

FVAP Statement on Research Reports Related to UOCAVA System Testing

Scope and Purpose

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 In 2015, Congress eliminated this requirement; however, the resulting reports from the commissioned research remained unpublished at the time of the repeal.

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

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

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

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

Limitations on Voting System Laboratory Testing (VSTL) Report

- Vendors did not submit source code or technical data packages and no code review was performed. There was no opportunity for remediation.
- Indications of pass/fail in the test results do not indicate how well a particular system would perform during a full certification test and may be the result of test interpretation or applicability.
- No systems were presented for certification and certification was not a potential outcome. Only a small portion of the complete UPPTR was studied. Sections two and five of the UPPTR were evaluated and the remaining eight sections were not evaluated.
- The formal EAC process for voting system certification was not followed. Manufacturers are normally allowed to remediate any deficiencies found and submit the system for retesting. For this study, there was no interaction between the EAC, the manufacturer, and the Voting System Testing Laboratory. Each system was evaluated once, in a limited fashion, and the results documented.

Limitations on Penetration Test Model Design and Methodology

- These tests were only intended to serve as a proof-of-concept for the establishment of a model design and methodology for future penetration testing.
- The manufacturer names are not disclosed. The purpose behind these tests was not to evaluate any specific system, but to evaluate the requirements and the process.
- The penetration test period was limited to 72 hours, a significant limitation from expected real world conditions.
- Certain types of attacks, such as Distributed Denial of Service, social engineering, and physical tampering were not allowed. Since the time of this research, the attack profiles and methodologies have significantly changed, thus these tests should be viewed only within the context of when they were conducted.

Conclusions

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

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

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


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

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

Recommendations

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

1. Integration of the individual report findings and recommendations into the consideration of future voting system standards.
2. Exploration into the viability of incorporating structured penetration testing for *UOCAVA*-related systems and qualifications for penetration testers.



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

11 November 2011





Voting System Testing Laboratory Functionality and Security Testing

Delivery Order # 80047-0037

Task Order # 5.1.1

Final Report

Version 2

11 November 2011

Executive Summary

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

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

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

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

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

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

VSTL Testing of UPPTR Section 5 (Security)

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

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

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

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

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

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

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

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

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

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

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

Conclusion

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

Table of Contents

Executive Summary	iii
Table of Contents	vi
Table of Figures	ix
1 Introduction	11
1.1 Background	11
1.2 FVAP Initiation of the VSTL Testing	12
1.3 VSTLs	12
1.4 VSTL Testing	13
2 Methodology	14
2.1 EAC Certification Requirements	14
2.2 VSTLs' Methodologies	14
2.2.1 SLI's Standard Methodology	14
2.2.2 Wyle's Standard Methodology	17
2.3 FVAP Approach	19
2.4 Impact of FVAP Approach	20
3 Electronic Ballot Delivery Systems (EBDS) Testing Results for UPPTR Section 5 (Security)	22
3.1 Access Control (UPPTR 5.1)	24
3.2 Identification and Authentication (UPPTR 5.2)	24
3.3 Cryptography (UPPTR 5.3)	25
3.4 Voting System Integrity Management (UPPTR 5.4)	25
3.5 Communications Security (UPPTR 5.5)	26

3.6	Logging (UPPTR 5.6)	26
3.7	Incident Response (UPPTR 5.7)	27
3.8	Physical and Environmental Security (UPPTR 5.8)	27
3.9	Penetration Resistance (UPPTR 5.9).....	28
3.10	Testing Summary for UPPTR Section 5	29
4	Internet Voting Systems (IVS) Testing Results for UPPTR Section 2 (Functional Requirements) and Section 5 (Security).....	32
4.1	SLI's Testing Results for UPPTR Section 2 (Functional Requirements)	32
4.1.1	Accuracy (UPPTR 2.1)	33
4.1.2	Operating Capabilities (UPPTR 2.2).....	33
4.1.3	Pre-Voting Capabilities (UPPTR 2.3).....	34
4.1.4	Voting Capabilities (UPPTR 2.4).....	34
4.1.5	Post-Voting Capabilities (UPPTR 2.5)	35
4.1.6	Audit and Accountability (UPPTR 2.6)	35
4.1.7	Performance Monitoring (UPPTR 2.7)	36
4.2	VSTL Testing Results for UPPTR Section 5 (Security)	36
4.2.1	Access Control (UPPTR 5.1)	37
4.2.2	Identification and Authentication (UPPTR 5.2).....	37
4.2.3	Cryptography (UPPTR 5.3).....	38
4.2.4	Integrity Management (UPPTR 5.4)	38
4.2.5	Communications Security (UPPTR 5.5)	38
4.2.6	Logging (UPPTR 5.6)	39
4.2.7	Incident Response (UPPTR 5.7)	39

4.2.8	Physical and Environmental (UPPTR 5.8).....	39
4.2.9	Penetration Resistance (UPPTR 5.9)	40
4.3	VSTL Full system Testing Summary	40
5	Recommendations.....	43
5.1	Recommendations for Changes to the UPPTR	43
5.2	Recommendation for the VSTLs.....	43
5.3	Recommendations for Standardizing Processes and Measurements for Future FVAP Testing...	44
5.4	Recommendations for Further Testing.....	45
	Appendix A – Glossary.....	47
	Appendix B – UOCAVA Pilot Program Testing Requirements.....	51
	Appendix C – VSTLs' Comments to the UPPTR	52
	Appendix D – Changes to the VSTL Standard Testing Methodology for UPPTR.....	53
	Appendix E – SLI Global Solutions Test Report.....	55
	Appendix F – Wyle Laboratories Test Plan and Test Report	56

Table of Figures

Figure 1: VSTLs' Standard Methodology for EAC Certification and Deviations.....	20
Figure 2: VSTLs' Assessment of the UPPTR Section 5 (Security).....	23
Figure 3: Access Control Test Results Averages and Ranges	24
Figure 4: Identification and Authorization Test Results Averages and Ranges	25
Figure 5: Cryptography Test Results Averages and Ranges.....	25
Figure 6: Integrity Management Test Results Averages and Ranges	26
Figure 7: Communications Security Test Results Averages and Ranges	26
Figure 8: Logging Test Results Averages and Ranges	27
Figure 9: Incident Response Test Results Averages and Ranges	27
Figure 10: Test Results Averages and Ranges for Physical and Environmental	28
Figure 11: Test Results Averages and Ranges for Penetration Resistance	29
Figure 12: VSTL Test Results for UPPTR Section 5 (Security)	30
Figure 12a: VSTLs' Average Pass / Fail Percentages.....	31
Figure 12b: Pass Percentages by System	31
Figure 13: SLI's Assessment of the UPPTR Section 2 (Functional Requirement)	33
Figure 14: Accuracy Test Results Averages	33
Figure 15: Operating Capabilities Test Results Averages	34
Figure 16: Pre-Voting Capabilities Test Results Averages.....	34
Figure 17: Voting Capabilities Test Results Averages	35
Figure 18: Post-Voting Capabilities Test Results Averages	35
Figure 19: Audit and Accountability Test Results Averages.....	36

Figure 20: Performance Monitoring Test Results Averages.....	36
Figure 21: Access Control Test Results Averages.....	37
Figure 22: Identification and Authentication Test Results Averages	37
Figure 23: Cryptography Test Results Averages	38
Figure 24: Integrity Management Test Results Averages.....	38
Figure 25: Communications Security Test Results Averages.....	39
Figure 26: Logging Test Results Averages.....	39
Figure 27: Incident Response Test Results Averages.....	39
Figure 28: Physical and Environmental Test Results Averages	40
Figure 29: Penetration Resistance Test Results Averages	40
Figure 30: SLI Testing Average Results for UPPTR Section 2 (Functional Requirements).....	41
Figure 31: SLI Testing Results for UPPTR Section 5 (Security)	41

1 Introduction

1.1 Background

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

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

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

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

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

¹ Public Law 111-84—Oct. 28, 2009. 123 STAT. 2335, SEC. 589. Technology Pilot Program., paragraph (e.)(1). Page 20.

² U.S. Election Assistance Commission. 2010. Uniformed and Overseas Citizens Absentee Voting Act Pilot Program Testing Requirements, August 25, 2010. Page 7. See [Appendix B](#).

³ Ibid, page 16 and page 134.

1.2 FVAP Initiation of the VSTL Testing

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

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

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

1.3 VSTLs

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

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

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

1.4 VSTL Testing

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

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

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

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

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

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

2 Methodology

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

2.1 EAC Certification Requirements

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

2.2 VSTLs' Methodologies

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

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

2.2.1 SLI's Standard Methodology

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

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

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

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

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

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

2.2.1.1 SLI First Phase - Documentation Review and Test Preparation

The first phase consists of six activities:

- Receipt of the system components and applicable documentation from the vendor;
- Technical Data Package (TDP) review;
- Vendor training on the various aspects of their system;
- A comparison of the documentation against applicable requirements to verify that all needed information is appropriately conveyed;
- A source code review; and
- A test plan is created at the end of this phase that details the system variations to be tested, and how the test suites⁶ will be constructed for testing the declared system functionality. The test plan development continues throughout the testing lifecycle and is completed at the end of phase five.

2.2.1.2 SLI Second Phase - System Familiarization & Readiness

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

2.2.1.3 SLI Third Phase - Test Development

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

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

2.2.1.4 SLI Fourth Phase - Test Validation

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

2.2.1.5 SLI Fifth Phase - Test Execution

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

2.2.1.6 SLI Sixth Phase - Project Administration and Reporting

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

2.2.1.7 SLI Seventh Phase - Finalization

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

2.2.1.8 SLI Test Result Definitions

SLI used the following definitions for reporting test results:

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

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

2.2.2 Wyle's Standard Methodology

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

2.2.2.1 Wyle First Phase - Test Plan and Engineering Analysis

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

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

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

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

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

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

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

2.2.2.2 Wyle Second Phase - Testing Phase

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

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

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

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

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

2.2.2.3 Wyle Third Phase - Test Report

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

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

2.2.2.4 Wyle Test Result Definitions

Wyle used the following definitions for reporting test results:

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

2.3 FVAP Approach

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

Inclusions:

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

Exclusions:

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

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

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

2.4 Impact of FVAP Approach

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

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

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

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

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

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

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

Section 5 of the UPPTTR consists of the following subsections:

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

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

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

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

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

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

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

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

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

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

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

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

3.1 Access Control (UPPTR 5.1)

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

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

Figure 3: Access Control Test Results Averages and Ranges

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

3.2 Identification and Authentication (UPPTR 5.2)

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

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

Figure 4: Identification and Authorization Test Results Averages and Ranges

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

3.3 Cryptography (UPPTTR 5.3)

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

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

Figure 5: Cryptography Test Results Averages and Ranges

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

3.4 Voting System Integrity Management (UPPTTR 5.4)

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

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

Figure 6: Integrity Management Test Results Averages and Ranges

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

3.5 Communications Security (UPPTR 5.5)

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

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

Figure 7: Communications Security Test Results Averages and Ranges

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

3.6 Logging (UPPTR 5.6)

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

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

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

Figure 8: Logging Test Results Averages and Ranges

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

3.7 Incident Response (UPPTR 5.7)

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

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

Figure 9: Incident Response Test Results Averages and Ranges

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

3.8 Physical and Environmental Security (UPPTR 5.8)

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

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

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

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

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

3.9 Penetration Resistance (UPPTR 5.9)

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

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

Figure 11: Test Results Averages and Ranges for Penetration Resistance

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

3.10 Testing Summary for UPPTR Section 5

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

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

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

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

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

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

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

Figure 13a: VSTLs' Average Pass / Fail Percentages

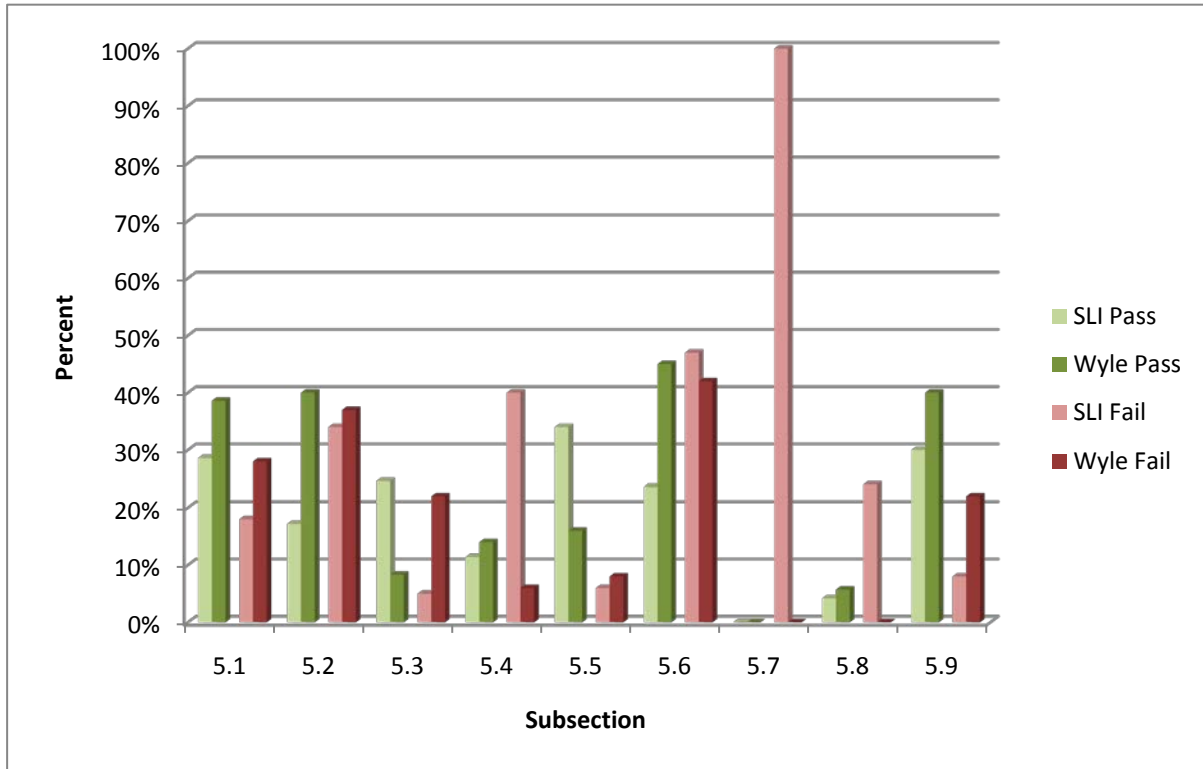
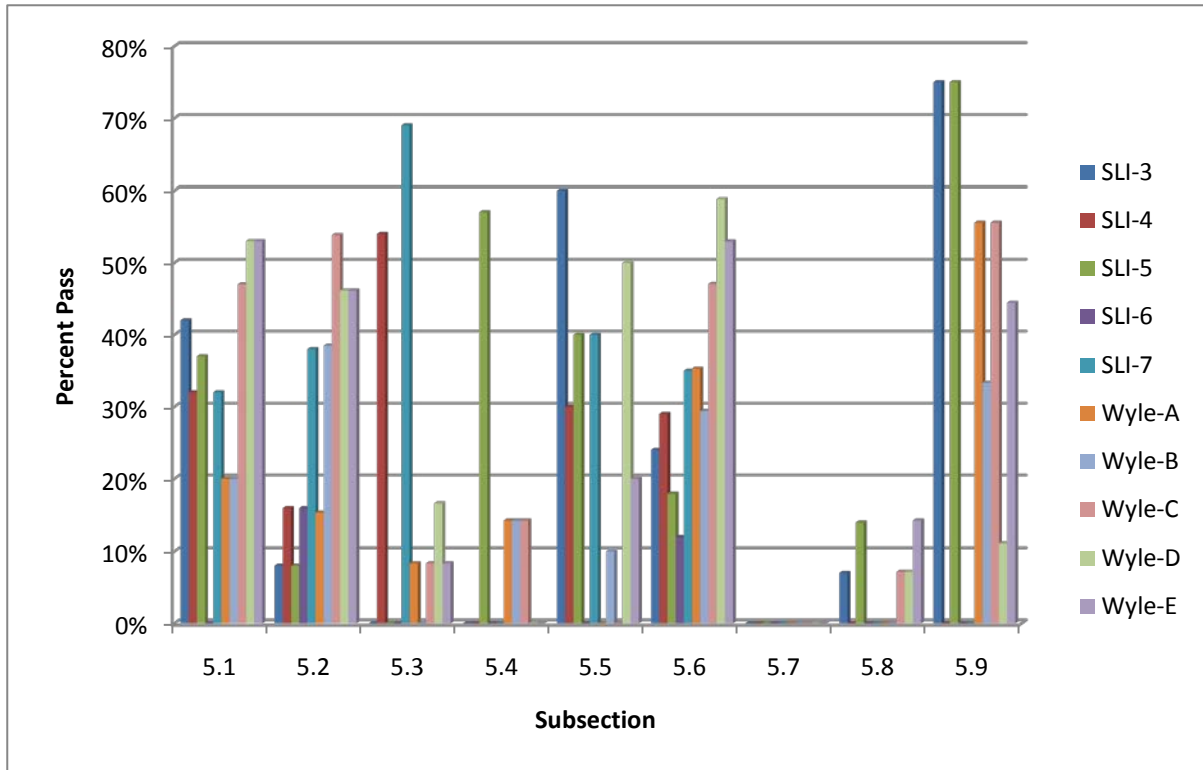


Figure 14b: Pass Percentages by System



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

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

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

4.1 SLI’s Testing Results for UPPTTR Section 2 (Functional Requirements)

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

Section 2 of the UPPTTR consists of the following subsections:

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

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

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

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

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

4.1.1 Accuracy (UPPTR 2.1)

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

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

Figure 16: Accuracy Test Results Averages

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

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

4.1.2 Operating Capabilities (UPPTR 2.2)

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

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

Figure 17: Operating Capabilities Test Results Averages

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

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

4.1.3 Pre-Voting Capabilities (UPPTR 2.3)

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

Figure 18: Pre-Voting Capabilities Test Results Averages

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

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

4.1.4 Voting Capabilities (UPPTR 2.4)

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

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

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

Figure 19: Voting Capabilities Test Results Averages

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

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

4.1.5 Post-Voting Capabilities (UPPTR 2.5)

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

Figure 20: Post-Voting Capabilities Test Results Averages

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

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

4.1.6 Audit and Accountability (UPPTR 2.6)

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

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

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

Figure 21: Audit and Accountability Test Results Averages

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

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

4.1.7 Performance Monitoring (UPPTR 2.7)

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

Figure 22: Performance Monitoring Test Results Averages

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

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

4.2 VSTL Testing Results for UPPTR Section 5 (Security)

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

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

Section 5 of the UPPTR consists of the following subsections:

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

4.2.1 Access Control (UPPTR 5.1)

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

Figure 23: Access Control Test Results Averages

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

4.2.2 Identification and Authentication (UPPTR 5.2)

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

Figure 24: Identification and Authentication Test Results Averages

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

System B	54%	38%	8%	0%
----------	-----	-----	----	----

4.2.3 Cryptography (UPPTR 5.3)

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

Figure 25: Cryptography Test Results Averages

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

4.2.4 Integrity Management (UPPTR 5.4)

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

Figure 26: Integrity Management Test Results Averages

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

4.2.5 Communications Security (UPPTR 5.5)

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

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

Figure 27: Communications Security Test Results Averages

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

4.2.6 Logging (UPPTR 5.6)

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

Figure 28: Logging Test Results Averages

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

4.2.7 Incident Response (UPPTR 5.7)

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

Figure 29: Incident Response Test Results Averages

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

4.2.8 Physical and Environmental (UPPTR 5.8)

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

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

Figure 30: Physical and Environmental Test Results Averages

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

4.2.9 Penetration Resistance (UPPTR 5.9)

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

Figure 31: Penetration Resistance Test Results Averages

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

4.3 VSTL Full system Testing Summary

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

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

5 Recommendations

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

5.1 Recommendations for Changes to the UPPTR

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

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

5.2 Recommendation for the VSTLs

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

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

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

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

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

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

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

5.3 Recommendations for Standardizing Processes and Measurements for Future FVAP Testing

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

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

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

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

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

5.4 Recommendations for Further Testing

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

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

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

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