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*

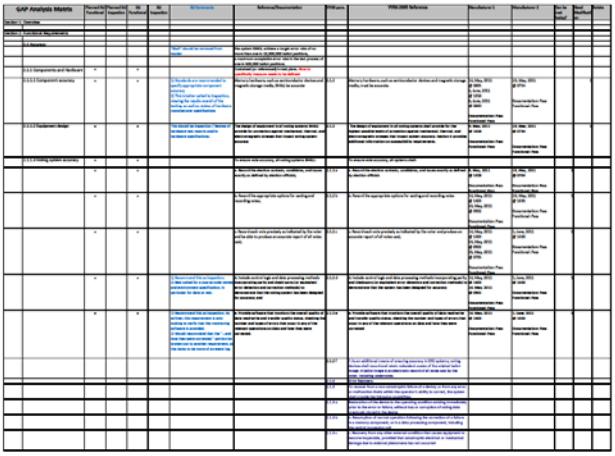
Prepared by:

216 16th St.
Suite 700
Denver, CO 80202
303-575-6881
www.SLIGlobalsolutions.com

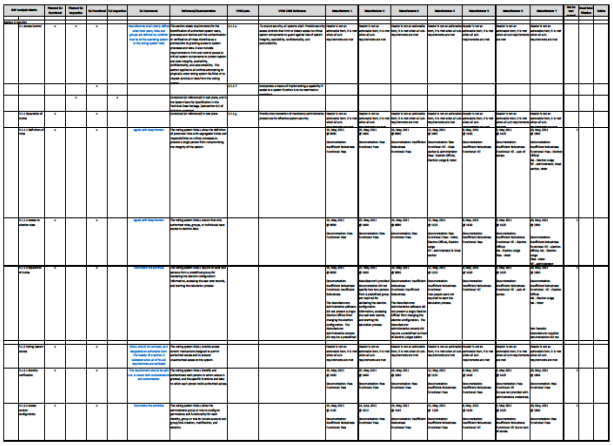
NVLAP LAB CODE 200755-0

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. There was no time-out	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 Modification	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: nsufficient 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	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