The health test function determines that the DRBG mechanism continues to function correctly.	N/A	1	1	1				1	1				N/C
5.4.1.1 Cast vote integrity; transmission	The integrity and authenticity of each individual cast vote SHALL be protected from any tampering or modification during transmission.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST	SC-8	Transmission Integrity	10.6.1; 10.8.1; 10.9.1	11.2.1; 11.2.4; 11.2.9; 16.2.14	AC-3.2	ECTM-1	5.B.3.a(11)	ECTM-2 Transmission Integrity Controls Good engineering practices with regards to the integrity mechanisms of COTS, GOTS, and custom developed solutions are implemented for incoming and outgoing files, such as parity checks and cyclic redundancy checks (CRCs). Mechanisms are in place to assure the integrity of all transmitted information (including labels and security parameters) and to detect or prevent the hijacking of a communication session (e.g., encrypted or covert communication channels).	N/A	1	1	1				1	1				N/C
5.4.1.2 Cast vote integrity; storage	The integrity and authenticity of each individual cast vote SHALL be preserved by means of a digital signature during storage.	Functional	VSTL	Functional Requirement. Loss of Integrity.	T=TEST	None	None	None	None	None	None	None	Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), Draft March 2006.	N/A		1					1	1		1		N/C
5.4.1.3 Cast vote storage	Cast vote data SHALL NOT be permanently stored on the vote capture device.	Functional	VSTL	Functional Requirement. Loss of Integrity.	T=TEST	None	None	None	None	None	None	None	Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), Draft March 2006.	N/A		1					1			1	1	N/C
5.4.1.4 Electronic ballot box integrity	The integrity and authenticity of the electronic ballot box SHALL be protected by means of a digital signature.	Functional	VSTL	Functional Requirement. Loss of Integrity and/or Confidentiality.	T=TEST	None	None	None	None	None	None	None	Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), Draft March 2006.	N/A		1					1			1	1	N/C
5.4.1.5 Malware detection	The voting system SHALL use malware detection software to protect against known malware that targets the operating system, services, and applications.	Inspection	VSTL	Loss of Integrity, Confidentiality and/or Availability.	T=TEST	SI-3 SI-4	Malicious Code Protection Information System Monitoring Tools and Techniques	10.4.1; 10.6.2; 10.10.1; 10.10.2; 10.10.4	11.1.1; 11.1.2	---	ECVP-1; VIVM-1; EBBD-1; EBVC-1; ECID-1	5.B.1.a(4); 7.B.4.b(1)		N/A	1	1	1			1		1				N/C
5.4.1.6 Updating malware detection	The voting system SHALL provide a mechanism for updating malware detection signatures.	Inspection	VSTL	Loss of Integrity, Confidentiality and/or Availability.	T=TEST	SI-3	Malicious Code Protection	10.4.1	11.1.1; 11.1.2	---	ECVP-1; VIVM-1	5.B.1.a(4); 7.B.4.b(1)	NIST Special Publication 800-61 provides guidance on detecting attacks through various types of security technologies. NIST Special Publication 800-83 provides guidance on detecting malware-based attacks through malicious code protection software. NIST Special Publication 800-92 provides guidance on monitoring and analyzing computer security event logs. NIST Special Publication 800-94 provides guidance on intrusion detection and prevention. Related security control: AC-8. National Institute of Standards and Technology Special Publication 800-83, Guide to Malware Incident Prevention and Handling, November 2005.	N/A	1	1	1			1		1				N/C
5.4.1.7 Validating software on kiosk voting devices	The voting system SHALL provide the capability for kiosk workers to validate the software used on the vote capture devices as part of the daily initiation of kiosk operations.	Inspection	VSTL	Functional Requirement No direct impact on security.	T=TEST	SI-6	Security Functionality Verification	---	11.2.1; 11.2.2	SS-2.2	DCSS-1	4.B.1.c(2); 5.B.2.b(2)	SI-6 SECURITY FUNCTIONALITY VERIFICATION Control: The information system verifies the correct operation of security functions [Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every [Assignment: organization-defined time-period]] and [Selection (one or more): notifies system administrator, shuts the system down, restarts the system] when anomalies are discovered. Supplemental Guidance: The need to verify security functionality applies to all security functions. For those security functions that are not able to execute automated self-tests, the organization either implements compensating security controls or explicitly accepts the risk of not performing the verification as required.	N/A		1					1	1				N/C
5.5.1.1 Data integrity protection	Voting systems that transmit data over communications links SHALL provide integrity protection for data in transit through the generation of integrity data (digital signatures and/or message authentication codes) for outbound traffic and verification of the integrity data for inbound traffic.	Functional	VSTL	Integrity Controls for transmission. Impacts confidentiality, Availability and Integrity.	I=INSPECTION	SC-16	Transmission of Security Parameters	7.2.2; 10.8.2; 10.9.2	16.1.6	AC-3.2	ECTM-2	4.B.1.a(3)	ECTM-2 Transmission Integrity Controls Good engineering practices with regards to the integrity mechanisms of COTS, GOTS, and custom developed solutions are implemented for incoming and outgoing files, such as parity checks and cyclic redundancy checks (CRCs). Mechanisms are in place to assure the integrity of all transmitted information (including labels and security parameters) and to detect or prevent the hijacking of a communication session (e.g., encrypted or covert communication channels).	N/A		1					1	1				N/C
5.5.1.2 TLS/SSL	Voting systems SHALL use at a minimum TLS 1.0, SSL 3.1 or equivalent protocols, including all updates to both protocols and implementations as of the date of the submission (e.g., RFC 5746 for TLS 1.0).	Functional	VSTL	Integrity Controls for transmission. Impacts confidentiality, Availability and Integrity.	T=TEST	SC-8 SC-16	Transmission Integrity	10.6.1; 10.8.1; 10.9.1	11.2.1; 11.2.4; 11.2.9; 16.2.14	AC-3.2	ECTM-1	5.B.3.a(11)	National Institute of Standards and Technology Special Publication 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations, June 2005. IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION Control: The information system identifies and authenticates specific devices before establishing a connection. Supplemental Guidance: The information system typically uses either shared known information (e.g., Media Access Control (MAC) or Transmission Control Protocol/Internet Protocol (TCP/IP) addresses) or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication) to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism is determined by the FIPS 199 security categorization of the information system with higher impact levels requiring stronger authentication. NIST Special Publication 800-77 provides guidance on protecting transmission integrity using IPsec. NIST Special Publication 800-81 provides guidance on Domain Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems.	N/A	1	1				1		1				N/C

6.1 General Requirements	At a minimum, this program SHALL: a. Include procedures for specifying, procuring, inspecting, accepting, and controlling parts and raw materials of the requisite quality; b. Require the documentation of the software development process; c. Require the documentation of the hardware specification and selection process; d. Identify and enforce all requirements for: i. In-process inspection and testing that the manufacturer deems necessary to ensure proper fabrication and assembly of hardware ii. Installation and operation of software and firmware e. Include plans and procedures for post-production environmental screening and acceptance testing; and f. Include a procedure for maintaining all data and records required to document and verify the quality inspections and tests.	Inspection	Manufacturer	Integrity Controls for transmission. Impacts confidentiality, Availability and Integrity.	I=INSPECTION	SA-4	Acquisitions	12.1.1	3.1.6; 3.1.7; 3.1.10; 3.1.11; 3.1.12	---	DCAS-1; DCDS-1; DCIT 1; DCMC-1	DCID: B.2.a; C.2.a; Manual:; 9.B.4	SA-4 ACQUISITIONS Control: The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards.	N/A	1	1	1			1		1				N/C
6.2 Components from Third Parties	A manufacturer who does not manufacture all the components of its voting system, but instead procures components as standard commercial items for assembly and integration into a voting system, SHALL verify that the supplier manufacturers follow documented quality assurance procedures that are at least as stringent as those used internally by the voting system manufacturer.	Inspection	Manufacturer	loss of Integrity, availability and/or Confidentiality	I=INSPECTION	None	None	None	None	None	None	None	Nothing found in referencfed documentation. However, this may be referenced within another publication involving acquisitions.	N/A	1	1	1			1				1		N/C
6.3 Responsibility for Tests	Manufacturer SHALL be responsible for performing all quality assurance tests, acquiring and documenting test data, and providing test reports for examination by the VSTL as part of the national certification process. These reports SHALL also be provided to the purchaser upon request.	Inspection	Manufacturer	loss of Integrity, availability and/or Confidentiality	I=INSPECTION	None	None	None	None	None	None	None	Nothing found in referencfed documentation. However, this may be referenced within another publication involving acquisitions.	N/A		1	1			1				1		N/C
6.4 Parts and Materials, Special Tests, and Examinations	In order to ensure that voting system parts and materials function properly, manufacturers SHALL: a. Select parts and materials to be used in voting systems and components according to their suitability for the intended application. Suitability may be determined by similarity of this application to existing standard practice or by means of special tests; b. Design special tests, if needed, to evaluate the part or material under conditions accurately simulating the actual voting system operating environment; and c. Maintain the resulting test data as part of the quality assurance program documentation.	Inspection	Manufacturer	loss of Integrity, availability and/or Confidentiality	I=INSPECTION	None	None	None	None	None	None	None	Nothing found in referencfed documentation. However, this may be referenced within another publication involving acquisitions.	N/A		1	1			1		1				N/C
6.5 Quality Conformance Inspections	The manufacturer performs conformance inspections to ensure the overall quality of the voting system and components delivered to the VSTL for national certification testing and to the jurisdiction for implementation. To meet the conformance inspection requirements the manufacturer SHALL: a. Inspect and test each voting system or component to verify that it meets all inspection and test requirements for the voting system; and b. Deliver a record of tests or a certificate of satisfactory completion with each voting system or component.	Inspection	Manufacturer	No specific requirement for vendor testing identified. Loss of Integrity, availability and/or Confidentiality	I=INSPECTION	None	None	None	None	None	None	None	ECMT-2 Conformance Monitoring and Testing Conformance testing that includes periodic, unannounced in-depth monitoring and provides for specific penetration testing to ensure compliance with all vulnerability mitigation procedures such as the DoD IAVA or other DoD IA practices is planned, scheduled, conducted, and independently validated. Testing is intended to ensure that the system's IA capabilities continue to provide adequate assurance against constantly evolving threats and vulnerabilities.	N/A		1	1			1		1				N/C
7.1.1 Configuration Management Requirements	The configuration management documentation provided for manufacturer registration SHALL be sufficient for pilot projects.	Inspection	Test Entity: EAC	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTION	CM-1	Configuration Management Policy and Procedures	12.4.1; 12.5.1; 15.1.1	---	---	DCCB-1; DCPR-1; DCAR-1; E3.3.8	DCID: B.2.a Manual: 2.B.4.e(5); 5.B.2.a(5)	CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	N/A		1	1			1		1				N/C
7.1.2 Audit of Configuration Management Documentation	The manufacturer SHALL provide the following documentation to the EAC for review. This documentation will be audited during the registration review which will be conducted during the pilot testing period. The items which the EAC will audit are the following: a. Application of configuration management requirements; b. Configuration management policy; c. Configuration identification; d. Baseline, promotion, and demotion procedures; e. Configuration control procedures; f. Release process; g. Configuration audits; and h. Configuration management resources.	Inspection	Test Entity: EAC	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTION & T=TEST	CM-1	Configuration Management Policy and Procedures	12.4.1; 12.5.1; 15.1.1	---	---	DCCB-1; DCPR-1; DCAR-1; E3.3.8	DCID: B.2.a Manual: 2.B.4.e(5); 5.B.2.a(5)	Not vendor specific CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	N/A		1	1			1		1				
7.2.1 Classification and Naming Configuration Items	Manufacturers SHALL describe the procedures and conventions used to classify configuration items into categories and subcategories, uniquely number or otherwise identify configuration items and name configuration items.	Inspection	Manufacturer	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTION	CM-1	Configuration Management Policy and Procedures	12.4.1; 12.5.1; 15.1.1	---	---	DCCB-1; DCPR-1; DCAR-1; E3.3.8	DCID: B.2.a Manual: 2.B.4.e(5); 5.B.2.a(5)	Not vendor specific CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	N/A		1	1			1		1				N/C
7.2.2 Versioning Conventions	When a voting system component is part of a higher level system element such as a subsystem, the manufacturer SHALL describe the conventions used to: a. Identify the specific versions of individual configuration items and sets of items that are incorporated in higher level system elements such as subsystems; b. Uniquely number or otherwise identify versions; and c. Name versions.	Inspection	Manufacturer	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTION	CM-1	Configuration Management Policy and Procedures	12.4.1; 12.5.1; 15.1.1	---	---	DCCB-1; DCPR-1; DCAR-1; E3.3.8	DCID: B.2.a Manual: 2.B.4.e(5); 5.B.2.a(5)	Not vendor specific CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	N/A		1	1			1		1				N/C
7.3 Baseline and Promotion Procedures	Manufacturers SHALL establish formal procedures and conventions for establishing and providing a complete description of the procedures and related conventions used to: a. Establish a particular instance of a component as the starting baseline; b. Promote subsequent instances of a component to baseline status as development progresses through to completion of the initial completed version released to the VSTL for testing; and c. Promote subsequent instances of a component to baseline status as the component is maintained throughout its life cycle until system retirement (i.e., the system is no longer sold or maintained by the manufacturer).	Inspection	Manufacturer	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTION	CM-2	Baseline Configuration	7.1.1; 15.1.2	1.1.1; 3.1.9; 10.2.7; 10.2.9; 12.1.4	CC-2.3; CC-3.1; SS-1.2	DCHW-1; DCSW-1	2.B.7.c(7); 4.B.1.c(3); 4.B.2.b(6)	Not vendor specific CM-2 BASELINE CONFIGURATION Control: The organization develops, documents, and maintains a current baseline configuration of the information system.	N/A	1	1	1			1		1				
7.4 Configuration Control Procedures	Configuration control is the process of approving and implementing changes to a configuration item to prevent unauthorized additions, changes or deletions. The manufacturer SHALL establish such procedures and related conventions, providing a complete description of those procedures used to: a. Develop and maintain internally developed items; b. Acquire and maintain third-party items; c. Resolve internally identified defects for items regardless of their origin; and d. Resolve externally identified and reported defects (i.e., by customers and VSTLs).	Inspection	Manufacturer	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTION	CM-3	Configuration Change Control	10.1.2; 10.2.3; 12.4.1; 12.5.1; 12.5.2; 12.5.3	3.1.4; 10.2.2; 10.2.3; 10.2.8; 10.2.10; 10.2.11	SS-3.2; CC-2.2	DCPR-1	2.B.7.c(7); 4.B.1.c(3); 4.B.2.b(6); 5.B.2.a(5)	Not vendor specific CM-3 CONFIGURATION CHANGE CONTROL Control: The organization authorizes, documents, and controls changes to the information system.	N/A		1	1		1			1				N/C

											FVAP	UOCA												
7.5.1 Physical Configuration Audit (PCA)	For the PCA, a manufacturer SHALL provide: a. Identification of all items that are to be a part of the pilot release; b. Specification of compiler (or choice of compilers) to be used to generate voting system executable programs; c. Identification of all hardware that interfaces with the software; d. Configuration baseline data for all hardware that is unique to the voting system; e. Copies of all software documentation intended for distribution to users, including program listings, specifications, operations manual, voter manual, and maintenance manual; f. Identification of any changes between the physical configuration of the voting system submitted for the PCA and that submitted for the Functional Configuration Audit (FCA), with a certification that any differences do not degrade the functional characteristics; and g. Complete descriptions of its procedures and related conventions used to support this audit by i. Establishing a configuration baseline of the software and hardware to be tested; and ii. Confirming whether the voting system documentation matches the corresponding system components.	Inspection	VSTL	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTION	CM-2	Baseline Configuration	7.1.1; 15.1.2	1.1.1; 3.1.9; 10.2.7; 10.2.9; 12.1.4	CC-2.3; CC-3.1; SS-1.2	DCHW-1; DCSW-1	2.B.7.c(7); 4.B.1.c(3); 4.B.2.b(6)	Not vendor specific CM-2 BASELINE CONFIGURATION Control: The organization develops, documents, and maintains a current baseline configuration of the information system.	N/A		1	1			1		1				N/C
7.5.2 Functional Configuration Audit (FCA)	The Functional Configuration Audit is conducted by the VSTL to verify that the voting system performs all the functions described in the system documentation. Manufacturers SHALL: a. Completely describe its procedures and related conventions used to support this audit for all voting system components; and b. Provide the following information to support this audit: c. Copies of all procedures used for module or unit testing, integration testing, and system testing; d. Copies of all test cases generated for each module and integration test, and sample ballot formats or other test cases used for system tests; and e. Records of all tests performed by the procedures listed above, including error corrections and retests.	Functional / Inspection	VSTL	Configuration/Testing	I=INSPECTION	None	None	None	None	None	None	None		N/A	1	1	1			1			1			N/C
8.1.1.1.1 Identify full system configuration	Manufacturers SHALL submit to the VSTL documentation necessary for the identification of the full system configuration submitted for evaluation and for the development of an appropriate test plan by the VSTL.	Inspection	Manufacturer	Documentation	I=INSPECTION	CM-2	Baseline Configuration	7.1.1; 15.1.2	1.1.1; 3.1.9; 10.2.7; 10.2.9; 12.1.4	CC-2.3; CC-3.1; SS-1.2	DCHW-1; DCSW-1	2.B.7.c(7); 4.B.1.c(3); 4.B.2.b(6)	DCHW-1 HW Baseline A current and comprehensive baseline inventory of all hardware (HW) (to include manufacturer, type, model, physical location and network topology or architecture) required to support enclave operations is maintained by the Configuration Control Board (CCB) and as part of the SSAA. A backup copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original.	N/A	1	1	1			1		1			1	N/C
8.1.1.1.2 Required content for pilot certification	Manufacturers SHALL provide a list of all documents submitted controlling the design, construction, operation, and maintenance of the voting system. At minimum, the TDP SHALL contain the following documentation: Implementation statement; Voting system user documentation (See Section 9 Voting Equipment User Documentation); System hardware specification; Application logic design and specification; System security specification; System test specification; Configuration for testing; and Training documentation.	Inspection	Manufacturer	Documentation	I=INSPECTION	CM-2	Baseline Configuration	7.1.1; 15.1.2	1.1.1; 3.1.9; 10.2.7; 10.2.9; 12.1.4	CC-2.3; CC-3.1; SS-1.2	DCHW-1; DCSW-1	2.B.7.c(7); 4.B.1.c(3); 4.B.2.b(6)	DCHW-1 HW Baseline A current and comprehensive baseline inventory of all hardware (HW) (to include manufacturer, type, model, physical location and network topology or architecture) required to support enclave operations is maintained by the Configuration Control Board (CCB) and as part of the SSAA. A backup copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original.	N/A		1			1		1			1	N/C
8.1.1.2.1 Table of contents and abstracts	The TDP SHALL include a detailed table of contents for the required documents, an abstract of each document, and a listing of each of the informational sections and appendices presented.	Inspection	Manufacturer	Documentation	I=INSPECTION	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD 1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	Hundreds of references to design and documentation requierments	N/A		1			1		1			1	N/C
8.1.1.2.2 Cross-index	A cross-index SHALL be provided indicating the portions of the documents that are responsive to the documentation requirements enumerated in section 8.1.1.1.2.	Inspection	Manufacturer	Documentation	I=INSPECTION	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD 1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	Hundreds of references to design and documentation requierments	N/A		1			1		1			1	N/C
8.1.2.1 Identify proprietary data	Manufacturers SHALL identify all documents, or portions of documents, containing proprietary information that is not releasable to the public.	Inspection	Manufacturer	Documentation	I=INSPECTION	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD 1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	Hundreds of references to design and documentation requierments	N/A		1	1		1		1			1	N/C
8.2.1 TDP Implementation Statement	The TDP SHALL include an implementation statement.	Inspection	Manufacturer	Documentation	I=INSPECTION	None	None	None	None	None	None	None	None	N/A			1		1				1	1	N/C
8.3.1 System Hardware Specification Scope	Manufacturers SHALL expand on the system overview included in the user documentation by providing detailed specifications of the hardware components of the voting system, including specifications of hardware used to support the telecommunications capabilities of the voting system, if applicable.	Inspection	Manufacturer	Documentation	I=INSPECTION	MA-1	System Maintenance Policy and Procedures	10.1.1; 15.1.1	10	---	PRMP-1; DCAR-1	DCID: B.2.a Manual: 2.B.4.e(5); 6.B.2.a(5)	Hundreds of references to design and documentation requierments	N/A			1		1		1			1	N/C
8.3.2.1 Description of hardware characteristics	Manufacturers SHALL provide a detailed discussion of the characteristics of the system, indicating how the hardware meets individual requirements defined in this document, including: a. Performance characteristics: Basic system performance attributes and operational scenarios that describe the manner in which system functions are invoked, describe environmental capabilities, describe life expectancy, and describe any other essential aspects of system performance; b. Physical characteristics: Suitability for intended use, requirements for security criteria, and vulnerability to adverse environmental factors; c. Reliability: System and component reliability stated in terms of the system's operating functions, and identification of items that require special handling or operation to sustain system reliability; and d. Environmental conditions: Ability of the system to withstand natural environments, and operational constraints in normal and test environments, including all requirements and restrictions regarding electrical service, telecommunications services, environmental protection, and any additional facilities or resources required to install and operate the system.	Inspection	Manufacturer	Documentation	I=INSPECTION	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD 1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	Hundreds of references to design and documentation requierments	N/A	1	1	1		1		1			1	N/C
8.3.3.1 System configuration	Manufacturers SHALL provide sufficient data, or references to data, to identify unequivocally the details of the system configuration submitted for testing.	Inspection	Manufacturer	Documentation	I=INSPECTION	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD 1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	Hundreds of references to design and documentation requierments	N/A			1			1		1			1	N/C

8.3.3.2 Photographs for hardware validation	Manufacturers SHALL provide photographs of the exterior and interior of devices included in the system to identify the hardware of the system configuration submitted for testing.	Inspection	Manufacturer	Documentation	I=INSPECTION	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	Hundreds of references to design and documentation requierments	N/A			1		1			1			1	N/C
8.3.3.3 List of materials	Manufacturers SHALL provide a list of materials and components used in the system and a description of their assembly into major system components and the system as a whole.	Inspection	Manufacturer	Documentation	I=INSPECTION	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	Not vendor specific Hundreds of references to design and documentation requierments	N/A	1	1	1		1			1			1	N/C
8.3.3.4 Design and construction miscellany	Text and diagrams SHALL be provided that describe: a. Materials, processes, and parts used in the system, their assembly, and the configuration control measures to ensure compliance with the system specification; b. Electromagnetic environment generated by the system; and c. Operator and voter safety considerations and any constraints on system operations or the use environment.	Inspection	Manufacturer	Documentation	I=INSPECTION	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	Hundreds of references to design and documentation requierments	N/A	1	1	1		1			1			1	N/C
8.3.4.1 Hardwired and mechanical implementations of logic	For each non-COTS hardware component (e.g., an application-specific integrated circuit or a manufacturer-specific integration of smaller components), manufacturers SHALL provide complete design and logic specifications, such as Computer Aided Design and Hardware Description Language files.	Inspection	Manufacturer	Industrial controll logic could impact Confidentiality, Integrity and/or Availability.	I=INSPECTION	None	None	None	None	None	None	None	NIST SP800-53 Reference: An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.	None	1	1	1				1		1			N/C
8.3.4.2 Logic specifications for PLDs, FPGAs and PICs	For each Programmable Logic Device (PLD), Field-Programmable Gate Array (FPGA), or Peripheral Interface Controller (PIC) that is programmed with non- COTS logic, manufacturers SHALL provide complete logic specifications, such as Hardware Description Language files or source code.	Inspection	Manufacturer	Industrial controll logic could impact Confidentiality, Integrity and/or Availability.	I=INSPECTION	None	None	None	None	None	None	None	NIST SP800-53 Reference: An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.	None	1	1	1				1		1			N/C
8.4.1 Application Logic Design and Specification	Manufacturers SHALL expand on the system overview included in the user documentation by providing detailed specifications of the application logic components of the system, including those used to support the telecommunications capabilities of the system, if applicable.	Inspection	Manufacturer	Documentation	I=INSPECTION	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	Not vendor specific. No specific IA Control referenced.	N/A	1	1	1		1			1			1	N/C
8.4.2.1 Application logic functions	Manufacturers SHALL describe the function or functions that are performed by the application logic comprising the system, including that used to support the telecommunications capabilities of the system, if applicable.	Inspection	Manufacturer	Documentation. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	No specific IA Control referenced.	N/A	1	1	1		1							N/C
8.4.3.1 Documents controlling application logic development	Manufacturers SHALL list all documents controlling the development of application logic and its specifications.	Inspection	Manufacturer	Documentation. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	No specific IA Control referenced.	N/A	1	1	1		1							N/C
8.4.4.1 Application logic overview	Manufacturers SHALL provide an overview of the application logic.	Inspection	Manufacturer	Documentation. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	No specific IA Control referenced.	N/A	1	1	1		1							N/C
8.4.4.2 Application logic architecture	The overview SHALL include a description of the architecture, the design objectives, and the logic structure and algorithms used to accomplish those objectives.	Inspection	Manufacturer	Documentation normally contained within the System Security Plan. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	PL-2	System Security Plan	6.1	4.1.5; 5.1.1; 5.1.2; 12.2.1	SP-2.1	DCSD-1	1.F.6; 2.B.6.c(3); 2.B.7.c(5); 9.E.2.a(1)(d); 9.F.2.a; Appendix C	PL-2 SYSTEM SECURITY PLAN Control: The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.	N/A	1	1	1		1			1				N/C
8.4.4.3 Application logic design	The overview SHALL include the general design, operational considerations, and constraints influencing the design.	Inspection	Manufacturer	Documentation normally contained within the System Security Plan. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	PL-2	System Security Plan	6.1	4.1.5; 5.1.1; 5.1.2; 12.2.1	SP-2.1	DCSD-1	1.F.6; 2.B.6.c(3); 2.B.7.c(5); 9.E.2.a(1)(d); 9.F.2.a; Appendix C	PL-2 SYSTEM SECURITY PLAN Control: The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.	N/A	1	1	1		1			1				N/C
8.4.4.4 Application logic overview miscellany	The overview SHALL include the following additional information for each separate software package: a. Package identification; b. General description; c. Requirements satisfied by the package; d. Identification of interfaces with other packages that provide data to, or receive data from, the package; and e. Concept of execution for the package.	Inspection	Manufacturer	Documentation normally contained within the System Security Plan.	I=INSPECTION	PL-2	System Security Plan	6.1	4.1.5; 5.1.1; 5.1.2; 12.2.1	SP-2.1	DCSD-1	1.F.6; 2.B.6.c(3); 2.B.7.c(5); 9.E.2.a(1)(d); 9.F.2.a; Appendix C	PL-2 SYSTEM SECURITY PLAN Control: The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.	N/A	1	1	1		1			1				N/C
8.4.5.1 Application logic standards and conventions	Manufacturers SHALL provide information on application logic standards and conventions developed internally by the manufacturer as well as published industry standards that have been applied by the manufacturer.	Inspection	Manufacturer	Documentation normally contained within the System Security Plan. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	PL-2	System Security Plan	6.1	4.1.5; 5.1.1; 5.1.2; 12.2.1	SP-2.1	DCSD-1	1.F.6; 2.B.6.c(3); 2.B.7.c(5); 9.E.2.a(1)(d); 9.F.2.a; Appendix C	PL-2 SYSTEM SECURITY PLAN Control: The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.	N/A	1	1	1		1			1				N/C
8.4.5.2 Application logic standards and conventions, checklist	Manufacturers SHALL provide information that addresses the following standards and conventions related to application logic: a. Development methodology; b. Design standards, including internal manufacturer procedures; c. Specification standards, including internal manufacturer procedures; d. Coding conventions, including internal manufacturer procedures; e. Testing and verification standards, including internal manufacturer procedures, that can assist in determining the correctness of the logic; and f. Quality assurance standards or other documents that can be used to examine and test the application logic. These documents include standards for logic diagrams, program documentation, test planning, and test data acquisition and reporting.	Inspection	Manufacturer	Documentation normally contained within the System Security Plan. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	PL-2	System Security Plan	6.1	4.1.5; 5.1.1; 5.1.2; 12.2.1	SP-2.1	DCSD-1	1.F.6; 2.B.6.c(3); 2.B.7.c(5); 9.E.2.a(1)(d); 9.F.2.a; Appendix C	PL-2 SYSTEM SECURITY PLAN Control: The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.	N/A	1	1	1		1			1				N/C
8.4.5.3 Justify coding conventions	Manufacturers SHALL furnish evidence that the selected coding conventions are "published" and "credible" as specified in section 4.3.1.	Inspection	Manufacturer	Documentation normally contained within the System Security Plan under "robustness". Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	None	None	None	None	None	None	None	NIST SP800-137 References coding practices. DCID 6/3: 1.H.1 In the following pages, the term "good engineering practice" refers to the state of the engineering art for commercial systems that have equivalent problems and solutions; a good engineering practice by definition meets commercial requirements. These practices are usually part of the normal installation and operating procedures for systems. When placing security reliance on items that implement good engineering practice (such as commercial off-the shelf [COTS] software), the DAAs or their designees shall verify that the item(s) are set up properly and are operating as expected.	N/A	1	1	1		1					1		N/C

8.4.6.1 Application logic operating environment	Manufacturers SHALL describe or make reference to all operating environment factors that influence the design of application logic.	Inspection	Manufacturer	Documentation normally contained within the System Security Plan under "robustness". Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	None	None	None	None	None	None	None	None	None	1	1	1			1			1		N/C
8.4.7.1 Hardware environment and constraints	Manufacturers SHALL identify and describe the hardware characteristics that influence the design of the application logic, such as: a. Logic and arithmetic capability of the processor; b. Memory read-write characteristics; c. External memory device characteristics; d. Peripheral device interface hardware; e. Data input/output device protocols; and f. Operator controls, indicators, and displays.	Inspection	Manufacturer	Documentation normally contained within the System Security Plan under "robustness". Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	None	None	None	None	None	None	None	None	None	1	1	1		1				1		N/C
8.4.8.1 Operating system	Manufacturers SHALL identify the operating system and the specific version thereof, or else clarify how the application logic operates without an operating system.	Inspection	Manufacturer	Documentation normally contained within the System Security Plan. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	PL-2	System Security Plan	6.1	4.1.5; 5.1.1; 5.1.2; 12.2.1	SP-2.1	DCSD-1	1.F.6; 2.B.6.c(3); 2.B.7.c(5); 9.E.2.a(1)(d); 9.F.2.a; Appendix C	PL-2 SYSTEM SECURITY PLAN Control: The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.	N/A	1	1	1		1			1				N/C
8.4.8.2 Compilers and assemblers	For systems containing compiled or assembled application logic, manufacturers SHALL identify the COTS compilers or assemblers used in the generation of executable code, and the specific versions thereof.	Inspection	Manufacturer	Documentation normally contained within the System Security Plan. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	None	None	None	None	None	None	None	None. Only references backups should provide for the protection of compilers.	None. Only references backups should provide for the protection of compilers.	1	1	1		1				1		N/C
8.4.8.3 Interpreters	For systems containing interpreted application logic, manufacturers SHALL specify the COTS runtime interpreter that SHALL be used to run this code, and the specific version thereof.	Inspection	Manufacturer	Documentation normally contained within the System Security Plan. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	None	None	None	None	None	None	None	None. Only references backups should provide for the protection of compilers.	None. Only references backups should provide for the protection of compilers.	1	1	1		1				1		N/C
8.4.9.1 Application logic functional specification	Manufacturers SHALL provide a description of the operating modes of the system and of application logic capabilities to perform specific functions.	Inspection	Manufacturer	Documentation normally contained within the System Security Plan. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	None	None	None	None	None	None	None	None	None	1	1	1		1				1		N/C
8.4.10.1 Functions and operating modes	Manufacturers SHALL describe all application logic functions and operating modes of the system, such as ballot preparation, election programming, preparation for opening the voting period, recording votes and/or counting ballots, closing the voting period, and generating reports.	Inspection	Manufacturer	Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	MA-1	System Maintenance Policy and Procedures	10.1.1; 15.1.1	10	---	PRMP-1; DCAR-1	DCID: B.2.a Manual: 2.B.4.e(5); 6.B.2.a(5)	CM-6; DCSS-1; ECSC-1	N/A	1	1	1		1			1				N/C
8.4.10.2 Functions and operating modes detail	For each application logic function or operating mode, manufacturers SHALL provide: a. A definition of the inputs to the function or mode (with characteristics, limits, tolerances or acceptable ranges, as applicable); b. An explanation of how the inputs are processed; and c. A definition of the outputs produced (again, with characteristics, limits, tolerances, or acceptable ranges, as applicable).	Inspection	Manufacturer	Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	SI-9	Information Input Restrictions	12.2.1; 12.2.2	---	SD-1	---	2.B.9.b(11)	SI-9 INFORMATION INPUT RESTRICTIONS Control: The organization restricts the capability to input information to the information system to authorized personnel. Supplemental Guidance: Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.	N/A		1			1		1					N/C
8.4.11.1 Application logic integrity features	Manufacturers SHALL describe the application logic's capabilities or methods for detecting or handling: a. Exception conditions; b. System failures; c. Data input/output errors; d. Error logging for audit record generation; e. Production of statistical ballot data; f. Data quality assessment; and g. Security monitoring and control.	Inspection	Manufacturer	Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	SI-11	Error Handling	12.2.1; 12.2.2; 12.2.3; 12.2.4	---	---	---	2.B.4.d	SI-11 ERROR HANDLING Control: The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries.	N/A	1	1	1			1		1				N/C
8.4.12.1 Programming specifications	Manufacturers SHALL provide in this section an overview of the application logic's design, its structure, and implementation algorithms and detailed specifications for individual modules.	Inspection	Manufacturer	Software Quality: Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	SI-2	Flaw Remediation	10.10.5; 12.4.1; 12.5.1; 12.5.2; 12.6.1	10.3.2; 11.1.1; 11.1.2; 11.2.2; 11.2.7	SS-2.2	DCSQ-1; DCCT-1; VIVM-1	5.B.2.a(5)(a)(3); 6.B.2.a(5)	DCSQ-1 Software Quality Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives.	N/A	1	1	1			1		1				N/C
8.4.13.1 Programming specifications overview, diagrams	This overview SHALL include such items as Unified Modeling Language diagrams, data flow diagrams, and/or other graphical techniques that facilitate understanding of the programming specifications.	Inspection	Manufacturer	Software Quality: Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	SI-2	Flaw Remediation	10.10.5; 12.4.1; 12.5.1; 12.5.2; 12.6.1	10.3.2; 11.1.1; 11.1.2; 11.2.2; 11.2.7	SS-2.2	DCSQ-1; DCCT-1; VIVM-1	5.B.2.a(5)(a)(3); 6.B.2.a(5)	DCSQ-1 Software Quality Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives.	N/A	1	1	1			1		1				N/C
8.4.13.3 Programming specifications overview, content	Implementation of the functions SHALL be described in terms of the architecture, algorithms, and data structures.	Inspection	Manufacturer	Software Quality: Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	SI-2	Flaw Remediation	10.10.5; 12.4.1; 12.5.1; 12.5.2; 12.6.1	10.3.2; 11.1.1; 11.1.2; 11.2.2; 11.2.7	SS-2.2	DCSQ-1; DCCT-1; VIVM-1	5.B.2.a(5)(a)(3); 6.B.2.a(5)	DCSQ-1 Software Quality Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives.	N/A	1	1	1			1		1				N/C
8.4.14.1 Programming specifications details	The programming specifications SHALL describe individual application logic modules and their component units, if applicable.	Inspection	Manufacturer	Software Quality: Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	SI-2	Flaw Remediation	10.10.5; 12.4.1; 12.5.1; 12.5.2; 12.6.1	10.3.2; 11.1.1; 11.1.2; 11.2.2; 11.2.7	SS-2.2	DCSQ-1; DCCT-1; VIVM-1	5.B.2.a(5)(a)(3); 6.B.2.a(5)	DCSQ-1 Software Quality Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives.	N/A	1	1	1			1		1				N/C
8.4.14.2 Module and callable unit documentation	For each application logic module and callable unit, manufacturers SHALL document: a. Significant module and unit design decisions, if any, such as algorithms used; b. Any constraints, limitations, or unusual features in the design of the module or callable unit; and c. A description of its inputs, outputs, and other data elements as applicable with respect to communication over system interfaces. (See section 8.4.16 Interfaces.)	Inspection	Manufacturer	Software Quality: Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	SI-2	Flaw Remediation	10.10.5; 12.4.1; 12.5.1; 12.5.2; 12.6.1	10.3.2; 11.1.1; 11.1.2; 11.2.2; 11.2.7	SS-2.2	DCSQ-1; DCCT-1; VIVM-1	5.B.2.a(5)(a)(3); 6.B.2.a(5)	DCSQ-1 Software Quality Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives.	N/A	1	1	1			1		1				N/C

8.4.14.3 Mixed-language software	If an application logic module is written in a programming language other than that generally used within the system, the specification for the module SHALL indicate the programming language used and the reason for the difference.	Inspection	Manufacturer	Software Quality: Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	SI-2	Flaw Remediation	10.10.5; 12.4.1; 12.5.1; 12.5.2; 12.6.1	10.3.2; 11.1.1; 11.1.2; 11.2.2; 11.2.7	SS-2.2	DCSQ-1; DCCT-1; VIVM-1	5.B.2.a(5)(a)(3); 6.B.2.a(5)	DCSQ-1 Software Quality Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives.	N/A	1	1	1			1		1				N/C
8.4.14.4 References for foreign programming languages	If a module contains embedded border logic commands for an external library or package (e.g., menu selections in a database management system for defining forms and reports, on-line queries for database access and manipulation, input to a graphical user interface builder for automated code generation, commands to the operating system, or shell scripts), the specification for the module SHALL contain a reference to user manuals or other documents that explain them.	Inspection	Manufacturer	Software Quality: Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	SI-2	Flaw Remediation	10.10.5; 12.4.1; 12.5.1; 12.5.2; 12.6.1	10.3.2; 11.1.1; 11.1.2; 11.2.2; 11.2.7	SS-2.2	DCSQ-1; DCCT-1; VIVM-1	5.B.2.a(5)(a)(3); 6.B.2.a(5)	DCSQ-1 Software Quality Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives.	N/A	1	1	1			1		1				N/C
8.4.14.5 Source code	For each callable unit (e.g., function, method, operation, subroutine, procedure) in application logic, border logic, and third-party logic, manufacturers SHALL supply the source code.	Inspection	Manufacturer	Loss of Availability	I=INSPECTION	SA-6	Software Usage Restrictions	15.1.2	10.2.10; 10.2.13	SS-3.2; SP-2.1	DCPD-1	2.B.9.b(11)	NIST SP500-209DCID 6/3 Requirement: the original (source) code must be available at any time, the code must be controlled in a configuration management process, and the code must be marked with ownership and authorship. DCPD-1 Public Domain Software Controls Binary or machine executable public domain software products and other software products with limited or no warranty, such as those commonly known as freeware or shareware are not used in DoD information systems unless they are necessary for mission accomplishment and there are no alternative IT solutions available. Such products are assessed for information assurance impacts, and approved for use by the DAA. The assessment addresses the fact that such software products are difficult or impossible to review, repair, or extend, given that the Government does not have access to the original source code and there is no owner who could make such repairs on behalf of the Government.	N/A			1			1		1				N/C
8.4.14.6 Inductive assertions	For each callable unit (e.g., function, method, operation, subroutine, procedure) in core logic, manufacturers SHALL specify: a. Preconditions and postconditions of the callable unit, including any assumptions about capacities and limits within which the system is expected to operate; and b. A sound argument (preferably, but not necessarily, a formal proof) that the preconditions and postconditions of the callable unit accurately represent its behavior, assuming that the preconditions and postconditions of any invoked units are similarly accurate.	Inspection	Manufacturer	Software Quality: Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	SA-8	Security Engineering Principles	12.1	3.2.1	---	DCBP-1; DCCS-1; E3.4.4	1.H.1	NIST SP500-209SA-8 SECURITY ENGINEERING PRINCIPLES Control: The organization designs and implements the information system using security engineering principles. Supplemental Guidance: NIST Special Publication 800-27 provides guidance on engineering principles for information system security. The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications, to the extent feasible, given the current state of the hardware, software, and firmware components within the system.	N/A	1	1	1			1		1				N/C
8.4.14.7 High-level constraints	Manufacturers SHALL specify a sound argument (preferably, but not necessarily, a formal proof) that the core logic as a whole satisfies each of the constraints for all cases within the aforementioned capacities and limits, assuming that the preconditions and postconditions of callable units accurately characterize their behaviors.	Inspection	Manufacturer	Software Quality: Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	SA-8	Security Engineering Principles	12.1	3.2.1	---	DCBP-1; DCCS-1; E3.4.4	1.H.1	NIST SP500-209SA-8 (Not in searched Documetation) SECURITY ENGINEERING PRINCIPLES Control: The organization designs and implements the information system using security engineering principles. Supplemental Guidance: NIST Special Publication 800-27 provides guidance on engineering principles for information system security. The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications, to the extent feasible, given the current state of the hardware, software, and firmware components within the system.	N/A	1	1	1			1		1				N/C
8.4.14.8 Safety of concurrency	Manufacturers SHALL specify a sound argument (preferably, but not necessarily, a formal proof) that application logic is free of race conditions, deadlocks, livelocks, and resource starvation.	Inspection	Manufacturer	Software Quality: Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	SC-6	Resource Priority	---	---	---	---	6.B.3.a(11)	SC-6 RESOURCE PRIORITY Control: The information system limits the use of resources by priority. Supplemental Guidance: Priority protection helps prevent a lower-priority process from delaying or interfering with the information system servicing any higher-priority process.			1	1			1		1				N/C
8.4.15.1 System database	Manufacturers SHALL identify and provide a diagram and narrative description of the system's databases and any external files used for data input or output.	Inspection	Manufacturer	Insufficient documentation could lead to difficulties supporting the application. Loss of Availability, and/or Integrity.	I=INSPECTION	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	SA-5 INFORMATION SYSTEM DOCUMENTATION Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.			1	1			1		1				N/C
8.4.15.2 Database design levels	For each database or external file, manufacturers SHALL specify the number of levels of design and the names of those levels (e.g., conceptual, internal, logical, and physical).	Inspection	Manufacturer	Software Quality: Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	SA-8	Security Engineering Principles	12.1	3.2.1	---	DCBP-1; DCCS-1; E3.4.4	1.H.1	NIST SP500-209SA-8 SECURITY ENGINEERING PRINCIPLES Control: The organization designs and implements the information system using security engineering principles. Supplemental Guidance: NIST Special Publication 800-27 provides guidance on engineering principles for information system security. The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications, to the extent feasible, given the current state of the hardware, software, and firmware components within the system.	N/A	1	1	1			1		1				N/C
8.4.15.3 Database design conventions	For each database or external file, the manufacturer SHALL specify any design conventions and standards (which may be incorporated by reference) needed to understand the design.	Inspection	Manufacturer	Insufficient documentation could lead to difficulties supporting the application. Loss of Availability, and/or Integrity.	I=INSPECTION	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	SA-5 INFORMATION SYSTEM DOCUMENTATION Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.	N/A		1	1			1		1				N/C
8.4.15.4 Data models	For each database or external file, manufacturers SHALL identify and describe all logical entities and relationships and how these are implemented physically (e.g., tables, files).	Inspection	Manufacturer	Insufficient documentation could lead to difficulties supporting the application. Loss of Availability, and/or Integrity.	I=INSPECTION	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	SA-5 INFORMATION SYSTEM DOCUMENTATION Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.	N/A		1	1			1		1				N/C
8.4.15.5 Schemata	Manufacturers SHALL document the details of table, record or file contents (as applicable), individual data elements and their specifications, including: a. Names/identifiers; b. Data type (e.g., alphanumeric, integer); c. Size and format (such as length and punctuation of a character string); d. Units of measurement (e.g., meters, seconds e. Range or enumeration of possible values (e.g., 0–99 f. Accuracy (how correct) and precision (number of significant digits); g. Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether business rules apply; h. Security and privacy constraints; and i. Sources (setting/sending entities) and recipients (using/receiving entities).	Inspection	Manufacturer	Insufficient documentation could lead to difficulties supporting the application. Loss of Availability, and/or Integrity.	I=INSPECTION	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	SA-5 INFORMATION SYSTEM DOCUMENTATION Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.	N/A		1	1			1		1				N/C

8.4.15.6 External file maintenance and security	For external files, manufacturers SHALL document the procedures for file maintenance, management of access privileges, and security.	Inspection	Manufacturer	Insufficient documentation could lead to difficulties supporting the application. Loss of Availability, and/or Integrity.	I=INSPECTION	MA-1	System Maintenance Policy and Procedures	10.1.1; 15.1.1	10	---	PRMP-1; DCAR-1	DCID: B.2.a Manual: 2.B.4.e(5); 6.B.2.a(5)	MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.	N/A	1	1	1			1		1				N/C
8.4.16.1 Description of interfaces	Using a combination of text and diagrams, manufacturers SHALL identify and provide a complete description of all major internal and external interfaces.	Inspection	Manufacturer	Insufficient documentation could lead to difficulties supporting the application. Loss of Availability, and/or Integrity.	I=INSPECTION	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD 1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	DCFA-1 Functional Architecture for AIS Applications For AIS applications, a functional architecture that identifies the following has been developed and is maintained: - all external/internal interfaces, the information being exchanged, and the protection mechanisms associated with each interface - user roles required for access control and the access privileges assigned to each role (See ECAN) - unique security requirements (e.g., encryption of key data elements at rest) - categories of sensitive information processed or stored by the AIS application, and their specific protection plans (e.g., Privacy Act, HIPAA) - restoration priority of subsystems, processes, or information (see COEF).	N/A	1	1	1			1		1				N/C
8.4.17.1 Interface identification details	For each interface identified in the system overview, manufacturers SHALL: a. Provide a unique identifier assigned to the interface; b. Identify the interfacing entities (e.g., systems, configuration items, users) by name, number, version, and documentation references, as applicable; and c. Identify which entities have fixed interface characteristics (and therefore impose interface requirements on interfacing entities) and which are being developed or modified (thus having interface requirements imposed upon them).	Inspection	Manufacturer	Insufficient documentation could lead to difficulties supporting the application. Loss of Availability, and/or Integrity.	I=INSPECTION	MA-1	System Maintenance Policy and Procedures	10.1.1; 15.1.1	10	---	PRMP-1; DCAR-1	DCID: B.2.a Manual: 2.B.4.e(5); 6.B.2.a(5)	MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.	N/A	1	1	1			1		1				N/C
8.4.18.1 Interface types	For each interface identified in the system overview, manufacturers SHALL describe the type of interface (e.g., real-time data transfer, data storage-and retrieval) to be implemented.	Inspection	Manufacturer	Insufficient documentation could lead to difficulties supporting the application. Loss of Availability, and/or Integrity.	I=INSPECTION	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD 1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	SA-5 INFORMATION SYSTEM DOCUMENTATION Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.	N/A		1	1			1		1				N/C
8.4.18.2 Interface signatures	For each interface identified in the system overview, manufacturers SHALL describe characteristics of individual data elements that the interfacing entity (ies) will provide, store, send, access, receive, etc., such as: a. Names/identifiers; b. Data type (e.g., alphanumeric, integer); c. Size and format (such as length and punctuation of a character string); d. Units of measurement (e.g., meters, seconds); e. Range or enumeration of possible values (e.g., 0–99); f. Accuracy (how correct) and precision (number of significant digits); g. Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether business rules apply; h. Security and privacy constraints; and i. Sources (setting/sending entities) and recipients (using/receiving entities).	Inspection	Manufacturer	Insufficient documentation could lead to difficulties supporting the application. Loss of Availability, and/or Integrity.	I=INSPECTION	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD 1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	SA-5 INFORMATION SYSTEM DOCUMENTATION Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.	N/A		1	1			1		1				N/C
8.4.18.3 Interface protocols	For each interface identified in the system overview, manufacturers SHALL describe characteristics of communication methods that the interfacing entity (ies) will use for the interface, such as: a. Communication links/bands/frequencies/media and their characteristics; b. Message formatting; c. Flow control (e.g., sequence numbering and buffer allocation); d. Data transfer rate, whether periodic/aperiodic, and interval between transfers; e. Routing, addressing, and naming conventions; f. Transmission services, including priority and grade; and g. Safety/security/privacy considerations, such as encryption, user authentication, compartmentalization, and auditing.	Inspection	Manufacturer	Insufficient documentation could lead to difficulties supporting the application. Loss of Availability, and/or Integrity.	I=INSPECTION	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD 1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	SA-5 INFORMATION SYSTEM DOCUMENTATION Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.	N/A		1	1			1		1				N/C
8.4.18.4 Protocol details	For each interface identified in the system overview, manufacturers SHALL describe characteristics of protocols the interfacing entity (ies) will use for the interface, such as: a. Priority/layer of the protocol; b. Packeting, including fragmentation and reassembly, routing, and addressing; c. Legality checks, error control, and recovery procedures; d. Synchronization, including connection establishment, maintenance, termination; and e. Status, identification, and any other reporting features.	Inspection	Manufacturer	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTION	CA-3	Information System Connections	10.6.2; 10.9.1; 11.4.5; 11.4.6; 11.4.7	1.1.1; 3.2.9; 4.1.8; 12.2.3	CC-2.1	DCID-1; EBCR-1; EBRU-1; EBPW-1; ECIC-1	9.B.3; 9.D.3.c	CA-3 INFORMATION SYSTEM CONNECTIONS Control: The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis. NIST Special Publication 800-47 provides guidance on connecting information systems. Related security controls: SC-7, SA-9.	N/A	1	1	1			1		1				N/C
8.4.18.5 Characteristics of interfaces	For each interface identified in the system overview, manufacturers SHALL describe any other pertinent characteristics, such as physical compatibility of the interfacing entity (ies) (e.g., dimensions, tolerances, loads, voltages, plug compatibility).	Inspection	Manufacturer	Loss of Availability	I=INSPECTION	CM-8	Information System Component Inventory	7.1.1; 15.1.2	1.1.1; 3.1.9; 10.2.7; 10.2.9; 12.1.4	CC-2.3; CC-3.1; SS-1.2	DCHW-1; DCSW-1	2.B.7.c(7); 4.B.1.c(3); 4.B.2.b(6)	CM-8 INFORMATION SYSTEM COMPONENT INVENTORY Control: The organization develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information. Supplemental Guidance: The organization determines the appropriate level of granularity for the information system components included in the inventory that are subject to management control (i.e., tracking, and reporting). The inventory of information system components includes any information determined to be necessary by the organization to achieve effective property accountability (e.g., manufacturer, model number, serial number, software license information, system/component owner). The component inventory is consistent with the accreditation boundary of the information system. Related security controls: CM-2, CM-6.	N/A		1	1			1		1				N/C
9.2.1 User Documentation System Overview	In the system overview, manufacturers SHALL provide information that enables the user to identify the functional and physical components of the system, how the components are structured, and the interfaces between them.	Inspection	Manufacturer	Loss of Availability	I=INSPECTION	CM-1	Configuration Management Policy and Procedures	12.4.1; 12.5.1; 15.1.1	---	---	DCCB-1; DCPR-1; DCAR-1; E3.3.8	DCID: B.2.a Manual: 2.B.4.e(5); 5.B.2.a(5)	CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.			1	1		1			1				N/C
9.2.2 System Overview Functional Diagram	The system overview SHALL include a high-level functional diagram of the system that includes all of its components. The diagram SHALL portray how the various components relate and interact.	Inspection	Manufacturer	Loss of Integrity	I=INSPECTION	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD 1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	Security Design and Configuration Integrity DCFA-1 Functional Architecture for AIS Applications For AIS applications, a functional architecture that identifies the following has been developed and is maintained: - all external interfaces, the information being exchanged, and the protection mechanisms associated with each interface - user roles required for access control and the access privileges assigned to each role (See ECAN) - unique security requirements (e.g., encryption of key data elements at rest) - categories of sensitive information processed or stored by the AIS application, and their specific protection plans (e.g., Privacy Act, HIPAA) - restoration priority of subsystems, processes, or information (see COEF).			1	1		1			1				N/C

9.2.3.1 User documentation system description	The system description SHALL include written descriptions, drawings and diagrams that present: a. A description of the functional components or subsystems, (e.g., environment, election management and control, vote recording, vote conversion, reporting, and their logical relationships); b. A description of the operational environment of the system that provides an overview of the hardware, firmware, software, and communications structure; c. A description that explains each system function and how the function is achieved in the design; d. Descriptions of the functional and physical interfaces between subsystems and components; e. Identification of all COTS products (both hardware and software) included in the system and/or used as part of the system's operation, identifying the name, manufacturer, and version used for each such component; f. Communications (network) software; g. Interfaces among internal components and interfaces with external systems. For components that interface with other components for which multiple products may be used, the manufacturers SHALL identify file specifications, data objects, or other means used for information exchange, and the public standard used for such file specifications, data objects, or other means; and h. Listings of all software and firmware and associated documentation included in the manufacturer's release in the order in which each piece of software or firmware would normally be installed upon system setup and installation.	Inspection	Manufacturer	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTION	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD 1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	SA-5 INFORMATION SYSTEM DOCUMENTATION Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system. Supplemental Guidance: Documentation includes administrator and user guides with information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features. When adequate information system documentation is either unavailable or non existent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), the organization documents attempts to obtain such documentation and provides compensating security controls, if needed.	N/A		1	1		1			1				N/C
9.2.3.2 Identify software and firmware by origin	The system description SHALL include the identification of all software and firmware items, indicating items that were: a. Written in-house; b. Written by a subcontractor; c. Procured as COTS; and d. Procured and modified, including descriptions of the modifications to the software or firmware and to the default configuration options.	Inspection	Manufacturer	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTION	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD 1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	SA-5 INFORMATION SYSTEM DOCUMENTATION Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system. Supplemental Guidance: Documentation includes administrator and user guides with information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features. When adequate information system documentation is either unavailable or non existent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), the organization documents attempts to obtain such documentation and provides compensating security controls, if needed.	N/A		1	1		1			1				N/C
9.2.3.3 Traceability of procured software	The system description SHALL include a declaration that procured software items were obtained directly from the manufacturer or from a licensed dealer or distributor.	Inspection	Manufacturer	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTION	None	None	None	None	None	None	None			1	1	1			1				1		N/C
9.2.4.1 User documentation system performance	Manufacturers SHALL provide system performance information including: a. Device capacities and limits that were stated in the implementation statement; b. Performance characteristics of each operating mode and function in terms of expected and maximum speed, throughput capacity, maximum volume (maximum number of voting positions and maximum number of ballot styles supported), and processing frequency; c. Quality attributes such as reliability, maintainability, availability, usability, and portability; d. Provisions for safety, security, voter privacy, ballot secrecy, and continuity of operations; and e. Design constraints, applicable standards, and compatibility requirements.	Inspection	Manufacturer	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTION	SA-4	Acquisitions	12.1.1	3.1.6; 3.1.7; 3.1.10; 3.1.11; 3.1.12	---	DCAS-1; DCDS-1; DCIT-1; DCMC-1	DCID: B.2.a; C.2.a; Manual:; 9.B.4	SA-4 ACQUISITIONS Control: The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards. Supplemental Guidance: Solicitation Documents The solicitation documents (e.g., Requests for Proposals) for information systems and services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities (security needs and, as necessary, specific security controls and other specific FISMA requirements); (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation. The requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented. NIST Special Publication 800-36 provides guidance on the selection of information security products. NIST Special Publication 800-35 provides guidance on information technology security services. NIST Special Publication 800-64 provides guidance on security considerations in the system development life cycle. Information System Documentation The solicitation documents include requirements for appropriate information system documentation. The documentation addresses user and systems administrator guidance and information regarding the implementation of the security controls in the information system. The level of detail required in the documentation is based on the FIPS 199 security category for the information system. Use of Tested, Evaluated, and Validated Products NIST Special Publication 800-23 provides guidance on the acquisition and use of tested/evaluated information technology products. Configuration Settings and Implementation Guidance The information system required documentation includes security configuration settings and security implementation guidance. OMB FISMA reporting instructions provide guidance on configuration requirements for federal information systems. NIST Special Publication 800-70 provides guidance on configuration settings for information	N/A		1	1				1	1				N/C
9.3.1 User Documentation, System Functionality Description	Manufacturers SHALL provide a listing of the system's functional processing capabilities, encompassing capabilities required by the UOCAVA Pilot Program Testing Requirements, and any additional capabilities provided by the system, with a description of each capability. a. Manufacturers SHALL explain, in a manner that is understandable to users, the capabilities of the system declared in the implementation statement; b. Additional capabilities (extensions) SHALL be clearly indicated; c. Required capabilities that may be bypassed or deactivated during installation or operation by the user SHALL be clearly indicated; d. Additional capabilities that function only when activated during installation or operation by the user SHALL be clearly indicated; and e. Additional capabilities that normally are active but may be bypassed or deactivated during installation or operation by the user SHALL be clearly indicated.	Inspection	Manufacturer	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTION	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD 1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	SA-5 INFORMATION SYSTEM DOCUMENTATION Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system. Supplemental Guidance: Documentation includes administrator and user guides with information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features. When adequate information system documentation is either unavailable or non existent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), the organization documents attempts to obtain such documentation and provides compensating security controls, if needed.	N/A		1	1		1			1				N/C
9.4.1.1 Access control implementation, configuration, and management	Manufacturers SHALL provide user documentation containing guidelines and usage instructions on implementing, configuring, and managing access control capabilities.	Inspection	Manufacturer	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTION	AC-1	Access Control Policy and Procedures	11.1.1; 11.4.1; 15.1.1	15.; 16.	---	ECAN-1; ECPA-1; PRAS-1; DCAR-1	2.B.4.e(5); 4.B.1.a(1)(b)	AC-1 ACCESS CONTROL POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls. Supplemental Guidance: The access control policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.	N/A		1	1			1		1				N/C

9.4.1.2 Access control policy	Manufacturers SHALL provide, within the user documentation, the access control policy under which the system was designed to operate.	Inspection	Manufacturer	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTION	AC-1	Access Control Policy and Procedures	11.1.1; 11.4.1; 15.1.1	15.; 16.	---	FVAP ECAN-1; ECPA-1; PRAS-1; DCAR-1	UOCA 2.B.4.e(5); 4.B.1.a(1)(b)	AC-1 ACCESS CONTROL POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls. Supplemental Guidance: The access control policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.	N/A	1	1				1		1				N/C
9.4.1.3 Privileged account	Manufacturers SHALL disclose and document information on all privileged accounts included on the system.	Inspection	Manufacturer	Loss of Integrity, Availability and/or Confidentiality	I=INSPECTION	AC-2	Account Management	6.2.2; 6.2.3; 8.3.3; 11.2.1; 11.2.2; 11.2.4; 11.7.2	6.1.8; 15.1.1; 15.1.4; 15.1.5; 15.1.8; 15.2.2; 16.1.3; 16.1.5; 16.2.12	AC-2.1; AC-2.2; AC-3.2; SP-4.1	IAAC-1	4.B.2.a(3)	AC-2 ACCOUNT MANAGEMENT Control: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts [Assignment: organization-defined frequency, at least annually]. Supplemental Guidance: Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The organization identifies authorized users of the information system and specifies access rights/privileges. The organization grants access to the information system based on: (i) a valid need-to-know/need-to-share that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage. The organization requires proper identification for requests to establish information system accounts and approves all such requests. The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. Account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' information system usage or need-to-know/need-to-share changes.	N/A	1	1	1			1						N/C
9.4.2.1 System event logging	Manufacturers SHALL provide user documentation that describes system event logging capabilities and usage.	Inspection	Manufacturer	Loss of Integrity and/or Confidentiality	I=INSPECTION	AU-2 & AU-3	Auditable Events	10.10.1	17.1.1; 17.1.2; 17.1.4	---	ECAR-3	4.B.2.a(4)(d)	AU-2 AUDITABLE EVENTS Control: The information system generates audit records for the following events: [Assignment: organization-defined auditable events]. Supplemental Guidance: The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system. The organization specifies which information system components carry out auditing activities. Auditing activity can affect information system performance. Therefore, the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Additionally, the security audit function is coordinated with the network health and status monitoring function to enhance the mutual support between the two functions by the selection of information to be recorded by each function. The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events. The organization defines auditable events that are adequate to support after-the-fact investigations of security incidents. NIST Special Publication 800-92 provides guidance on computer security log management.	N/A		1	1			1	1				N/C
9.4.2.2 Log format	Manufacturers SHALL provide fully documented log format information.	Inspection	Manufacturer	Provides forensic capability in the event of data loss. Provides troubleshooting abilitieis.	I=INSPECTION	AU-3	Content of Audit Records	10.10.1; 10.10.4	17.1.1	---	ECAR-1; ECAR-2; ECAR-3; ECLC-1	4.B.2.a(4)(a) ; 4.B.2.a(5)(a)	AU-3 CONTENT OF AUDIT RECORDS Control: The information system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. Supplemental Guidance: Audit record content includes, for most audit records: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) user/subject identity; and (v) the outcome (success or failure) of the event. NIST Special Publication 800-92 provides guidance on computer security log management.	N/A	1	1	1			1		1				N/C
9.4.3.1 Ballot decryption process	Manufacturers SHALL provide documentation on the proper procedures for the authorized entity to implement ballot decryption while maintaining the security and privacy of the data.	Inspection	Manufacturer	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTION	CM-1	Configuration Management Policy and Procedures	12.4.1; 12.5.1; 15.1.1	---	---	DCCB-1; DCPR-1; DCAR-1; E3.3.8	DCID: B.2.a Manual: 2.B.4.e(5); 5.B.2.a(5)	CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls. Supplemental Guidance: The configuration management policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The configuration management policy can be included as part of the general information security policy for the organization. Configuration management procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.	N/A	1	1				1	1				N/C
9.4.3.2 Ballot decryption key reconstruction	Manufacturers SHALL provide documentation describing the proper procedure for the authorized entity to reconstruct the election private key to decrypt the ballots.	Inspection	Manufacturer	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTION	IA-5	Authenticator Management	11.5.2; 11.5.3	15.1.6; 15.1.7; 15.1.9; 15.1.10; 15.1.11; 15.1.12; 15.1.13; 16.1.3; 16.2.3	AC-3.2	IAKM-1; IATS-1	4.B.2.a(7); 4.B.3.a(11)	IA-5 AUTHENTICATOR MANAGEMENT Control: The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.	N/A		1				1	1				N/C
9.4.3.3 Ballot decryption key destruction	Manufacturers SHALL document when any cryptographic keys created or used by the system may be destroyed. The documentation SHALL describe how to delete keys securely and irreversibly at the appropriate time.	Inspection	Manufacturer	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTION	SC-12	Cryptographic Key Establishment and Management	12.3.1; 12.3.2	16.1.7; 16.1.8	---	IAKM-1	1.G	SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT Control: When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures. Supplemental Guidance: NIST Special Publication 800-56 provides guidance on cryptographic key establishment. NIST Special Publication 800-57 provides guidance on cryptographic key management.	N/A	1	1	1			1	1				N/C

9.4.4.1 Physical security	Manufacturers SHALL provide user documentation explaining the implementation of all physical security controls for the system, including procedures necessary for effective use of countermeasures.	Inspection	Manufacturer	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTION	PE-1	Physical and Environmental Protection Policy and Procedures	15.1.1	7	PETN-1; DCAR-1	DCID: B.2.a; Manual: 2.B.4.e(5)	8.D	PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls. Supplemental Guidance: The physical and environmental protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The physical and environmental protection policy can be included as part of the general information security policy for the organization. Physical and environmental protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.		1	1	1				1	1				N/C
9.4.5.1 Ballot count and vote total auditing	The system's user documentation SHALL fully specify a secure, transparent, workable and accurate process for producing all records necessary to verify the accuracy of the electronic tabulation result.	Inspection	Manufacturer	Loss of data Integrity	I=INSPECTION	None	None	None	None	None	None	None	None	None	1	1	1				1			1		N/C
9.5.1.1 Software list	Manufacturers SHALL provide a list of all software to be installed on the programmed devices of the system and installation software used to install the software.	Inspection	Manufacturer	Loss of system Integrity and availability. Provides disaster recovery capability.	I=INSPECTION	CM-8	Information System Component Inventory	7.1.1; 15.1.2	1.1.1; 3.1.9; 10.2.7; 10.2.9; 12.1.4	CC-2.3; CC-3.1; SS-1.2	DCHW-1; DCSW-1	2.B.7.c(7); 4.B.1.c(3); 4.B.2.b(6)	CM-8 INFORMATION SYSTEM COMPONENT INVENTORY Control: The organization develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information. Supplemental Guidance: The organization determines the appropriate level of granularity for the information system components included in the inventory that are subject to management control (i.e., tracking, and reporting). The inventory of information system components includes any information determined to be necessary by the organization to achieve effective property accountability (e.g., manufacturer, model number, serial number, software license information, system/component owner). The component inventory is consistent with the accreditation boundary of the information system. Related security controls: CM-2, CM-6.	N/A	1	1	1				1	1				N/C
9.5.1.2 Software information	Manufacturers SHALL provide at a minimum, the following information for each piece of software to be installed or used to install software on programmed devices of the system: software product name, software version number, software manufacturer name, software manufacturer contact information, type of software (application logic, border logic, third party logic, COTS software, or installation software), list of software documentation, component identifier(s) (such filename(s)) of the software, type of software component (executable code, source code, or data).	Inspection	Manufacturer	Loss of system Integrity and availability. Provides disaster recovery capability.	I=INSPECTION	CM-8	Information System Component Inventory	7.1.1; 15.1.2	1.1.1; 3.1.9; 10.2.7; 10.2.9; 12.1.4	CC-2.3; CC-3.1; SS-1.2	DCHW-1; DCSW-1	2.B.7.c(7); 4.B.1.c(3); 4.B.2.b(6)	CM-8 INFORMATION SYSTEM COMPONENT INVENTORY Control: The organization develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information. Supplemental Guidance: The organization determines the appropriate level of granularity for the information system components included in the inventory that are subject to management control (i.e., tracking, and reporting). The inventory of information system components includes any information determined to be necessary by the organization to achieve effective property accountability (e.g., manufacturer, model number, serial number, software license information, system/component owner). The component inventory is consistent with the accreditation boundary of the information system. Related security controls: CM-2, CM-6.	N/A	1	1	1				1	1				N/C
9.5.1.3 Software location information	Manufacturers SHALL provide the location (such as full path name or memory address) and storage device (such as type and part number of storage device) where each piece of software is installed on programmed devices of the system.	Inspection	Manufacturer	Loss of system Integrity and availability. Provides disaster recovery capability.	I=INSPECTION	CM-8	Information System Component Inventory	7.1.1; 15.1.2	1.1.1; 3.1.9; 10.2.7; 10.2.9; 12.1.4	CC-2.3; CC-3.1; SS-1.2	DCHW-1; DCSW-1	2.B.7.c(7); 4.B.1.c(3); 4.B.2.b(6)	CM-8 INFORMATION SYSTEM COMPONENT INVENTORY Control: The organization develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information. Supplemental Guidance: The organization determines the appropriate level of granularity for the information system components included in the inventory that are subject to management control (i.e., tracking, and reporting). The inventory of information system components includes any information determined to be necessary by the organization to achieve effective property accountability (e.g., manufacturer, model number, serial number, software license information, system/component owner). The component inventory is consistent with the accreditation boundary of the information system. Related security controls: CM-2, CM-6.	N/A	1	1	1				1	1				N/C
9.5.1.4 Election specific software identification	Manufacturers SHALL identify election specific software in the user documentation.	Inspection	Manufacturer	No securiyt impact	I=INSPECTION	None	None	None	None	None	None	None	None	Special denotation within the supplied documentation		1				1			1			N/C
9.5.1.5 Installation software and hardware	Manufacturers SHALL provide a list of software and hardware required to install software on programmed devices of the system in the user documentation.	Inspection	Manufacturer	System integrity and availability	I=INSPECTION	CM-8	Information System Component Inventory	7.1.1; 15.1.2	1.1.1; 3.1.9; 10.2.7; 10.2.9; 12.1.4	CC-2.3; CC-3.1; SS-1.2	DCHW-1; DCSW-1	2.B.7.c(7); 4.B.1.c(3); 4.B.2.b(6)	Security Design and Configuration Availability DCSW-1 SW Baseline A current and comprehensive baseline inventory of all software (SW) (to include manufacturer, type, and version and installation manuals and procedures) required to support DoD information system operations is maintained by the CCB and as part of the C&A documentation. A backup copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original.	N/A		1	1		1			1				N/C
9.5.1.6 Software installation procedure	Manufacturers SHALL document the software installation procedures used to install software on programmed devices of the system.	Inspection	Manufacturer	System integrity and availability	I=INSPECTION	CM-8	Information System Component Inventory	7.1.1; 15.1.2	1.1.1; 3.1.9; 10.2.7; 10.2.9; 12.1.4	CC-2.3; CC-3.1; SS-1.2	DCHW-1; DCSW-1	2.B.7.c(7); 4.B.1.c(3); 4.B.2.b(6)	Security Design and Configuration Availability DCSW-1 SW Baseline A current and comprehensive baseline inventory of all software (SW) (to include manufacturer, type, and version and installation manuals and procedures) required to support DoD information system operations is maintained by the CCB and as part of the C&A documentation. A backup copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original.	N/A		1	1		1			1				N/C
9.5.1.7 Compiler installation prohibited	The software installation procedures used to install software on programmed devices of the system SHALL specify that no compilers SHALL be installed on the programmed device.	Inspection	Manufacturer	No direct security implication of this addition to the documentation. However, installation of compilers could impact confidentiality, availablity and integrity.	I=INSPECTION	None	None	None	None	None	None	None	End user software is prohibited. However, no specific guidance on compilers within the referenced documetation.	None	1	1	1			1				1			N/C
9.5.1.8 Procurement of system software	The software installation procedures SHALL specify that system software SHALL be obtained from the VSTL or approved distribution repositories.	Inspection	Manufacturer	Approved software use only. Potential loss of availability, integrity and confidentiality.	I=INSPECTION	SA-1	System and Services Acquisition Policy and Procedures	12.1; 15.1.1	3	---	DCAR-1	DCID: B.2.a; Manual: 2.B.4.e(5)	No direct security implication of this addition to the documentation. However, installation of compilers could impact confidentiality, availablity and integrity.	None		1	1		1							N/C
9.5.1.9 Erasable storage media preparation	The software installation procedures SHALL specify how previously stored information on erasable storage media is removed before installing software on the media.	Inspection	Manufacturer	Medium: Loss of Integrity	I=INSPECTION	MP-1 MP-6	Media Protection Policy and Procedures	10.1.1; 10.7; 15.1.1; 15.1.3	8.2	---	PESP-1; DCAR-1	DCID: B.2.a Manual:; 2.B.6.c(7); 8.B.2	MP-1 MEDIA PROTECTION POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.	N/A	1	1			1			1				Recommend that DoD guidance for erasable media be used.
9.5.1.10 Installation media unalterable storage media	The software installation procedures SHALL specify that unalterable storage media SHALL be used to install software on programmed devices of the system.	Inspection	Manufacturer	Medium: Loss of Integrity	I=INSPECTION	MP-1	Media Protection Policy and Procedures	10.1.1; 10.7; 15.1.1; 15.1.3	8.2	---	PESP-1; DCAR-1	DCID: B.2.a Manual:; 2.B.6.c(7); 8.B.2	MP-1 MEDIA PROTECTION POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.	N/A		1	1			1		1				N/C

											FVAP	UOCA												
9.5.1.11 Software hardening	Manufacturers SHALL provide documentation that describes the hardening procedures for the system.	Inspection	Manufacturer	High: Loss of Integrity, Availability, and/or Confidentiality	I=INSPECTION	SA-11	Developer Security Testing	12.5.1; 12.5.2	3.2.1; 3.2.2; 10.2.5; 12.1.5	SS-3.1; CC-2.1	E3.4.4	4.B.4.b(4)	NIST SP800-137: A security configuration checklist, sometimes referred to as a lockdown guide, hardening guide, or benchmark configuration, is essentially a document that contains instructions or procedures for configuring an information technology (IT) product to a baseline level of security. SA-11 DEVELOPER SECURITY TESTING Control: The organization requires that information system developers create a security test and evaluation plan, implement the plan, and document the results. Supplemental Guidance: Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security relevant modifications to the information system subsequent to developer testing. Test results may be used in support of the security certification and accreditation process for the delivered information system. Related security controls: CA-2, CA-4.	N/A	1	1	1				1	1				N/C
9.6.1 Setup inspection process	Manufacturers SHALL provide a setup inspection process that the system was designed to support.	Inspection	Manufacturer	High: Loss of Integrity, Availability, and/or Confidentiality	I=INSPECTION	None	None	None	None	None	None	None	DCID 6/3 Requirement: 4.B.2.b(7)(b) A test plan and procedures shall be developed and include: 4.B.2.b(7)(b)(1) A detailed description of the manner in which the system's Security Support Structure meets the technical requirements for the Protection Levels and Levels-of-Concern for integrity and availability. 4.B.2.b(7)(b)(2) A detailed description of the assurances that have been implemented, and how this implementation will be verified. 4.B.2.b(7)(b)(3) An outline of the inspection and test procedures used to verify this compliance.	N/A	1	1	1				1	1				N/C
9.6.1.1 Minimum properties included in a setup inspection process	A setup inspection process SHALL, at a minimum, include the inspection of system software, storage locations that hold election information that changes during an election, and execution of logic and accuracy testing related to readiness for use in an election.	Inspection	Manufacturer	High: Loss of Integrity, Availability, and/or Confidentiality	I=INSPECTION	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	SA-5 INFORMATION SYSTEM DOCUMENTATION Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system. Supplemental Guidance: Documentation includes administrator and user guides with information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features. When adequate information system documentation is either unavailable or non existent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), the organization documents attempts to obtain such documentation and provides compensating security controls, if needed.		1	1	1			1		1				N/C
9.6.1.2 Setup inspection record generation	The setup inspection process SHALL describe the records that result from performing the setup inspection process.	Inspection	Manufacturer		I=INSPECTION	None	None	None	None	None	None	None	NIST SP800-100 States: In addition, developing a security requirements checklist based on the security requirements specified for the system during the conceptual, design, and implementation phases of the SDLC can be used to provide a 360-degree inspection of the system.		1	1	1			1			1		N/C
9.6.1.3 Installed software identification procedure	Manufacturers SHALL provide the procedures to identify all software installed on programmed devices.	Inspection	Manufacturer	High: Loss of Integrity, Availability, and/or Confidentiality	I=INSPECTION	SI-1	System and Information Integrity Policy and Procedures	15.1.1	11	---	DCAR-1	DCID: B.2.a; Manual: 2.B.4.e(5); 5.B.1.b(1) 5.B.2.a(5)(a)(1)	SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls. Supplemental Guidance: The system and information integrity policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.	N/A		1	1			1		1				N/C
9.6.1.4 Software integrity verification procedure	Manufacturers SHALL describe the procedures to verify the integrity of software installed on programmed devices of system.	Inspection	Manufacturer	High: Loss of Integrity, Availability, and/or Confidentiality	I=INSPECTION	SI-1	System and Information Integrity Policy and Procedures	15.1.1	11	---	DCAR-1	DCID: B.2.a; Manual: 2.B.4.e(5); 5.B.1.b(1) 5.B.2.a(5)(a)(1)	SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls. Supplemental Guidance: The system and information integrity policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.	N/A		1				1	1				N/C
9.6.1.5 Election information value	Manufacturers SHALL provide the values of system storage locations that hold election information that changes during the election, except for the values set to conduct a specific election.	Inspection	Manufacturer	Medium: Loss of Integrity, Availability and/or confidentiality	I=INSPECTION	MP-4	Media Storage	10.7.1; 10.7.2; 10.7.3; 10.7.4; 15.1.3	7.1.4; 8.2.1; 8.2.2; 8.2.9; 10.1.2	AC-3.1	PESS-1	2.B.9.b(4); 4.B.1.a(7)	MP-4 MEDIA STORAGE Control: The organization physically controls and securely stores information system media within controlled areas.	N/A	1	1	1			1		1			N/C
9.6.1.6 Maximum values of election information storage locations	Manufacturers SHALL provide the maximum values for the storage locations where election information is stored.	Inspection	Manufacturer	Medium: Loss of Integrity, Availability and/or confidentiality	I=INSPECTION	MP-4	Media Storage	10.7.1; 10.7.2; 10.7.3; 10.7.4; 15.1.3	7.1.4; 8.2.1; 8.2.2; 8.2.9; 10.1.2	AC-3.1	PESS-1	2.B.9.b(4); 4.B.1.a(7)	MP-4 MEDIA STORAGE Control: The organization physically controls and securely stores information system media within controlled areas.	N/A	1	1	1			1		1			N/C
9.6.1.7 Backup power operational range	Manufacturers SHALL provide the nominal operational range for the backup power sources of the voting system.	Inspection	Manufacturer	Medium: Loss of Integrity, Availability and/or confidentiality	I=INSPECTION	PE-11	Emergency Power	9.2.2	7.1.18	SC-2.2	COPS-1; COPS-2; COPS-3	6.B.2.a(6); 6.B.2.a(7)	PE-11 EMERGENCY POWER Control: The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss. Supplemental Guidance: None.	N/A	1	1	1		1			1			N/C
9.6.1.8 Backup power inspection procedure	Manufacturers SHALL provide the procedures to inspect the remaining charge of the backup power sources of the voting system.	Inspection	Manufacturer	Medium: Loss of Integrity and/or Availability	I=INSPECTION	PE-1	Physical and Environmental Protection Policy and Procedures	15.1.1	7	PETN-1; DCAR-1	DCID: B.2.a; Manual: 2.B.4.e(5)	8.D	PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	N/A		1	1			1		1				N/C
9.6.1.9 Cabling connectivity inspection procedure	Manufacturers SHALL provide the procedures to inspect the connectivity of the cabling attached to the vote capture device.	Inspection	Manufacturer	Medium: Loss of Integrity and/or Availability	I=INSPECTION	PE-1	Physical and Environmental Protection Policy and Procedures	15.1.1	7	PETN-1; DCAR-1	DCID: B.2.a; Manual: 2.B.4.e(5)	8.D	PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	N/A		1	1			1		1				N/C
9.6.1.10 Communications operational status inspection procedure	Manufacturers SHALL provide the procedures to inspect the operational status of the communications capabilities of the vote capture device.	Inspection	Manufacturer	Medium: Loss of Integrity and/or Availability	I=INSPECTION	PE-1	Physical and Environmental Protection Policy and Procedures	15.1.1	7	PETN-1; DCAR-1	DCID: B.2.a; Manual: 2.B.4.e(5)	8.D	PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	N/A		1	1				1	1				N/C

9.6.1.11 Communications on/off status inspection procedure	Manufacturers SHALL provide the procedures to inspect the on/off status of the communications capabilities of the vote capture device.	Inspection	Manufacturer	Medium: Loss of Integrity and/or Availability	I=INSPECTION	PE-4	Access Control for Transmission Medium	9.2.3	7.2.2; 16.2.9	---	---	8.D.2; 4.B.1.a(8)	PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM Control: The organization controls physical access to information system distribution and transmission lines within organizational facilities. Supplemental Guidance: Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.	N/A		1	1				1	1				N/C
9.6.1.12 Consumables quantity of vote capture device	Manufacturers SHALL provide a list of consumables associated with the vote capture device, including estimated number of usages per quantity of consumable.	Inspection	Manufacturer	No known security risk.	I=INSPECTION	None	None	None	None	None	None	None	No specific IA Control referenced.	None			1		1					1		N/C
9.6.1.13 Consumable inspection procedure	Manufacturers SHALL provide the procedures to inspect the remaining amount of each consumable of the vote capture device.	Inspection	Manufacturer	No known security risk.	I=INSPECTION	None	None	None	None	None	None	None	No specific IA Control referenced.	None			1		1					1		N/C
9.6.1.14 Calibration of vote capture device components nominal range	Manufacturers SHALL provide a list of components associated with the vote capture devices that require calibration and the nominal operating ranges for each component.	Inspection	Manufacturer	No known security risk.	I=INSPECTION	None	None	None	None	None	None	None	No specific IA Control referenced.	None		1				1				1		N/C
9.6.1.15 Calibration of vote capture device components inspection procedure	Manufacturers SHALL provide the procedures to inspect the calibration of each component.	Inspection	Manufacturer	No known security risk.	I=INSPECTION	None	None	None	None	None	None	None	No specific IA Control referenced.	None		1				1				1		N/C
9.6.1.16 Calibration of vote capture device components adjustment procedure	Manufacturers SHALL provide the procedures to adjust the calibration of each component.	Inspection	Manufacturer	Calibration could impact system Integrity	I=INSPECTION	CM-1	Configuration Management Policy and Procedures	12.4.1; 12.5.1; 15.1.1	---	---	DCCB-1; DCPR-1; DCAR-1; E3.3.8	DCID: B.2.a Manual: 2.B.4.e(5); 5.B.2.a(5)	CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	N/A		1	1				1					N/C
9.6.1.17 Checklist of properties to be inspected	Manufacturers SHALL provide a checklist of other properties of the system to be inspected.	Inspection	Manufacturer	Checklists are important, but may not have direct impact on security.	I=INSPECTION	CM-1	Configuration Management Policy and Procedures	12.4.1; 12.5.1; 15.1.1	---	---	DCCB-1; DCPR-1; DCAR-1; E3.3.8	DCID: B.2.a Manual: 2.B.4.e(5); 5.B.2.a(5)	CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	N/A		1	1				1					N/C
9.7.1.1 System operations manual	The system operations manual SHALL provide all information necessary for system set up and use by all personnel who administer and operate the system at the state and/or local election offices and at the kiosk locations, with regard to all system functions and operations identified in Section 9.3 System Functionality Description.	Inspection	Manufacturer	High: Loss of Integrity, Availability, and/or Confidentiality	I=INSPECTION	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD 1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	SA-5 INFORMATION SYSTEM DOCUMENTATION Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system. Supplemental Guidance: Documentation includes administrator and user guides with information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features. When adequate information system documentation is either unavailable or non existent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), the organization documents attempts to obtain such documentation and provides compensating security controls, if needed.	N/A	1	1	1			1		1				N/C
9.7.1.2 Support training	The system operations manual SHALL contain all information that is required for the preparation of detailed system operating procedures and for the training of administrators, state and/or local election officials, election judges, and kiosk workers.	Inspection	Manufacturer	High: Loss of Integrity, Availability, and/or Confidentiality	I=INSPECTION	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD 1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	Nothing found about training the operators!		1	1	1			1		1				N/C
9.7.2.1 Functions	Manufacturers SHALL provide a summary of system operating functions to permit understanding of the system's capabilities and constraints.	Inspection	Manufacturer	High: Loss of Integrity, Availability, and/or Confidentiality	I=INSPECTION	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD 1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	DCSQ-1 Software Quality Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives.	N/A	1	1	1			1		1				N/C
9.7.2.2 Roles	The roles of operating personnel SHALL be identified and related to the functions of the system.	Inspection	Manufacturer	High: Loss of Integrity, Availability, and/or Confidentiality	I=INSPECTION	AC-2	Account Management	6.2.2; 6.2.3; 8.3.3; 11.2.1; 11.2.2; 11.2.4; 11.7.2	6.1.8; 15.1.1; 15.1.4; 15.1.5; 15.1.8; 15.2.2; 16.1.3; 16.1.5; 16.2.12	AC-2.1; AC-2.2; AC-3.2; SP-4.1	IAAC-1	4.B.2.a(3)	DCPR-1 CM Process A configuration management (CM) process is implemented that includes requirements for: (1) Formally documented CM roles, responsibilities, and procedures to include the management of IA information and documentation; (2) A configuration control board that implements procedures to ensure a security review and approval of all proposed DoD information system changes, to include inter-connections to other DoD information systems; (3) A testing process to verify proposed configuration changes prior to implementation in the operational environment; and (4) A verification process to provide additional assurance that the CM process is working effective	N/A			1		1			1					N/C
Totals														**150**	**246**	**191**	**0**	**41**	**130**	**88**	**186**	**0**	**28**	**58**	**15**

NIST Security Objective	Potential Impact		
	Low	Medium	High
Confidentialy Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or
Integrity Guarding against improper information modification or destruction, and includes ensuring information non repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. Basic Testing A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.